IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe LB271 Security comment resolutions – Part 1 | | | | |
| Date: 2023-04-28 | | | | |
| 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 15068, 18019, 16368, 15194, 15067, 15142, 15179, 15180, 15181, 15188, 15191, 15192, 15193, 15179, 15195, 15196, 15197, 15512, 18283, 15198, 15148, 15149, 15199, 18062, 15150, 15025, 15151, 15152, 15200, 15201, 15136, 15153, 15154, 15137, 15202, 15203, 15206, 15207

Rev 0. Initial submission

Rev 1. Updates based on offline comments.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 15068 | 12.1 | 395.09 | Don't redefine STA | strike the "'STA' means that..." line. Define how such a thing works in an MLO, it''s an MLD or whatever and then use that term when needed. |

### Discussion:

* The cited text is:

Text

Description automatically generated

* The commenter does not believe the highlighted line above is necessary.
* Looking through the D3.0, I would agree with the commenter that there are few places where STA could be interpreted as affiliated STA. Uses of the term “affiliated STA” look to be clearly called out.

### Proposed Resolution: (15068)

ACCEPTED.

### 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. |
| 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, 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:

“The SA and DA for an MSDU containing an EAPOL PDU shall be set to the applicable Supplicant and Authenticator MLD MAC address.”

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”

### 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.

### Proposed Resolution: (15067, 15194)

REVISED. The term “SAE peer” is already used in the baseline and with a definition, includes STA and MLD peers. Replace “SAE entity” with “SAE peer” throughout the TGbe draft.

Locations are as follows:

At 61.1, change “(SAE) entity” to “(SAE) peer”

At 397.47, 397.56, 398.35, 398.38, 399.17, 399.19, 399.56, 400.8, 400.12, 400.28, 400.44, 400.50, 400.58, 401.6, 401.17, 401.18, 401.20, 401.23

### 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 and managing the MLD MAC address. The above requirements defined for a non-AP STA in selecting and managing its MAC address during association or establishing transaction state with an AP shall apply to the non-AP MLD in selecting and managing its MLD MAC address during association or establishing transaction state with an AP MLD.

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.

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 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** |
| 15179 | 12.3.3.1 | 395.40 | Incorrect editing instruction. No prior instruction shifts paragraphs within this subclause, so "Change the now-shifted third and fourth paragraphs as follows:" doesn't make sense here. | Change instruction to "Change the first and second paragraphs as follows:" |

### Discussion:

* Cited text in context:

Graphical user interface, text, application

Description automatically generated

* The baseline text shown in the TGbe draft is the first two paragraphs of the clause. Therefore the commenter is correct.

### Proposed Resolution: (15179)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15180 | 12.3.3.2.1 | 396.14 | "A STA or an MLD may decline ..., respectively" implies that an MLD may NOT decline to authticate with a STA that requsts authentication. | Remove ",respectively" |
| 15181 | 12.3.3.2.1 | 396.14 | If a STA (not an MLD) attempts to auth or associates with an MLD, it should be rejected by the MLD. Also MLD->STA should be rejected. | Add requirement for mismatched auth or assoc attempts to be rejected. |

### Discussion:

* Cited text in context:

Text, timeline

Description automatically generated

* CID 15180: Agree with the commenter. “respectively” is not needed in the cited sentence.
* CID 15181: Looking through the draft in clauses that describe 802.11 authentication, there was no explicit statement to indicate that an AP MLD shall reject an authentication request from a non-AP STA, and similarly, an AP shall reject an authentication request from a non-AP MLD. The location for this normative statement looks to be clause 12.3.3.2.3 prior to the last paragraph:

Timeline

Description automatically generated

### Proposed Resolution:

**(CID 15180):** ACCEPTED

**(CID 15181):** REVISED. Add a clarification to indicate that an MLD shall reject an authentication request from STA, and similarly, a STA shall reject an authentication request from an AP:

Relative to REVme D3.0at 2794.18, add the following paragraph:

“An AP MLD shall reject an authentication request from a non-AP STA with the Status Code field set to REQUEST\_DECLINED and an AP shall reject an authentication request from a non-AP MLD with the Status Code field set to REQUEST\_DECLINED.”

