IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe LB266 Security comment resolutions | | | | |
| Date: 2022-08-08 | | | | |
| 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 LB266 on Clause 12 of P802.11be D2.0. The resolutions will be shown relative to D2.0.

CIDs 13193, 11990, 13156, 13157, 13158, 13159, 12090, 13160, 12091, 13161, 13162, 13163, 13173, 12092. 12093, 12322, 13164, 13165, 13166, 13167, 13168, 13169, 13170, 12371, 12979, 12372, 13171, 13172, 13599

Rev 1: Tagged some CIDs in green (Alfred Asterjadhi) as part of the fast track process.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13193 | 12 |  |  | "value of the LinkID field" v "value in the LinkID field" inconsistency | Pick one |

### Discussion:

* The location of the cited phrases is here:

Timeline

Description automatically generated

* In this context, the “value in the” makes more sense.

### Proposed Resolution: (13193)

REVISED. At 355.18, change “value of the LinkID field.” 5o “value in the LinkID field.”

### Comments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 11990 | 12.2.4 | 333 | 23 | Spelling error | Change "EAPoL-key" to "EAPOL-key" |
| 13156 | 12.2.4 | 333 | 23 | "EAPoL-key frames" are referred to as "EAPOL-Key frames" | As it says in the comment |

### Discussion:

* The spelling should be EAPOL-Key.

### Proposed Resolution: (11190, 13156)

REVISED. At the cited location, change “EAPol-key” to “EAPOL-Key”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13157 | 12.2.4 | 333 | 22 | It is not clear what this new text is trying to say. The contents of the frames are defined in Clause 9, so an additional "shall" here is not necessary. Also EAPOL-Key frames do not have frame bodies; they are a PDU | Do not make the changes proposed in this subclause |
| 13158 | 12.2.4 | 333 | 22 | It is not clear what this new text is trying to say. The contents of the frames are defined in Clause 9, so an additional "shall" here is not necessary. Also EAPOL-Key frames do not have frame bodies; they are a PDU | Change to "When an RSNA is established between peer MLD SMEs, the MAC address that appears in the frame body of Authentication and Association frames (see 9.4.2.312 (Multi-Link element)) and within EAPOL-Key frames (see 12.7.2 (EAPOL-Key frames)) shall be the MLD MAC address not the STA MAC address." |

### Discussion:

* CID 13157 and CID 13158 are the same comment with different proposed resolutions
* Cited text is the following:

Graphical user interface, text

Description automatically generated

* The text requires the MLD MAC address to be carried in authentication, association, and EAPOL-Key frames for MLO.
* The text is behavioral so it cannot be deleted.
* The proposed change in CID 13158 looks reasonable but the STA MAC address MAC address is never carried in the frame body of these frames.

### Proposed Resolution: (13157, 13158)

REVISED. At the cited location, change

“When an RSNA is established between peer MLD SMEs, the MLD MAC address shall be included in the frame body of Authentication, Association (see 9.4.2.312 (Multi-Link element)), and EAPoL-key frames (see 12.7.2 (EAPOL-Key frames)).’

To

“When an RSNA is established between peer MLD SMEs, the MAC address that appears in the

frame body of authentication and association frames (see 9.4.2.312 (Multi-Link element)) and within EAPOL-Key frames (see 12.7.2 (EAPOL-Key frames)) shall be the MLD MAC address.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13159 | 12.2 | 333 | 14 | All these "STA or MLD" and similar are unclear: so, which shall do whatever it is? What if on one side the MLD decides to do it while on the other side a STA decides to do it? | Recast in terms of "MLD (if it exists) or otherwise the STA" |

### Discussion:

* The term “STA or MLD” is used 8 times in Clause 12 and generally refers to either the STA or the MLD negotiating a security association.
* A security association is only negotiated between peer STAs or peer MLDs, so the usage of the term above makes sense.
* It might be good to add a clarification in 12.1 to explain the usage of this term.

### Proposed Resolution: (13159)

REVISED. At 333.12, replace

“For MLO, the “SME” is the entity that manages the MLD.”

with

“For MLO, security associations are negotiated between peer MLDs. The use of the term “STA or MLD” refers to requirements on a STA when peer STAs establish a security association, or requirements on an MLD when peer MLDs establish a security association. In the case where MLDs negotiate a security association, the “SME” is the entity that manages the MLD.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 12090 | 12.3.3.2.2 | 334 | 35 | In pg 334 line 18 it implies that the requester is the MLD instead of the STA affiliated with the MLD, while in pg 334 line 35, it says the requester is a non-AP STA affiliated with a non-AP MLD, please clarify. | Change to "If the requester is a non-AP MLD" |
| 13160 | 12.3.3.2.2 | 334 | 35 | It's not clear what this "may" is about. Obviously it may transmit on the recommended link, but if it's just a recommended link it could pick another link. The "unless specified otherwise" makes it even more confusing | Change to "NOTE---If the requester is a non-AP STA affiliated with a non-AP MLD, it might initiate the transmission of the Authentication frame on the recommended link included in the MLME-AUTHENTICATE.request primitive, unless specified otherwise, or it might pick another link." |

