IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe LB266 Comment resolutions for RSNA and Keying |
| Date: 2022-09-07 |
| 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 12.6 and 12.7 of P802.11be D2.0. The resolutions will be shown relative to D2.0.

CIDs 13179, 13182, 13183, 13184, 10294, 10293, 13185, 11086, 13186, 13187, 13189, 13190, 14100, 13191, 12097, 13192, 11071, 12098, 13194, 10678, 12099, 13195, 12100, 10679, 12101, 13196, 13197, 12102, 14094, 12103, 12104, 13198, 13199, 13200, 13201, 13202, 10593

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13179 | 12.6.2 | 347 | 49 | "All APs affiliated with an AP MLD shall advertise the same RSNE and RSNXE if included" needs a comma | Change to "All APs affiliated with an AP MLD shall advertise the same RSNE, and RSNXE if included" |

### Discussion:

* The location of the cited phrases is here:



* The proposed change adds a comma between “RSNE” and “and”.

### Proposed Resolution: (13179)

ACCEPTED

###  Comments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13182 | 12.6.3.1 | 348 | 12 | "its (Re)Association Request" missing "frame" | Append " frame" |
| 13183 | 12.6.3.1 | 348 | 17 | "For MLO, there shall be only one RSNE and RSNXE inserted into the(Re)Association Request frame initiated by the non-AP MLD." -- isn't this already the case for non-MLO? Also, this suggests an RSNXE is mandatory but I'm not sure it is, per "if included" elsewhere | Do not insert this sentence |
| 13184 | 12.6.3.1 | 348 | 23 | "A non-AP MLD would determine the appropriate AKM suite selector and pairwisecipher suite selector during MLO discovery by monitoring Beacon frames transmitted by APs affiliated withthe AP MLD or performing basic probing with each AP affiliated with the AP MLD or by performing MLprobing with one or more APs affiliated with the AP MLD." -- this hypothetical language is very odd indeed. And what is "basic probing"?! | Change to "A non-AP MLD determines the appropriate AKM suite selector and pairwisecipher suite selector during MLO discovery by passively or actively scanning for APs affiliated withthe AP MLD or by performing MLprobing with one or more APs affiliated with the AP MLD." |
| 10294 | 12.6.3.1 | 348 | 26 | There is no basic probing. | At cited location, change ""basic probing" to "passive or active scanning" |
| 10293 | 12.6.3.1 | 348 | 27 | There is no such thing as ML probing | At cited location, change "ML probing" to "an exchange of Multi-Link Probe Request and Multi-Link Probe Response frames" |

### Discussion:

* The cited text is:



* CID 13182 correctly points out that in the first line, (Re)Association Request is missing frame.
* CID 13183 requests that the last sentence of the paragraph be removed since the behavior is no different from the baseline. However, the advertisement of the RSNE and RSNXE, if present, is done per link rather than for the MLD, so it would be beneficial to combine the last sentence of the first paragraph with the first sentence of the second paragraph. So the change would be:

At 348.17, delete “For MLO, there shall be only one RSNE and RSNXE inserted into the (Re)Association Request frame initiated by the non-AP MLD.”

At 348.20, replace “For MLO, the initiating non-AP MLD’s RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD.”

With

“For MLO, the initiating non-AP MLD shall include only one RSNE, and RSNXE if present, in the (Re)Association Request frame. The RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD.”

* CIDs 13184, 10293, and 10294 comment on the same sentence. Incorporating all comment suggestions results in the following change:

At 348.23, replace

“A non-AP MLD would determine the appropriate AKM suite selector and pairwise cipher suite selector during MLO discovery by monitoring Beacon frames transmitted by APs affiliated with the AP MLD or performing basic probing with each AP affiliated with the AP MLD or by performing ML probing with one or more APs affiliated with the AP MLD.”

with

“A non-AP MLD determines the appropriate AKM suite selector and pairwise

cipher suite selector during MLO discovery by passively or actively scanning for APs affiliated with the AP MLD or by an exchange of Multi-Link Probe Request and Multi-Link Probe Response frames with one or more APs affiliated with the AP MLD.”

