IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe LB271 Security comment resolutions – Part 2 |
| Date: 2023-05-05 |
| 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 LB271 on Clause 12 of P802.11be D3.0. The resolutions will be shown relative to D3.0.

CIDs 15145, 15697, 16683, 15205, 15208, 15168, 15143, 15144, 15513, 15204, 16329. 16330, 15514, 15532, 15515

Rev 0. Initial submission

Rev 1.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 15145 | 12.12.3 | 431.17 | The intention of having Mandatory support for GCMP-256 is to enable increased security strength. However, to enable incerased security strength, we need to also mandate the AKM that are used to support higher secuirty strength, i.e. SHA-384 for key derivaiton. | Suggest to add the following in 12.6.3 RSNA policy selection in an infrastructure BSS. "If an EHT AP includes the AKM suite selector value 00-0F-AC:8 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:24 in the RSNE." |
| 15697 | 12.12.3 | 431.17 | The intention of having Mandatory support for GCMP-256 is to enable increased security strength. However, to enable incerased security strength, we need to also mandate the AKM that are used to support higher secuirty strength, i.e. SHA-384 for key derivaiton. | Suggest to add the following in 12.6.3 RSNA policy selection in an infrastructure BSS. "If an EHT AP includes the AKM suite selector value 00-0F-AC:9 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:25 in the RSNE." |
| 16683 | 12.12.3 | 431.17 | "An EHT AP shall have dot11BeaconProtectionEnabled set to 1 when using RS." It is important to mandate EHT STA to support beacon protection also. | As in comment |

### Discussion:

* The cited text is:



* CIDs 15145 and 15697 are requesting that the negotiation of SAE and SAE-FT AKMs be mandated for negotiation between EHT STAs.
* For these CIDs, The commenter suggest the following text:

"If an EHT AP includes the AKM suite selector value 00-0F-AC:8 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:24 in the RSNE. If an EHT AP includes the AKM suite selector value 00-0F-AC:9 in the RSNE, then the EHT AP shall include the AKM suite selector value 00-0F-AC:25 in the RSNE.

* An EHT AP could advertise 00-0F-AC:8 or 00-0F-AC:9 to support connectivity from legacy devices. Also, an EHT AP could advertise 00-0F-AC:24 or 00-0F-AC:25 without including AKMs 8 and 9.
* The requirement should be that a non-AP EHT STA and an EHT AP shall negotiate 00-0F-AC:8 or 00-0F-AC:9 in establishing a security association. Also, this can be generalized to an EHT STA.
* CID 16683 is requesting that EHT STAs negotiate beacon protection when enabled on the AP. The text should be modified to require an EHT STA to set dot11BeaconProtectionEnabled. Note that this should be good for an EHT STA since it only enables beacon protection when it receives a BIGTK. It will always receive a BIGTK from an EHT AP.

### Proposed Resolution:

(**15145, 15697**) REVISED. Make changes suggested by the commenter to restrict SAE authentication between EHT STAs to AKMs 24 and 25.

At 431.22, add the following text:

“An EHT STA shall use 00-0F-AC:24 or 00-0F-AC:25 while negotiating the AKM for SAE authentication with another EHT STA.”

(**16683**) REVISED. Make changes suggested by the commenter

At the cited location change

“An EHT AP shall have dot11BeaconProtectionEnabled set to 1 when using RSN.”

to

“An EHT non-AP STA and EHT AP shall have dot11BeaconProtectionEnabled set to 1 when using RSN.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 15205 | 12.6.1.1.9 | 410.19 | An AP that has both MLD STAs and non-MLD STAs associated must use the same IGTKSA for protected group management traffic to all stations. | Change "with all non-AP STAs ... PTKSA" to "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 and with all non-MLD non-AP STAs that are associated with the AP operating on that link." |
| 15208 | 12.6.1.1.9 | 410.29 | If an AP affiliated with an MLD has both MLD and non-MLD STAs associated, the IGTKSA for non-MLD STAs will be identified by the AP MLD MAC address (the Authenticator), whereas the IGTKSA (for the same IGTK) will be identified by the MAC address of the AP operating on the link, which means the SME will have two IGTKSAs for the same IGTK. | Change "-- For non-MLO, Authenticator MAC address. For MLO, the MAC address of the AP operating on the link corresponding to the IGTKSA" to "-- Authenticator MAC address.-- If dot11MultiLinkActivated is true, the MAC address of the AP operating on the link corresponding to the IGTKSA." (i.e. retain the auth mac address, and add an additional item if MLO is enabled) |

### Discussion:

* The cited text is:



* The comments is asking that the \*\*\*\*\*\*\*\*\*
* CID 15205 is asking for the following text change:

“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”

to

“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 and with all non-MLD non-AP STAs that are associated with the AP operating on that link."

* For MLO or non-MLO the IGTKSA consists of the Authenticator address. As the commenter points out, with MLO the IGTK is associated with the affiliated AP address.
* Other things “that operate on the link” is not really required. It’s a non-AP STA that is affiliated with a non-AP MLD with a valid PTKSA.

### Proposed Resolution:

(**15205**) REVISED. Modify the cited text in the direction proposed by the commenter:

At the cited location change:

“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”

to

“with all non-AP STAs affiliated with the non-AP MLD with a valid PTKSA and with all non-AP STAs that are associated with the AP operating on that link."

(**15208**) REVISED. Modify the cited text in the direction proposed by the commenter and also make a similar change for the BIGTKSA.

At the cited location change:

“—For non-MLO, Authenticator MAC address. For MLO, the MAC address of the AP operating on the link corresponding to the IGTKSA.”

to

“— Authenticator MAC address.

— For MLO, the MAC address of the AP operating on the link corresponding to the IGTKSA."