### Comment

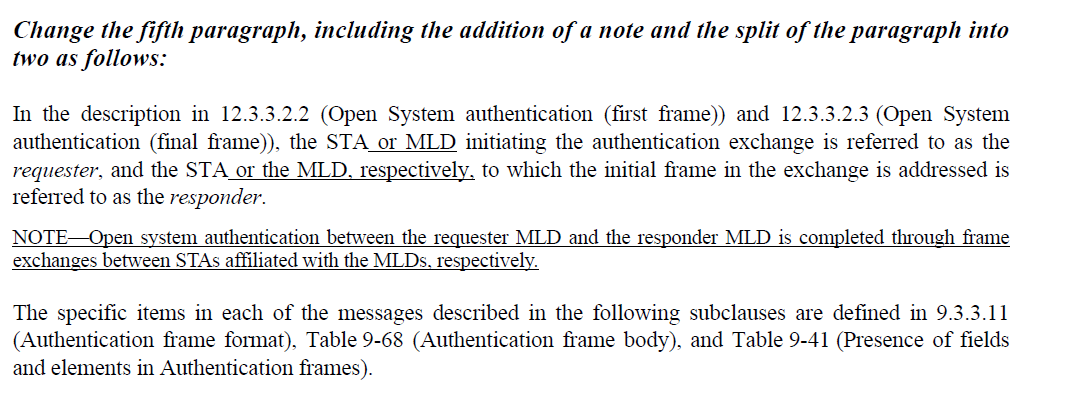
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15188 | 12.3.3.2.1 | 396.32 | How does a responder MLD/STA affiliated with the responder MLD know if an open system authentication request is from an MLD STA (so pertains to state maintained by the MLD), or from a non-MLD STA? | Clarify addressing/handling of auth requests using "frame exchanges between STAs affiliated with the MLDs." |

### Discussion:

* Cited text in context:

Graphical user interface, text, application

Description automatically generated



* The commenter is asking how Open System Authentication can be distinguished between a non-AP STA and an AP, and a non-AP MLD and AP MLD. The difference is that the MLD MAC Address is included in the frame body.
* Add a sentence to clarify that the MLD includes its MAC address in the authentication frame body. The note would then become:
* “NOTE—Open system authentication between the requester MLD and the responder MLD is completed through frame exchanges between STAs affiliated with the MLDs, respectively. The MLD includes its MLD MAC address in the frame body of the authentication frame.”

### Proposed Resolution: (15188)

REVISED. Modify the note to include a statement that the MLD MAC Address is included in the frame body.

At cited location, append the following sentence to the note:

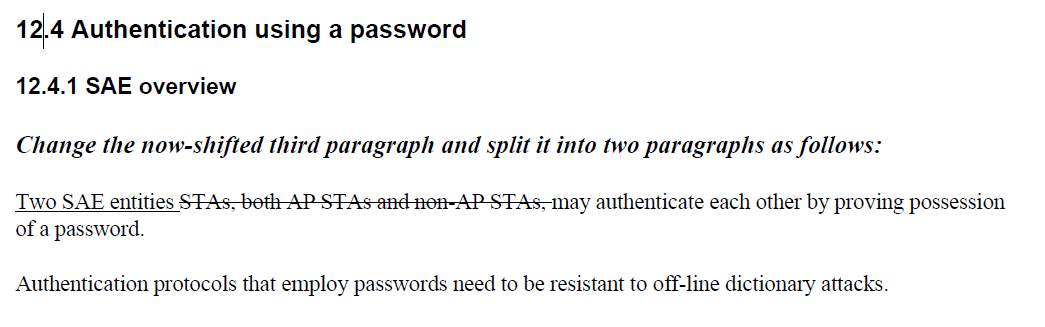
“The MLD includes its MLD MAC address in the MLD MAC Address field of the Multilink element, in the frame body of the Authentication frame.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15191 | 12.4.1 | 396.55 | Incorrect editing instruction. No prior instruction shifts paragraphs within this subclause, so "Change the now-shifted ..." doesn't make sense here. | Change instruction to "Change the first paragraph and split it into two paragraphs as follows:" |