### Proposed Resolution:

**(13182)** ACCEPTED.

**(13183)** REVISED. For MLO, the non-AP MLD selects the contents of the RSNE by information discovered from affiliated APs.

At 348.17, delete “For MLO, there shall be only one RSNE and RSNXE inserted into the (Re)Association Request frame initiated by the non-AP MLD.”

At 348.20, replace “For MLO, the initiating non-AP MLD’s RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD.”

With

“For MLO, the initiating non-AP MLD shall include only one RSNE, and RSNXE if present, in the (Re)Association Request frame. The RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD.”

**(10293, 10294)** ACCEPTED. Note to Editor: the proposed changes are given in the resolution to CID 13184.

**(13184)** REVISED. Update the text in the direction suggested by the commenter.

At 348.23, replace

“A non-AP MLD would determine the appropriate AKM suite selector and pairwise cipher suite selector during MLO discovery by monitoring Beacon frames transmitted by APs affiliated with the AP MLD or performing basic probing with each AP affiliated with the AP MLD or by performing ML probing with one or more APs affiliated with the AP MLD.”

with

“A non-AP MLD determines the appropriate AKM suite selector and pairwise

cipher suite selector during MLO discovery by passively or actively scanning for APs affiliated with the AP MLD or by an exchange of Multi-Link Probe Request and Multi-Link Probe Response frames with one or more APs affiliated with the AP MLD.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 11086 | 12.6.3.2 | 348 | 48 | We should provide a table for the counterpart of Table 12-5--Robust management frame selection in an infrastructure BSS for MLD. The reason is that APs affiliated with the AP MLD may have different value of MFPR based on the following texts "All APs affiliated with an AP MLD shall advertise the same RSNE and RSNXE if included, with theexception of the AKM Suite List field and the MFPR subfield of the RSN Capabilities field. All APs affiliated with an AP MLD shall advertise at least one common AKM suite selector in the AKM Suite List field.". We can assume APs affilaited with AP MLD will have MFPC equal to 1 due to mandatory support of beacon protection and all non-AP STAs affiliated with the non-AP MLD will have the same MFPC or MFPR bit setting. | It is hard to describe the whole table, so the commenter will only describe the key texts. The only ambiguous setting is when MFPC and MFPR of non-AP STAs affiliated with the non-AP MLD to be 0 and 0. In that case, it is possible some APs affiliated with the MLD will have MFPC and MFPR equal to 1 and 0 or 1 and 1. Clarify by saying the following: "A requested link maybe accepted during multi-link setup if the MFPC and MFPR of the non-AP MLD is set to 0 and 0, and the MFPC and MFPR of the corresponding AP of the requested link is set to 1 and 0. A requested link shall be rejected with the Status CodeROBUST\_MANAGEMENT\_POLICY\_VIOLATION during multi-link setup if the MFPC and MFPR of the non-AP MLD is set to 0 and 0, and the MFPC and MFPR of the corresponding AP of the requested link is set to 1 and 1. MFP is enabled after MLD assocaition in each setup link if the MFPC of the non-AP MLD is set to 1. Note - All APs affilaited with an AP MLD have MFPC set to 1." |
| 13186 | 12.6.3.2 | 348 | 51 | "if itchooses to accept the association as a secure association" -- what does this mean? | Change to "if it chooses to accept the request" |

### Discussion:

* Cited text is the following:



* CID 13186 proposes changing “if it chooses to accept the association as a secure association” to “if it chooses to accept the request”. The frame being processed is a (re)association request, so the proposed text is more consistent with the baseline.
* CID 11086 seems to be referring to Table 12-5, which is given here from REVme D1.3:



* In CID 11086, the comment states: “We can assume APs affilaited with AP MLD will have MFPC equal to 1 due to mandatory support of beacon protection and all non-AP STAs affiliated with the non-AP MLD will have the same MFPC or MFPR bit setting.”
* The non-AP MLD provides a single RSNE/RSNXE in the association request. The AP MLD can advertise a different MFPR per link.
* Therefore, the best way to address this issue is for the AP MLD to evaluate the MFPR/MFPC settings in the RSNE provided by the non-AP MLD against each MFPR/MFPC setting for each link. The AP MLD could then use table 12-5 to accept or reject the link.
* The paragraph can be modified as follows:

“If an AP MLD Authenticator receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall

* + use the AKM suite and pairwise cipher suite in the (Re)Association Request frame to establish an RSNA with a non-AP MLD.
	+ compare the values of the MFPC and MFPR bits in the in the (Re)Association Request frame with the MFPC and MFPR bits in the requested links and use Table 12-5 to determine the links that can be accepted.