### Discussion:

* Text

  Description automatically generatedThe cited text is:
* In the case of MLO, the requestor is a non-AP MLD.
* It’s the SME of MLD that is initiating the MLME-AUTHENTICATE.request.
* It looks like this is really a “may” requirement.

### Proposed Resolution: (12090, 13160)

REVISED. At cited location, replace:

“If the requester is a non-AP STA affiliated with a non-AP MLD, it may initiate the transmission of the Authentication frame on the recommended link included in the MLME-AUTHENTICATE.request primitive, unless specified otherwise.

with

“If the requester is a non-AP MLD, it may initiate the transmission of the Authentication frame by the affiliated STA operating on the recommended link included in the MLME-AUTHENTICATE.request primitive.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 12091 | 12.4.1 | 334 | 48 | Duplicate claiming of "STA" and "SME" as clause 12.1 | Remove it |
| 13161 | 12.4.1 | 334 | 48 | These statements are covered by the statements in 12.1 | Delete lines 47-53 |
| 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 an SAE Entity can refer to AP peers that perform SAE and proposes an updated definition. The current definition is
* 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), access point (AP) or a multi-link device  
(MLD)."

### Proposed Resolution:

**(12091)** REVISED. Delete lines 47-52. Note to Editor: This resolution to this CID is the same as CID 13161.

**(13161)** ACCEPTED. Note to Editor: The resolution to this CID is the same as CID 12091.

**(13162)** ACCEPTED. Note to Editor: In the cited definition, change “an entity that is a station (STA) or a multi-link device (MLD)” to “an entity that is a station (STA), access point (AP) or a multi-link device (MLD)."

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13163 | 12.4.1 | 335 | 29 | If you're going to refer to Entity-A and A-MAC you need to make sure all locations that currently refer to STA-A and STA-A-MAC (including any locations buried in non-searchable figures) are updated to use the new terminology | As it says in the comment |

### Discussion:

* The cited text is:

Text, letter

Description automatically generated

* The commenter did not bother to provide locations from Clause 12.4 where the changes were missing. After comparing REVme D1.0 vs P802.11be D2.0, the following locations need to be changed: Clause 12.4.4.2.2 at 3106.51 and 3107.5; and Clause 12.4.4.3.2 at 3112.6

### Proposed Resolution (13163):

REVISED. Based on analysis of the baseline, the updated entity terminology needs to be applied to the following locations relative to REVme D1.0:

Change “STA-A-MAC” to “A-MAC” and “STA-B-MAC” to “B-MAC” at the following locations:

Clause 12.4.4.2.2 at 3106.51 and 3107.5

Clause 12.4.4.3.2 at 3112.6

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13173 | 12.5 |  |  | The comments on the CCMP subclauses also apply to the GCMP subclauses | Make the changes proposed in 12.5.3 to the corresponding locations in 12.5.5 |

### Discussion:

* The comment is just stating that comments on the CCMP sub clauses apply to the GCMP sub-clauses. Presumably the commenter wants the task group to consider changes in both clauses for the comments on CCMP.
* There are neither proposed changes nor comments referred to in the Proposed Resolution.

### Proposed Resolution: (13173)

REJECTED. The commenter fails to provide insufficient detail on the changes to clause 12.5.3 that need to be applied in clause 12.5.5.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 12092 | 12.5.3.3.1 | 339 | 53 | How about individual addressed robust management frames and group addressed data frames for MLD? | Please clarify |
| 12093 | 12.5.3.3.4 | 341 | 2 | Does the "otherwise" case include individual addressed robust management frames and group addressed data frames for MLD? | Please clarify |
| 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:

Text

Description automatically generated

* 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.”

### Proposed Resolution: (12092, 12093, 12322)

REVISED. For MLO, the AAD and Nonce construction for both CCM and GCM for Management frame transmissions use the values of the header fields for the link that the frame is transmitted on. This is no different from non-MLO behavior. Group addressed frames on the uplink are transmitted as unicast data frames and on the downlink are transmitted by the affiliated AP, so no additional behavior needs to be described in this clause. Add a note to clarify MLO individually addressed management frame behavior for both CCMP and GCMP.