### Discussion:

* Cited text in context:



* Agree with the commenter that the editing instruction is incorrect. The proposed editing instruction is correct.

### Proposed Resolution: (15191)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15192 | 12.4.1 | 397.01 | Incorrect editing instruction. Paragraph is now third. | Change instruction to "Change the now-shifted third paragraph as follows:" |
| 15193 | 12.4.1 | 397.27 | Incorrect editing instruction. Paragraph is now fifth. | Change instruction to "Change the now-shifted fifth paragraph as follows:" |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* With the paragraph break added in the first change in the clause, the commenter is correct in stating that the editing instructions are incorrect. The proposed editing instructions are correct.

### Proposed Resolution: (15192, 15193)

ACCEPTED

### 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

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

REVISED. Clarify the MAC address identities for the SAE. Note that CID 15194 and 15067 changed “SAE entity” to “SAE peer”

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

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 18018 | 12.4.6 | 401.25 | SAE Auth frames carry anti-clogging-token when the threshold is met for the SAE auth handling inside the AP. The spec says that the length of the anti-clogging-token, when it is not sent as part of the container Information Element, is derived from the total length of the Auth frame and the length of the scalar and FFE fields within the SAE-Auth frame.  The text from the rev-md spec "Since the Anti-Clogging Token field is of fixed size and the size of the peer-commit-scalar and PEERCOMMIT-ELEMENT are inferred from the finite cyclic group being used, it is straightforward to determine whether a received SAE Commit message includes an Anti-Clogging Token field or not."  This method of calculation will not work when ML-IE or any information element is included in the Auth frame | Mandate the use of the anti-clogging-token for EHT STAs. One option is to forbid AKM suite selector values 00-0F-AC:8 (SAE authentication) and the AKM suite selector value 00-0F-AC:9 (FT authentication over SAE for MLO association. |

### Discussion:

* Here is a description from the baseline on Anti-Clogging tokens: Text

  Description automatically generated
* Anti-clogging tokens were added to SAE authentication to mitigate DoS attacks on an AP. The comment asks to mandate them.
* The Anti-Clogging Token field is conditionally present at the beginning of the Authentication frame so the presence of elements at the end of the frame should not affect the parsing of the element.
* In Wi-Fi Protected Access Security Considerations, see <https://www.wi-fi.org/file/wi-fi-protected-access-security-considerations> there is an analysis of the effectiveness of anti-clogging tokens which concludes that anti-clogging tokens guard against rudimentary DoS attacks but not against more sophisticated attacks.
* As a result of this analysis, it does not make sense to mandate the use of anti-clogging tokens.
* Mandating hash-to-element for SAE would, to a certain extent, reduce the effect of DoS attacks. This could be mandated for EHT STAs.

### Proposed Resolution: (18018)

REJECTED. While anti-clogging tokens guard against rudimentary DoS attacks, they are not effective against more sophisticated attacks (see <https://www.wi-fi.org/file/wi-fi-protected-access-security-considerations>). With this analysis, there is no justification to mandate the use of anti-clogging tokens for EHT STAs.

***or***

REVISED. While anti-clogging tokens guard against rudimentary DoS attacks, they are not effective against more sophisticated attacks (see <https://www.wi-fi.org/file/wi-fi-protected-access-security-considerations>). Rather than make anti-clogging tokens, mandate hash-to-element negotiation between EHT STAs.