The AP MLD manages the PTKSA while the affiliated APs manage the GTKSA.”

### Proposed Resolution:

**(13186)** ACCEPTED. Note to Editor. The text change is included in the resolution to CID 11086.

**(11086)** REVISED. Incorporate the changes in <this> document under “Proposed Resolution: (11086)”

***Modify the cited paragraph at 348.51 as follows:***

“If an AP MLD Authenticator receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall

* + use the AKM suite and pairwise cipher suite in the (Re)Association Request frame to establish an RSNA with a non-AP MLD.
	+ compare the values of the MFPC and MFPR bits in the in the (Re)Association Request frame with the MFPC and MFPR bits in the advertised by each affiliated AP for each requested link, and use Table 12-5 to determine the links that can be accepted.

The AP MLD manages the PTKSA while the affiliated APs manage the GTKSA.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13187 | 12.6.10.2 | 349 | 10 | Odd verb tenses again | Change last 2 sentences to "The AP MLD Authenticator receives EAPOL-Start frames via theDS and initiates IEEE 802.1X authentication with the non-AP MLD via the DS. The DS forwards themessages between the non-AP MLD and AP MLD." |

### Discussion:

* Cited text is the following:



* The comment just proposes updating the tense of the last two sentences.

### Proposed Resolution: (13187)

ACCEPTED

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13189 | 12.7.1.1 | 350 | 25 | This para is not clear. Is it trying to say that an MLD is required to support encryption? Also line 27 is missing "pair" after the ">" | As it says in the comment |

### Discussion:

* The cited text is:

###

* The paragraph follows this text in the baseline:

“An RSNA STA shall support at least one pairwise key for any <TA,RA> pair for use with enhanced data cryptographic encapsulation mechanisms. The <TA,RA> identifies the pairwise key, which does not correspond to any WEP key identifier.”

* The cited text is consistent with the baseline and does mandate that the MLD peers support at least one pairwise key for cryptographic encapsulation.
* Agree with the commenter that “pair” is missing on line 27.

### Proposed Resolution (13189):

REVISED. The inserted paragraph is consistent with the baseline text and mandates that the MLD peers support at least one pairwise key for cryptographic encapsulation.

At 350.27, change “<transmitter\_MLD MAC address, receiver\_MLD MAC address> identifies” to “<transmitter\_MLD MAC address, receiver\_MLD MAC address> pair identifies”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13190 | 12.7.2 | 350 | 53 | "For MLO,the Key Data field may include one MLO GTK KDE, one MLO IGTK KDE, and one MLO BIGTKKDE for each of the setup links and shall be encrypted." is not clear. It seems to suggest no group keys might be present | Change to "For MLO,the Key Data field shall, for each of the setup links, contain one MLO GTK KDE, one MLO IGTK KDE (where appropriate), and one MLO BIGTKKDE (where appropriate), and shall be encrypted." |

### Discussion:

* The cited text is:



* The commenter is suggesting that the wording of the cited sentence starting with “For MLO,” be reworded as:

“For MLO, the Key Data field shall, for each of the setup links, contain one MLO GTK KDE, one MLO IGTK KDE (where appropriate), and one MLO BIGTK KDE (where appropriate), and shall be encrypted."

* Agree with the commenter that the proposed change is better wording. However this is the group key handshake, which may not contain group keys for every link. So the wording could be changed to:

“For MLO, the Key Data field shall, for each of the setup links updated by the group key handshake, contain one MLO GTK KDE, one MLO IGTK KDE (where appropriate), and one MLO BIGTK KDE (where appropriate), and shall be encrypted."