At 410.53, change

“For non-MLO, Authenticator MAC address. For MLO, the MAC address of the AP operating on the link corresponding to the BIGTKSA.”

to

“— Authenticator MAC address.

— For MLO, the MAC address of the AP operating on the link corresponding to the BIGTKSA."

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15168 | 12.6.14 | 412.36 | Use non-AP STAs for STAs affiliated with a non-AP MLD. | Use non-AP STAs for STAs affiliated with a non-AP MLD. |

### Discussion:

* The cited text in context is:



* Agree with the commenter that it would better to use non-AP STAs rather than STAs in this case.

### Proposed Resolution: (15168)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15143 | 12.6.2 | 411.11 | Add a note that the RSNE and RSNXE selection for non-AP MLD is described in 12.6.3.1 so that people do not misunderstand that the rule for non-AP MLD is missing.. | As described in comment. |

### Discussion:

* The cited text in context:



* The commenter suggests adding a note, however it would be better to add a reference in the text to 12.6.3. This could be done by adding the following sentence:

“Non-AP MLD RSNA policy selection for MLO is described in 12.6.3.1”

### Proposed Resolution: (15143)

REVISED. Add the reference to the RSNE policy selection clause as suggested by the commenter. Append the following sentence to the paragraph cited by the commenter:

“RSNA policy selection for a non-AP MLD is described in 12.6.3.1”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15144 | 12.6.3.1 | 411.34 | There are group data cipher suite and group managmenet cipher suite. Simply just say "one group cipher suite selector" is confusing when client needs to include both group data cipher suite and group managmeent cipher suite. | change "The RSNE shall include one AKM suite selector, one pairwise cipher suiteselector, and one group cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD." to "The RSNE shall include one AKM suite selector, one pairwise cipher suiteselector, one group data cipher suite selector and one group management cipher suite selector that are common among those advertised by the APs affiliatedwith the targeted AP MLD." |

### Discussion:

* Cited text in context:



* The commenter is requesting that the sentence needs to be changed:

"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."

to

"The RSNE shall include one AKM suite selector, one pairwise cipher suite

selector, one group data cipher suite selector and one group management cipher suite selector that are common among those advertised by the APs affiliated with the targeted AP MLD."

* The commenter is correct. Note that the field that carries the group cipher suite is called “Group Data Cipher Suite” field, but the group cipher applies to both group addressed data and management frames when MFP is negotiated.

### Proposed Resolution: (15144)

ACCEPTED

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15513 | 12.7.1.1 | 413.33 | The first sentence implies there may be multiple pairwise keys, whilst the second sentence says 'identifies the pairwise key', which is confusing. | Change 'identifies the pairwise key' to:identifies the pairwise key(s) |

### Discussion:

* Cited text in context:



* This text seems to be adapted from the baseline text that addresses multi-band operation.
* Since multi-band and multi-link operation are distinct and cannot be combined, there should only be a single key.
* The text should be modified to specify a single key. The updated text would then be:
* “An MLD shall support one pairwise key for any <transmitter\_MLD MAC address, receiver\_MLD MAC address> pair for use with enhanced data cryptographic encapsulation mechanisms. The <transmitter\_MLD MAC address, receiver\_MLD MAC address> pair identifies the pairwise key.”

### Proposed Resolution (15513):

REVISED. There is only a single pairwise key derived for use between an AP MLD and a non-AP MLD.

At 413.33, change “shall support at least one pairwise key” to “shall support one pairwise key”.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15204 | 12.7.1.4 | 413.40 | Changes not correctly identified. | None of the text in this clause is shown with strikethroughs or underlines. What text is being changed? |

### Discussion:

* Cited text in context:



* The only text that has been added is the note.

### Proposed Resolution: (15204)

REVISED. Underline the note at 413.50.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 16329 | 12.7.2 | 416.01 | "a MLO" is not correct. | Please change as: "an MLO". |
| 16330 | 12.7.6.4.4 | 424.30 | "a MLO" is not correct. | Please change as: "an MLO". |

### Discussion:

* Cited text in context:



* There are 3 locations where “a MLO” is used and 8 locations where “an MLO is used. According to IEEE SA P&P, the usage is up to the publication editor, but it would be good to make the usage consistent.

### Proposed Resolution:

**(16329)** ACCEPTED

**(16330)** ACCEPTED. Note to Editor: In addition, make the same change at 547.23

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15514 | 12.7.4 | 418.19 | Clarify 'MAC Address' refers to 'MAC Addresss KDE' | Change to: is the MAC Address KDE, contains MLD MAC address of the MLD with which the transmitting STA is affiliated. |
| 15515 | 12.7.6.1 | 419.12 | Change 'MAC Address' to 'MAC Addresss KDE' in this paragraph | As in comment |
| 16332 | 12.7.6.1 | 419.63 | "an MAC" is not correct. | Please change as: "a MAC". |

### Discussion:

* Cited text in context:







* These comments have to do with EAPOL-Key notation that is used to explain the 4-way handshake and group key handshake in later clauses.
* For CID 15514, agree with the commenter that the description could be improved by indicating that the MAC address is carried in the MAC Address KDE.
* For CID 15515, The notation of MAC Address is consistent with other KDEs in the notation. For example, GTK[N].
* Note that the description at the bottom of the page explains that the MAC Address KDE contains the MLD MAC Address.
* CID 16632 is editorial

### Proposed Resolution:

**(15514)** ACCEPTED

**(15532)** ACCEPTED

**(15515)** REJECTED. The use of “MAC Address” at the cited location refers to the MAC Address KDE. The notation is defined in 12.7.4. Also, the description at the bottom of the page (419.63) indicates that the MLD MAC address is carried in the MAC Address KDE