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.”

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

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

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13164 | 12.5.3.3.2 | 340 | 15 | "If the MPDU is to be transmitted by a STA that is affiliated with an MLD and PTK is the temporal key" -- the PTK is always a temporal key | Delete "and PTK is the temporal key" |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* Agree with the commenter that the PTK is the temporal key and “and PTK is the temporal key” is not required text in this context.
* Also, “STAs in the MLD” is ambiguous. It should be affiliated STAs and the PN space is managed at the MLD level.
* It would be better to change the cited sentence to:

“If the MPDU is to be transmitted by a STA that is affiliated with an MLD, a single PN space maintained by the MLD shall be used for all affiliated STAs.”

### Proposed Resolution: (13164)

REVISED. The commenter is correct in pointing out that PTK does not need to be mentioned in this context since the clause covers PN processing. Also “STAs in the MLD” is ambiguous.

At the cited location,

Chanage

“If the MPDU is to be transmitted by a STA that is affiliated with an MLD and PTK is the temporal key, the STAs in the MLD shall share a single PN space for all the links.”

to

“If the MPDU is to be transmitted by a STA that is affiliated with an MLD, a single PN space maintained by the MLD shall be used for all affiliated STAs.”

### Comment

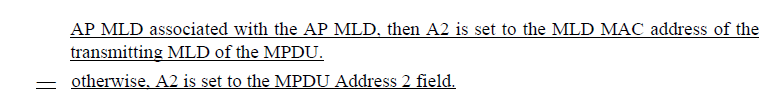
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13165 | 12.5.3.3.3 | 340 | 51 | "If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, " is not clear as to what the middle clause pertains to (first or last clause). Note a STA does not have direct access to a peer's MIB. Actually, the end of the sentence already constrains this to MLDs. Ditto at line 61 | Change the para to "If the To DS or From DS subfields in the MAC header of the MPDU are not both set to 0, and the MPDU is an individually addressed Data frame between an AP MLD and a non- AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver MLD of the MPDU." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated



* The proposed change for A1 at the cited location of the comment is:

At 340.52, change

“If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver MLD of the MPDU.”

to

“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 between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver.”

* The proposed change describes the value of A1 in relation to the receiver of the frame. Under ToDS and FromDS conditions, the frame could only be transmitted between MLDs, therefore the proposed change works.
* The proposed change for A2 would be:

At 340.61, change

“If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to the MLD MAC address of the transmitting MLD of the MPDU.”

to

“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 between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to the MLD MAC address of the transmitting MLD.”

### Proposed Resolution: (13165)

REVISED. Make the changes in line with the changes proposed by the commenter.

At 340.52, change

“If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver MLD of the MPDU.”

to

“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 between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver.”

At 340.61, change

“If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to the MLD MAC address of the transmitting MLD of the MPDU.”

to

“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 between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to the MLD MAC address of the transmitting MLD.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13166 | 12.5.3.3.3 | 341 | 5 | Missing articles in "MPDU Address 3 field is BSSID". Ditto at 341.17 | Change to "the MPDU Address 3 field is the BSSID" |
| 13167 | 12.5.3.3.3 | 341 | 9 | ", where the corresponding AP with the BSSID is affiliated with the AP MLD" is not clear. Ditto at line 20 | Delete the cited text |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* The proposed change for CID 13166 is editorial, adding “the” before “MPDU Address 3” and “BSSID”
* The proposed change for CID 13167 removes a phrase describing the BSSID which is extraneous for both A3 and A4 since in this case, the AP has to be affiliated with an AP MLD.

### Proposed Resolution: (13166, 13167)

CID 13166: ACCEPTED.

CID 13167: ACCEPTED. Note to editor. The changes are at 341.9 and 341.20

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13168 | 12.5.3.3.4 | 341 | 40 | Apparently we're not allowed to change field names | Do not add " Or MLD" |
| 13169 | 12.5.3.3.4 | 341 | 48 | "either To DS or From DS subfields in the MAC header of the MPDU are set to 1" is not clear or grammatical | Change to "the To DS or From DS subfields in the MAC header of the MPDU are not both set to 0" |

### Discussion:

* Cited text in context:

Graphical user interface, text, application

Description automatically generated

* For CID 13168, the commenter is correct. Field names are not modified once an 802.11 standard or amendment is published. The changes would be:

Delete “Or MLD “ at 341.40, 341.51, and 341.52.