### Proposed Resolution (13190):

REVISED. Agree with the commenter on the improved wording, but group keys for all setup links are not necessarily updated in each group key handshake.

At cited location, change:

“For MLO,the Key Data field may include one MLO GTK KDE, one MLO IGTK KDE, and one MLO BIGTK KDE for each of the setup links and shall be encrypted.”

to

“For MLO, the Key Data field shall, for each of the setup links updated by the group key handshake, contain one MLO GTK KDE, one MLO IGTK KDE (where appropriate), and one MLO BIGTK KDE (where appropriate), and shall be encrypted."

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 11071 | 12.7.6.1 | 355 | 45 | The description implies that OCI KDE can be used for MLO. However, OCI KDE needs to be redesigned to include link ID and information for 320 MHz verification because 320 MHz may have 320 MHz-1 or 320 MHz-2. | Define MLO OCI KDE. Ideally, follow the format of OCI KDE to include link ID and change "Frequency Segment 1Channel Number" to simply "Channel center frequeny of 320 MHz", which is set to channel center frequency of 320 MHz when 320 MHz is used and 0 otherwise. |
| 10678 | 12.7.6.3 | 358 | 46 | For MLO, OCI verification should occur on all the links. Will need to make sure OCI works correctly for MLO. e.g., we should include the OCI KDE for each requested link in msg 2 for the AP MLD to verify the operating channels of the STAs corresponding to the requested links | As in the comment |
| 10679 | 12.7.6.4 | 361 | 11 | For MLO, OCI verification should occur on all the links. Will need to make sure OCI works correctly for MLO. e.g., we should include the OCI KDE for each requested link in msg 3 for the non-AP MLD to verify the operating channels of the APs corresponding to the requested links | As in the comment |
| 14100 | 12.7.2 | 351 | 5 | OCI KDE should have a corresponding MLO KDE defined because RNR in ML probe response is not protected | As in comment |

### Discussion:

* The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.
* The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.
* In addition to the baseline, operating channel validation is defined and explained in <https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx>
* OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.
* ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.
* Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.

### Proposed Resolution: (14100, 11071, 10678, 10679)

REJECTED. Operating channel validation, which leverages the OCI element, protects a security exchange between two STAs. Given that security exchanges in MLO occur on a single link, operating channel validation as specified in the baseline should work for peer MLDs. For more information on operating channel validation, see <https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx>. Also note that the OC and CN for 320 MHz channels are specified in Annex E of REVme D1.3.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13191 | 12.7.2 | 351 | 27 | What does "Length" refer to? Ditto at 351.47, 353.22 | Just change the length to "variable" |

### Discussion:

* The cited text is:



* The comment refers to the “Length” under the GTK.
* A recent approved comment in REVme changed length expressions for KDEs throughout the baseline to “variable”.
* The proposed resolution is consistent with REVme D1.0

### Proposed Resolution: (13191)

ACCEPTED.

Note to editor. The formula below the GTK field in the figure is changed to “variable”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13192 | 12.7.4 | 354 | 52 | "MAC Address is the MLD MAC address of the MLD" is very confusing | Rename to "MLD MAC Address" |

### Discussion:

* The cited text is:



* This comment was considered in the initial comment collection.
* The MAC Address KDE is already specified in the baseline (see REVme D1.0 at 3208.49) so defining a new KDE for the MLD MAC Address is not required.

### Proposed Resolution: (13192)

REJECTED. The MAC Address KDE is already specified in REVme D1.0 (see 3208.49) and the KDE can be used to carry the MLD MAC Address.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13194 | 12.7.6.1 | 356 | 52 | "exchange of successful (Re)Association Request/Response frame" should be plural | Change to "exchange of successful (Re)Association Request/Response frames" |

### Discussion:

* The cited text is:



* The commenter is correct.