Modify 12.12.3 as follows

At 431.22, add the following paragraph to the clause

“When an EHT STA performs SAE authentication with a peer EHT STA, it shall set the SAE Hash-to-element field to 1 in the RSNXE and use the SAE hash-to-element method when SAE authentication is negotiated.”

### 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, the frame body of an MPDU is not encapsulated with a new PN when retransmitted on another link.”

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

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15198 | 12.5.2.3.2 | 403.07 | PN spaces are maintained per temporal key. APs affiliated with an MLD may send individually addressed frames to non-MLD STAs. | Change paragraph to: "If the individually addressed MPDU is to be transmitted by a STA that is affiliated with an MLD to a STA that is affiliated with an MLD, a single PN space for the PTKSA shall be maintained by the MLDs and shall be used for all affiliated STAs." |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* The commenter suggests changing the cited text to the following:

“If the individually addressed MPDU is to be transmitted by a STA that is affiliated with an MLD to a STA that is affiliated with an MLD, a single PN space for the PTKSA shall be maintained by the MLDs and shall be used for all affiliated STAs."

* It’s PN space that is associated with the MLD and the MPDU is transmitted through an affiliated STA. To make the behaviour clearer, it would be better to associate the MPDU with the MLD:

“If the individually addressed MPDU is to be transmitted by an MLD through an affiliated STA to a receiving STA that is affiliated with an MLD, a single PN space for the PTKSA shall be maintained by the MLDs and shall be used for all affiliated STAs."

* Note that the receiver MLD also needs an equivalent requirement.

### Proposed Resolution: (15198)

REVISED. Make the change in line with the Proposed Change, making it clear that the PN space is maintained between MLDs.

At the cited location, modify the cited text, changing:

”If the individually addressed 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.”

to

“If the individually addressed MPDU is to be transmitted by an MLD to a receiving MLD through an affiliated STA, a single PN space for the PTKSA shall be maintained for transmissions through all affiliated STAs."

To cover the receiver case, append the following to 12.5.2.4.4 as item g):

“For individually addressed MPDUs received by an affiliated STA from a transmitting MLD, the receiving MLD shall maintain a single set of replay counters for the PTKSA for all affiliated STAs."

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15148 | 12.5.2.3.3 | 403.42 | It is redundant to mention To DS and from DS. We only need to mention individually addressed data frame between AP MLD and non-AP MLD | Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and" |
| 15149 | 12.5.2.3.3 | 403.49 | It is redundant to mention To DS and from DS. We only need to mention individually addressed data frame between AP MLD and non-AP MLD | Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and" |
| 15199 | 12.5.2.3.2 | 403.54 | Superfluous punctuation. | Remove the extra "." |
| 18062 | 12.5.2.3.3 | 403.54 | Extra period | Remove extra period after "transmitting MLD." |
| 15150 | 12.5.2.3.3 | 403.57 | It is redundant to mention "dot11MultiLinkActivated is true". The following description alreadys says data frame between AP MLD and a non-AP MLD | Delete "dot11MultiLinkActivated is true, " |
| 15025 | 12.5.2.3.3 | 403.58 | "the MPDU Address 3 field is the BSSID" is referred to the baseline table 9-58, "the MPDU Address 3 field is Address field contents for Data frames transmitted by nonmesh STAs". Here, a reference to the table is required to know when the A3 is BSSID. | add a reference to the table 9-58 in the baseline |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* With all of the changes requested in the above comments, the resulting text becomes:

2)A1 – MPDU Address 1 field.A1 is set as follows:

—If 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.

—otherwise, Al is set to the MPDU Address 1 field.

3)A2 – MPDU Address 2 field.A2 is set as follows:

—If 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.

—otherwise, A2 is set to the MPDU Address 2 field.

4)A3 – MPDU Address 3 field.If the MPDU Address 3 field is the BSSID and is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then:

—A3 is set to the MLD MAC address of the AP MLD

—Otherwise, A3 is set to the MPDU Address 3 field.

