IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe LB266 Comment resolutions for RSNA and Keying |
| Date: 2022-10-25 |
| 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.

CIDs13179, 13191, 13198, 14100, 11071, 10678, 10679

R3 – Removed all resolved comments.

R4 – Updated resolution for CID 11071

### 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”.
* Not sure what to change or why this CID was deferred.

### Proposed Resolution: (13179)

ACCEPTED

### 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 (CID 213) in REVme changed length expressions for KDEs throughout the baseline to “variable”.
* The current text is not consistent with the latest REVme draft. The proposed resolution aligns the text with REVme D2.0

### Proposed Resolution: (13191)

ACCEPTED.

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

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 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. The change could be further improved with the following:

Change

“For MLO, when present, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links”

to

“For MLO, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for each of the setup links with a new GTK.”

* For the IGTK and BIGTK, the wording could be changed to (example with the IGTK)

Change

“For MLO, when present, the MLO IGTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links”

to

“For MLO, when present, the MLO IGTK KDE (see 12.7.2 (EAPOL-Key frames)) for each of the setup links with a new IGTK”

### Proposed Resolution:

(**13198**) REVISED. Make the change in the direction provided by the commenter. Also update the text for MLO IGTK and MLO BIGTK.

Change

“— For MLO, when present, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links

— For MLO, when present, the MLO IGTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links

— For MLO, when present, the MLO BIGTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links”

to

“— For MLO, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for each of the setup links with a new GTK.

— For MLO, when present, the MLO IGTK KDE (see 12.7.2 (EAPOL-Key frames)) for each of the setup links with a new IGTK

— For MLO, when present, the MLO BIGTK KDE (see 12.7.2 (EAPOL-Key frames)) for each of the setup links with a new BIGTK”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 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, 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** |
| 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. |

### Discussion:

* The OCI element protects the security protocol by allowing each party to validate the operating channel during security negotiations. The link ID is not required for the OCI KDE.
* The OCI element does need further clarification in the case where 320 MHz channels are used.

### Proposed Resolution: (11071)

REVISED. The link ID is not required in the OCI KDE for MLO. However the requirements for the Frequency Segment field need to be updated. Incorporate the changes in <this> document.

***Insert 9.4.2.236 and modify as follows:***

**9.4.2.236 OCI element**

***Modify the 5th paragraph as follows:***

The Frequency Segment 1 Channel Number field is set to the channel center frequency index of the

secondary segment (frequency segment 1) being used currently, if applicable.~~, or set to 0 otherwise.~~ If the channel specified by the operating class is 320 MHz in bandwidth, the Frequency Segment 1 Channel Number field is set to the center frequency of the channel. Otherwise, the field is set to 0. The value of the Frequency Segment 1 Channel Number field is one of the center frequency indices from the row corresponding to the operating class as defined in Annex E.

***Note that with REVme D2.0 the corresponding text in 12.7.2. for the OCI KDE has been removed and now refers to this clause 9 text.***