### Proposed Resolution: (13192)

ACCEPTED

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 12098 | 12.7.6.1 | 355 | 56 | In message 3, the number of MLO Link KDE could be different from the number of MLO GTK KDE. | Change the number of MLD Link KDE from "n" to "m" |

### Discussion:

* The cited text is:



* The commenter is correct in the MLO Link KDE could have a different number of instances than the GTK KDEs. Using a different subscript would be clearer.
* Also a similar change is required for the clause 13,
	+ In the FT initial mobility domain association MLO\_Link subscript can differ from the MLO group key KDEs, so it should have a subscript of m (at 372.17). as well.

### Proposed Resolution: (13192)

REVISED. At 355.55 and 355.56, change the subscript for MLO Link from “n” to “m”. At 372.17, change the subscript for the MLO\_Link KDE from “n” to “m”.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 12097 | 12.7.2 | 352 | 13 | Does it imply for MLO the non-AP MLD may not include requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame? | Please clarify |
| 12099 | 12.7.6.3 | 358 | 53 | Does it mean for MLO, it may request only one link? | Remove "when more than one link is requested," |
| 12100 | 12.7.6.3 | 359 | 23 | Change "requested link(s)" to "requested links" | As commented |
| 13195 | 12.7.6.3 | 358 | 55 | "in (Re)Association Request frame" missing article | Change to "in the (Re)Association Request frame" |

### Discussion:

* CIDs 12097, 12099, and 12100 are related.
* The cited text in 12.7.2 is in the second paragraph



* The cited text for CID 12099 and CID 13195 in 12.7.6.3 in the description of Key Data contents for Message 2 of the 4-way handshake is:



* The cited text for CID 12100 in 12.7.6.3, which deals with the validation of the message 2 key data is:



* The requirements describe the behaviour where if the non-AP MLD supplicant is requesting more than one link, it includes the additional links in the MLO Link KDE in message 2 of the 4-way handshake. The AP MLD authenticator validates the information in the MLO Link KDE against the information provided in the (Re-)Association Request frame sent by the non-AP MLD.
* For CID 12097, it would be better to replace

“For MLO, if the non-AP MLD includes requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame, the non-AP MLD shall include a MLO Link KDE containing the LinkID field and affiliated STA MAC address for each link included by the non-AP MLD in the Multi-Link element in the (Re)Association Request frame”

With

“For MLO when more than one link is requested by the non-AP MLD in the (Re)Association Request frame, it shall include an MLO Link KDE containing the LinkID field and affiliated STA MAC address corresponding to each link included in the Multi-Link element.”

* For CID 12099, the MLO Link KDE is only included when the non-AP MLD is requesting more than one link.
* For CID 12100, the term “requested link(s)” could be single or plural because the Basic Multi-Link element could include the information of one or more links.
* For CID 13195, there is an article missing.

### Proposed Resolution:

**(12097)** REVISED. The non-AP MLD only includes the Multi-Link element when it requests more than one link. The cited text has been changed to clarify that requirement:

At 352.13, change

“For MLO, if the non-AP MLD includes requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame, the non-AP MLD shall include a MLO Link KDE containing the LinkID field and affiliated STA MAC address for each link included by the non-AP MLD in the Multi-Link element in the (Re)Association Request frame”

to

“For MLO when more than one link is requested by the non-AP MLD in the (Re)Association Request frame, it shall include an MLO Link KDE containing the LinkID field and affiliated STA MAC address corresponding to each link included in the Multi-Link element.”

**(12099)** REJECTED. The non-AP MLD may only include a single requested link. The 4-way handshake is taking place on that link so there is no need to include a Multi-Link element since the non-AP MLD is operating on the requested link.

**(12100)** REJECTED. At the cited location, requested links refers to the link information included in the “Basic Multi-Link element” and the “MLO Link KDEs”. The number of links that could be included are 1 or more, so “(s)” is appropriate.