**Commenter does not specify where the reference to Table 9-58 should go.**

* A3 is set to either the SA, DA, or BSSID according to Table 9-58. It should be the SA, the DA, or the MLD MAC address of the AP MLD, replacing the BSSID.

### Proposed Resolution: (15148, 15149, 15199, 18062, 15150)

ACCEPTED

**(15025)** REVISED. Clarify that for the purpose of constructing the AAD, the A3 field is set to the AP MLD MAC address rather than the BSSID in cases where A3 is set to the BSSID.

At 401.57, change

“is the BSSID”

to

“is the BSSID (see Table 9-58).”

Also clean-up the style to match the baseline:

At 403.42, 403.49, and 404.6, change

“is set as follows” to “is determined as follows”

At 403.45, 403.48, 403.53, 403.55, 403.61, 403.63, 404.8, and 404.9, change

“is set to” to “is”

At 403.48, 403.56, and 404.9, change

“otherwise” to “Otherwise”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15151 | 12.5.2.3.3 | 404.04 | It is redundant to mention "dot11MultiLinkActivated is true". The following description alreadys says data frame between AP MLD and a non-AP MLD | Delete "dot11MultiLinkActivated is true, " |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* Agree with the commenter that the cited text is redundant.

### Proposed Resolution: (15151)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15152 | 12.5.2.3.4 | 404.26 | It is redundant to mention To DS and from DS. We only need to mention individually addressed data frame between AP MLD and non-AP MLD | Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and" |
| 15200 | 12.5.2.4.1 | 404.62 | Decapsulation processing should be conditionalized on both tx and rx being MLDs, and should be consistent with the encapsulation processing. | Change "transmitted by a STA affiliated with an MLD" to "between an AP MLD and a non- AP MLD associated with the AP MLD" |

### Discussion:

* Cited text in context:

Graphical user interface, text, application

Description automatically generated



* The proposed change for CID 15152 looks good. However a similar change should be made at 404.59
* The proposed change for CID 15200 looks better than the original text, but should indicate that the frames are transmitted between affiliated STA and AP.

### Proposed Resolution:

**(15152)** REVISED. Make the proposed change at the cited location and also modify similar text in clause 12.5.2.4.1 at 404.59.

At 404.26, delete “the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and”

At 404.59, delete “the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and”

**(15200)** REVISED. Make changes in line with those proposed by the commenter noting that the frames are transmitted between affiliated STA and affiliated AP

At 404.61, change

“an individually addressed Data frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD”

to

“an individually addressed Data frame transmitted between an AP MLD and a non-

AP MLD associated with the AP MLD over a setup link between an affiliated AP and affiliated STA, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD”

### Comment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15201 | 12.5.2.4.4 | 405.36 | Decapsulation processing should be conditionalized on both tx and rx being MLDs. | Change "transmitted by a STA affiliated with an MLD" to "between an AP MLD and a non- AP MLD associated with the AP MLD" |
| 15136 | 12.5.2.4.4 | 405.45 | We need similar sentence for management frame as well because management frame replay is also not based on TA. | Add the following at the end of bullet (d). "For MLO, if the receiver set the MFPC bit of any affiliated STA 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 transmitter MLD MAC address of that individually addressed Management frame." |

### Discussion:

* Cited text in context:

A picture containing text

Description automatically generated

* For CID 15201, the commenter is trying to suggest a modification to the text to indicate that the frames are exchanged between MLDs and transmitted through affiliated STAs. The commenter suggests:

“transmitted by a STA affiliated with an MLD" to "between an AP MLD and a non-

AP MLD associated with the AP MLD”

* The updated baseline text expands TA, RA, and priority value.
* It would be better to clarify that the frame is transmitted through an affiliated STA, that is, to modify the text to read:

“transmitted between an AP MLD and a non-AP MLD associated with the AP MLD through an affiliated STA”

* For CID 15136, the commenter is asking for text to be added to clarify processing of management frames for MLO. The commenter proposes adding the following:

“For MLO, if the receiver set the MFPC bit of any affiliated STA 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 transmitter MLD MAC address of that individually addressed Management frame."