* For CID 13169, the proposed wording is an improvement over the existing wording. The changes would be:

At cited location, change

“If dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed Data frame”

To

“If dot11MultiLinkActivated is true, the To DS or From DS subfields in the MAC header of the MPDU are not both set to 0, and the MPDU is an individually addressed Data frame”

### Proposed Resolution: (13168, 13169)

CID 13168: REVISED. Make the changes in the manner proposed by the commenter. Delete “Or MLD “ at 341.40, 341.51, and 341.52.

CID 13169: ACCEPTED.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13170 | 12.5.3.3.7 | 341 | 62 | "Each transmitter STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each MLD shall maintain a single PN (48-bit counter) for each PTKSA. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA. Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD." is confusing at best and self-contradictory at worse. An AP is also a STA, so the first sentence is saying no PN for APs of an MLD, but the third sentence is saying yes PN | Delete the third sentence |

### Discussion:

* The cited text in context is:Graphical user interface, text, application, email

  Description automatically generated
* The third sentence is “Each MLD shall maintain a single PN (48-bit counter) for each PTKSA.”
* For MLO, the MLD mantains the single PN for the PTKSA and the affiliated APs maintain the PN for the GTKSA. The cited text is clear and is required to describe MLO.

### Proposed Resolution: (13170)

REJECTED. The cited sentence and the following sentence describe the behavior for MLO and are both required. The PN for the PTKSA is maintained at the MLD level, and the PN for the GTKSA is maintained at the affiliated STA level.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 12371 | 12.5.3.3.7 | 342 | 1 | "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD." This sentence is not valid for the case of GTKSA, in which case the PNs are maintained by the affiliated APs. | Rephrase as: "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD (for PTKSA) or by the STA (for GTKSA)." |
| 12979 | 12.5.3.3.7 | 342 | 1 | Since "Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA", this PN has to be maintained by the MLD? | Fix the text in "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD" to be consistent with previous text and intention. |
| 12372 | 12.5.5.3.6 | 344 | 9 | "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD." This sentence is not valid for the case of GTKSA, in which case the PNs are maintained by the affiliated APs. | Rephrase as: "Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD (for PTKSA) or by the STA (for GTKSA)." |

### Discussion:

* Cited text in context (for clause 12.5.3):

Graphical user interface, text, application, email

Description automatically generated

* The proposed change for CID 13271 looks to be consistent with the baseline, however it would be good to remove the parenthesis around PTKSA and GTKSA. So the change would be:

At 342.1 and 344.9, change

“Each MLD shall maintain a single PN (48-bit counter) for each PTKSA. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA.”

To

“Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD for the PTKSA, or by the STA for GTKSA.”

### Proposed Resolution: (12371, 12979, 12372)

REVISED. At 342.1 and 344.9, change

“Each MLD shall maintain a single PN (48-bit counter) for each PTKSA. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA.”

to

“Each transmitter STA that is affiliated with an MLD shall use the PN (48-bit counter) that is maintained by the MLD for the PTKSA, or by the STA for GTKSA.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13171 | 12.5.3.4.1 | 342 | 38 | This para has the problems described in other comments on prior C12 subclauses | Change to "In addition, the To DS or From DS subfields in the MAC header of the MPDU are not both set to 0, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD to an AP affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see 12.5.3.3.3 (Construct AAD)) and nonce (see 12.5.3.3.4 (Construct CCM nonce)) values." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* Also note that similar text is included in the GCMP clause (344.47)

Text

Description automatically generated

* The proposed change is to replace:

“In addition, if dot11MultiLinkActivated is true, either or both To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to“

with

“In addition, 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 to an AP affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to “

* The new text removes the dependency on the dot11MultiLinkActivated MIB variable and is simpler to parse. However the proposed text does not cover both uplink and downlink frames transmitted between an AP MLD and a non-AP MLD. Input to the AAD needs to be applied foreither an uplink frame or a downlink frame.
* The change needs to be made at both the cited locations for both CCMP and GCMP.

### Proposed Resolution: (13171)

REVISED. Make the changes proposed by the commenter for both CCMP and GCMP. At 342.38 and 344.47, change:

“In addition, if dot11MultiLinkActivated is true, either or both To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to“

with

“In addition, 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, then the transmitter and receiver are set to the respective MLD MAC addresses and are passed to“

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13172 | 12.5.5.3.1 | 343 | 40 | "being set to known value" missing article | Change to "being set to a known value" |

### Discussion:

* Cited text in context:

Text

Description automatically generated with medium confidence

* The comment resolution proposes adding a missing article.

### Proposed Resolution: (13172)

ACCEPTED.

### 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):

Text, letter

Description automatically generated

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

Text

Description automatically generated

* 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 neeed 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.”

### 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 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 shall be set to the MLD MAC address of the transmitting MLD. 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 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 shall be set to the MLD MAC address of the transmitting MLD. 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.