**(13195)** ACCEPTED

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13196 | 12.7.6.4 | 361 | 19 | "for each affiliated AP that was sent by the Authenticator" -- an Authenticator does not send APs | Delete "that was sent by the Authenticator" |
| 12101 | 12.7.6.4 | 361 | 14 | For MLO, there is no Beacon for MLD, so what is "the RSNXE that the Authenticator sent in its Beacon or Probe Response frame"? | Change to "The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent, or; For MLO, a MLO Link KDE containing the LinkID field, the affiliated AP MAC address, RSNE, and RSNXE (if present) for each affiliated AP that was sent by the Authenticator" |

### Discussion:

* The cited paragraph is:



* For CID 12101, the commenter is citing the third last bullet which refers to the baseline behavior for the Authenticator. Throughout clause 12, the TGbe draft designates MLO behavior, where applicable with the qualifier “For MLO,”, and it’s clear between the third bullet and the 5th bullet what the non-MLO and MLO behaviour is. The cited bullet in the baseline makes reference to the RSNXE, so the proposed text is confusing.
* For CID 13196, the commenter points out that APs are not “sent by an authenticator”, which is correct. Also the RSNE and RSNXE are present in Beacon and Probe Response frames sent by each affiliated AP.
* It would be better to change the last bullet to the following:

“For MLO, a MLO Link KDE containing the LinkID field, the affiliated AP MAC address, the RSNE, and RSNXE (if present) sent in Beacon and Probe Response frames by each affiliated AP.”

### Proposed Resolution: (12101, 13196)

REVISED. As the commenter points out in the comment, for MLO the Authenticator does not transmit Beacons and Probe Response frames. It would be good to clarify that the information is transmitted by affiliated APs in Beacon and Probe Response frames.

At 361.18, change

“For MLO, a MLO Link KDE containing the LinkID field, the affiliated AP MAC address, RSNE, and RSNXE (if present) for each affiliated AP that was sent by the Authenticator.”

to

“For MLO, a MLO Link KDE containing the LinkID field, the affiliated AP MAC address, and the RSNE and RSNXE (if present) sent in Beacon and Probe Response frames by each affiliated AP.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13197 | 12.7.6.4 | 361 | 58 | "If any of these verification steps includes a mismatch, the STA shall disassociate or deauthenticate.If a second RSNE is provided in the message, the Supplicant deauthenticates." -- why is disassociation not acceptable in the second case? And how can the Supplicant deauthenticate? | Change to "If any of these verification steps includes a mismatch, or a second RSNE is provided in the message, the STA shall disassociate or deauthenticate." |
| 12102 | 12.7.6.4 | 361 | 59 | Change "If a second RSNE is provided in the message" to "If a second RSNE for any requested link is provided in the message" | As commented |
| 14094 | 12.7.6.4 | 361 | 59 | In 12.6.3.1 " the initiating non-AP MLD's RSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD" does not mandate that non-AP MLD must select a mandatorily supported stronger pairwise cipher. Suggest to allow AP to upgrade pairwise cipher suite to GCMP-256 in 4 way handshake message 3 | Change to p361.59 to "If a second RSNE is provided in MLO Link KDE of the link receiving the message 3, the Supplicant uses the pairwise cipher suite specified in the second RSNE or deauthenticates"Change p354.1 to "The RSNE field contains one or two RSNEs of the affiliated STA for the link specified in the Link Information field." |

### Discussion:

* The cited text in context is:



* For CID 13197, agree with the commenter that “disassociation” is missing from the second cited sentence. Also it would be better to align with the baseline and change “includes” to “indicates” in the first sentence.
* For CID 12102, commenter is correct in pointing out that any second RSNE would be provided on a per-link basis. And given MBO and MLO cannot operate simultaneously, the MLD should disassociate or deauthenticate.
* The use of STA in the cited text is also ambiguous given that this is MLO behavior. It would be better to use supplicant.
* For CID 14094 refers to baseline behavior for a “second RSNE”. In the baseline, when the second RSNE is supplied by the authenticator in message 3, the supplicant either accepts the pairwise cipher suite supplied by the authenticator or deauthenticates. In MLO, the “second RSNE” procedure is not supported and if the STA receives a “second RSNE” it deauthenticates.

### Proposed Resolution: (13164, 12102)

REVISED. The text has been modified in the direction proposed by the comments. Note that the procedures for the second RSNE are not supported in TGbe.