* However, the baseline on REVme D3.0 with respect to this case was updated to

“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(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame.”

* It’s not good enough that the MFPC bit is set, MFP needs to be negotiated on the link. Also, it would be good to separate the MFPC case into a separate paragraph and then incorporate the proposed text. So the text would become:

“<PAR> If MFP is negotiated for a given link, the receiver 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(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame. For MLO, if MFP is negotiated for a given link, the MLD 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 transmitter MLD MAC address of that individually addressed Management frame, (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI.”

### Proposed Resolution:

**(15201)** REVISED. Make the changes in line with the Proposed Change, clarifying that the frame is transmitted through an affiliated STA.

Change

“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."

to

“transmitted between an AP MLD and a non-AP MLD associated with the AP MLD through an affiliated STA, 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, receiver MLD MAC address (individual or group address), and priority value of the received MPDU.”

**(15136)** REVISED. Make the changes in line with the Proposed Change and align the proposed text with the updated 802.11 baseline.

Add a paragraph break at the beginning of the sentence on p405.41

Change

“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.”

to

“If MFP is negotiated for a given link, the receiver 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(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame. For MLO, if MFP is negotiated for a given link, the MLD 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 transmitter MLD MAC address, and (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15153 | 12.5.4.3.4 | 406.58 | It is redundant to mention To DS and from DS. We only need to mention individually addressed data frame between AP MLD and non-AP MLD | Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and" |

### Discussion:

* Cited text in context:

Graphical user interface, text, application

Description automatically generated

* The condition is with the “and” condition in the same sentence.

### Proposed Resolution: (15153)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15154 | 12.5.4.4.1 | 407.46 | Revise the texts to say between AP MLD and non AP MLD rather than using To DS and from DS description. We only need to mention individually addressed data frame between AP MLD and non-AP MLD | Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and" Change "the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD" to "the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD" |

### Discussion:

* Cited text in context:

Timeline

Description automatically generated with medium confidence

* The Proposed Change removes the redundant condition and clarifies that the frame is transmitted between the non-AP MLD and AP MLD. The resulting text would be:

“In addition, if the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see 12.5.5.3.3 (Construct AAD)) and nonce (see 12.5.4.3.4 (Construct GCM nonce)) values.”

* “In addition,” is not needed in this case

### Proposed Resolution: (15154)

REVISED. Make the changes in line with the proposed change:

Delete “In addition,”

Delete "the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and"

Change

"the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD"

to

"The MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD"

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15137 | 12.5.4.4.4 | 408.12 | We need similar sentence for management frame as well because management frame replay is also not based on TA. | For MLO, if the receiver set the MFPC bit of any affiliated STA 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 transmitter MLD MAC address of that individually addressed Management frame. |
| 15202 | 12.5.4.4.4 | 408.03 | Decapsulation processing should be conditionalized on both tx and rx being MLDs. | Change "transmitted by a STA affiliated with an MLD" to "between an AP MLD and a non- AP MLD associated with the AP MLD" |

### Discussion:

* Cited text is in the clause describing PN and replay detection for GCMP:

Text

Description automatically generated

* These are similar comments to CID 15201 and 15136. Propose similar resolutions to these comments.
* The updated baseline is as follows:

### Proposed Resolution:

**(15202)** REVISED. Make the changes in line with the Proposed Change, clarifying that the frame is transmitted through an affiliated STA.

Change

“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."

to

“transmitted between an AP MLD and a non-AP MLD associated with the AP MLD through an affiliated STA, 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, receiver MLD MAC address (individual or group address), and priority value of the received MPDU.”

**(15137)** REVISED. Make the changes in line with the Proposed Change and align the proposed text with the updated 802.11 baseline.

Add a paragraph break at the beginning of the sentence on p408.3

Change

“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.”

to

“If MFP is negotiated for the link, the receiver 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(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame. For MLO, if MFP is negotiated for a given link, the MLD 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 transmitter MLD MAC address, and (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15203 | 12.6.1.1.8 | 409.40 | An AP that has both MLD STAs and non-MLD STAs associated must use the same GTKSA for broadcast traffic to all stations. "one GTKSA used exclusively for encrypting group addressed MPDUs that are transmitted by the affiliated AP operating on the link and for decrypting group addressed transmissions that are received by the affiliated non-AP STA operating on the link" implies that this GTKSA is not also used by non-AP non-MLD STAS. | Add "An AP affiliated with an MLD that has both MLD-affiliated non-AP STAs and non-MLD non-AP STAs associated uses the same GTKSA for encrypting group addressed MPDUs they they can be decrypted by all associated non-AP STAs." |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* It makes sense to clarify this behavior, however the inserted sentence could be worded as follows:

“An AP affiliated with an AP MLD uses the same GTKSA to encrypt group addressed MPDUs for both STAs affiliated with an associated non-AP MLD and associated non-AP STAs."

### Proposed Resolution: (15203)

REVISED. Make changes in line with the Proposed Change by the commenter.

At 409.46 insert the following sentence:

“An AP affiliated with an AP MLD uses the same GTKSA to encrypt group addressed MPDUs for STAs affiliated with an associated non-AP MLD and for associated non-AP STAs."

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15206 | 12.6.1.1.8 | 409.49 | MLD case for GTKSA not considered in "The GTKSA is created by the Authenticator's SME ...", whereas the corresponding text for IGTKSA was updated. The two cases should be handled in a similar fashion. | Update to match IGTKSA text. |
| 15207 | 12.6.1.1.8 | 409.57 | If an AP affiliated with an MLD has both MLD and non-MLD STAs associated, the GTKSA for non-MLD STAs will be identified by the AP MLD MAC address (the Authenticator), whereas the GTKSA (for the same GTK) will be identified by the MAC address of the AP operating on the link, which means the SME will have two GTKSAs for the same GTK. | Change "-- For non-MLO, Authenticator MAC address. For MLO, the MAC address of the AP operating on the link corresponding to the GTKSA" to "-- Authenticator MAC address. -- If dot11MultiLinkActivated is true, the MAC address of the AP operating on the link corresponding to the GTKSA." (i.e. retain the auth mac address, and add an additional item if MLO is enabled) |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* In 15206, the commenter is referring to the following text for the IGTKSA:

“An AP MLD’s SME creates an IGTKSA for each of its links when it establishes or changes the IGTK with all non-AP STAs that operate on the link and are affiliated with the non-AP MLDs to which it has a valid PTKSA”

* It makes sense to add equivalent text in the GTKSA clause
* For 15207, the commenter is asking that the “Authenticator MAC Address” in the GTKSA does not have an “non-MLO” qualifier. For an MLD, the Authenticator MAC address of the AP MLD is used to perform the GTK handshake so it does provide a role.

### Proposed Resolution:

**(15206)** REVISED. Make changes to the GTKSA text to match the IGTKSA text:

At 409.45, change:

“The GTKSA is created by the Authenticator’s SME when the SME changes the GTK and has sent the GTK to all STAs with which it has a PTKSA. It has the same lifetime as the BSS, unless superseded. A GTKSA consists of the following:”

To

“The GTKSA is created by the Authenticator’s SME when the SME changes the GTK and has sent the GTK to all STAs with which it has a PTKSA. It has the same lifetime as the BSS, unless superseded. An AP MLD’s SME creates an GTKSA for each of its links when it establishes or changes the GTK with all non-AP STAs that operate on the link and are affiliated with the non-AP MLDs to which it has a valid PTKSA. A GTKSA has the same lifetime as the BSS, unless superseded. A GTKSA consists of the following:”

**(15207)** ACCEPTED