At the cited location,

Change

“If any of these verification steps includes a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant deauthenticates.”

to

“If any of these verification steps indicates a mismatch, the supplicant shall disassociate or deauthenticate. If a second RSNE is provided for any requested link in the message, the supplicant shall disassociate or deauthenticate.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 12103 | 12.7.7.2 | 364 | 27 | Add "For non-MLO," | As commented |
| 12104 | 12.7.7.2 | 364 | 28 | Add "For non-MLO," | As commented |
| 13198 | 12.7.2.2 | 364 | 33 | "For MLO, when present, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for anyof the setup links" -- what does "when present" refer to? MLO? And can it really be the GTK for any of the links; doesn't it have to be for each of the links? Ditto next 2 bullets | Change to "For MLO, an MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for eachof the setup links" |

### Discussion:

* The cited text in context is:



* CID 12103 and 12104 suggest adding “For non-MLO,” at the beginning of the IGTK and BIGTK bullets.
* For CID 13198, the comment suggests better wording for the MLO GTK bullet.

### Proposed Resolution: (12103, 12104, 13198)

ACCEPTED

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13199 | 12.7.8.2 | 365 | 56 | "the TDLS setup frames transmitted by at least one of theparticipating STAs does not include the TDLS Multi-Link element carrying the AP MLD MAC Address" -- what is "the TDLS setup frames"? And doesn't the TDLS MLe always carry the AP MLD address? And the wording is poor | Change to "the frames transmitted during the TPK handshake by at least one of theSTAs do not include a TDLS Multi-Link element". At 366.20 change "the TDLS setup frames transmitted by both peers include theTDLS Multi-Link element carrying the AP MLD MAC Address" to "the frames transmitted during the TPK handshake by both peers include aTDLS Multi-Link element" |

### Discussion:

* The cited text at 365.56:



* The cited text at 366.20:



* The commenter is noting that the frames are not TDLS setup frames, but frames transmitted during the TPK handshake.
* The change at 365.56 would be:

"the TDLS setup frames transmitted by at least one of the participating STAs does not include the TDLS Multi-Link element carrying the AP MLD MAC Address"

to

“the frames transmitted during the TPK handshake by at least one of the STAs do not include a TDLS Multi-Link element”

* The change at 366.20 would be:

"the TDLS setup frames transmitted by both peers include the TDLS Multi-Link element carrying the AP MLD MAC Address"

to

"the frames transmitted during the TPK handshake by both peers include a TDLS Multi-Link element"

### Proposed Resolution: (13199)

ACCEPTED.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13200 | 12.7.8.2 | 366 | 21 | It would be helpful to give a xref to where the TPK is defined when the setup is for multi-link TDLS | As it says in the comment |

### Discussion:

* Cited text in context:



* There should be a reference to the sub-clause on single link TDLS.
* Note that in the resolution below, the clause title will be inserted when the TGbe editor adds the cross reference to the clause.

### Proposed Resolution: (13200)

REVISED. Make changes in the direction proposed by the commenter. At the end of the paragraph at 366.20, change

“is for a single link TDLS:”

To

“is for single link TDLS (see 35.3.21.2):”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13201 | 12.7.8.4.3 | 367 | 11 | This is supposed to be a list of what's included, so saying "(when present)" is less than useful. Ditto at line 44 | Change to "(for multi-link TDLS)" |
| 13202 | 12.7.8.4.3 | 367 | 44 | No changes are identified | Underline line 44 |
| 10593 | 12.7.8.4.4 | 367 | 45 | Line 45 needs to be underlined | As in comment |

### Discussion:

* The cited text for CID 13201 in context is:



* Note that this describes the contents of TPK handshake message 2. CIDs 13202 and 10593 refer to the same text in the description of the contents for TPK handshake message 3.
* It would be good to modify the text to not only include multi-link TDLS, but a reference to the subclause describing the procedures.

### Proposed Resolution: (13201, 13202, 10593)

REVISED. Modify the text for both TPK handshake message 2 and TPK handshake message 3. At 367.12 and 367.45, change

“TDLS Multi-Link element (when present)”

to

“TDLS Multi-Link element (when present for TDLS setup procedures with multi-link operation, see 35.3.21)”

Note to Editor: the cited text at 367.45 needs to be underlined.