IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe LB266 Comment resolutions for non-clause 12 security comments | | | | |
| Date: 2022-10-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Background

This contribution proposes comment resolutions to TGbe comments received in LB266 on comments outside of clause 12.

CIDs 10587, 13132, 12061, 13133, 13134, 12369, 14104, 14105

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 10587 | 11.2.3.16.1 | 306 | 11 | The frame exchange needs to occur on an enabled link. Furthermore, clarify the respective STA and AP are affiliated with a non-AP MLD and an AP MLD respectively. | Modify sentence as "... through their respective affiliated non-AP STA and AP over an enabled link." |

### Discussion:

* The cited text is:

Text

Description automatically generated

* The comment is requested the following modification:

Change

“through an affiliated STA and an affiliated AP over a setup link.”

to

“through their respective affiliated non-AP STA and AP over an enabled link.”

* The use of “setup link” rather than “enabled link” is more appropriate here.

### Proposed Resolution: (10587)

REVISED. At 306.11 relative to D1.0, change

“through an affiliated STA and an affiliated AP over a setup link.”

to

“through their respective affiliated STA and AP over a setup link.”

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13132 | 11.2.3.16.3 | 306 | 31 | "andis negotiated" should be "is negotiated" | As it says in the comment |
| 12061 | 11.2.3.16.3 | 306 | 32 | "and" should be also stricked out, otherwise it reads "- If management frame protection and is negotiated ..." | As in comment |
| 13133 | 11.2.3.16.3 | 306 | 33 | "BIGTK\_shall" should be "BIGTK shall" | As it says in the comment |
| 13134 | 11.2.3.16.3 | 306 | 35 | This is a technical change, as the middle item previously didn't depend on having a PTK. And how can the IGTK be updated if MFP is not negotiated, and why does updating the BIGTK depend on having a PTK? | Add "where appropriate" where appropriate |
| 12369 | 11.2.3.16.3 | 306 | 43 | The term "MLD association" is not defined in 11.3, so its better to reference 4.5.3.3 where the term is defined. | Add reference to 4.5.3.3 where the term is defined. |

### Discussion:

* The cited text is:

Text

Description automatically generated

* In the first bullet of the first list, there is an extraneous “and” (“If management frame protection and is negotiated …”) which should be removed per CIDs 13132 and 12061s
* In the second bullet of the first list, there is an extraneous “\_” between “BIGTK” and “shall” that needs to be removed per CID 13133
* For CID 13134, the commenter correctly points out that IGTK and BIGTK would only be present if MFP was negotiated, so “current GTK, IGTK, and BIGTK” should be “ current GTK, IGTK when management frame protection is negotiated, and BIGTK when beacon protection is negotiated ”. Also “pending GTK(s), IGTK(s), and BIGTK(s) should be “pending GTK(s), IGTK(s) when management frame protection is negotiated, and BIGTK(s) when beacon protection is negotiated,”
* For CID 12369. It’s true that the term “MLD Association” is not defined. However the term association is. It would be better to update the text to avoid introducing a new term. Also, CID 10270 which has already been resolved, removed the cited text.

### Proposed Resolution:

### (13132. 12061, 13133) ACCEPTED

**(13134)** REVISED. At 306.33 and 306.46 relative to D1.0, change

“current GTK, IGTK, and BIGTK”

to

“current GTK, IGTK when management frame protection is negotiated, and BIGTK when beacon protection is negotiated “

At 306.36 aand 306.49 change

“pending GTK, IGTK, and BIGTK”

to

“pending GTK, IGTK when management frame protection is negotiated, and BIGTK when beacon protection is negotiated “

**(12369)** REVISED. Revise the text to remove the term “MLD Association”.

At 306.29, change

“When the association is not an MLD association”

ro

“For non-MLO, with RSN and a valid PTK is configured for the STA:”

At 206.43, change

When the association is an MLD association“

to

“For MLO, with RSN and a valid PTK is configured for the non-AP MLD:”

Note to Editor: This CID is the same resolution of 10270. No further changes are required.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 14104 | 35.2.5.2 | 423 | 41 | " Each AP and the corresponding non-AP STA affiliated with an associated non-AP MLD maintains a single PN/IPN/BIPN for each GTK/IGTK/BIGTK."  After non-AP switching link from link 1 to link 2 for receiving group addressed frame , it does not know the updated PN/IPN of link 2, and the received group addressed frame can be of an outdated PN and with a forged SN. The link switching and group frame replay protection should have similar security as in WNM sleep response | Allow a protected DTIM beacon to advertise the last PN/IPN of group addressed frames of that link |
| 14105 | 35.2.5.2 | 423 | 41 | " Each AP and the corresponding non-AP STA affiliated with an associated non-AP MLD maintains a single PN/IPN/BIPN for each GTK/IGTK/BIGTK." After non-AP switching link from link 1 to link 2 for receiving Beacon frame, it does not know the updated BIPN of the link 2. The received Beacon on link 2 could be replayed with a forged timestamp | Change in 12.5.3.4 "BIP replay protection" such that BIPN is increment by 1 for each TBTT (instead of a strictly increasing integer), such that a non-AP MLD switching to this link has an idea what is the expected BIPN |

### Discussion:

* The cited text is:

Text

Description automatically generated

* For CID 14104. The comment discusses a scenario when a non-AP MLD switches the link that it uses to receive group-addressed traffic. The comment claims

“After non-AP switching link from link 1 to link 2 for receiving group addressed frame , it does not know the updated PN/IPN of link 2, and the received group addressed frame can be of an outdated PN and with a forged SN. The link switching and group frame replay protection should have similar security as in WNM sleep response.”

* The proposed resolution for CID 14104 suggests advertising the PN values in some protected manner in each DTIM frame.
* The PNs are managed by the affiliated APs on a per-link basis and follow the baselinr procedures for incrementing the PN. As long as the PN used to encapsulate a group-addressed frame is greater than the PN received in the most recent 4-way handshake, group-key handshake, or successfully received group-addressed frame, the PN is valid.
* It should be noted that there are multiple causes for a legacy non-AP STA to miss multiple group-addressed frame transmissions and receive a PN that is larger than its currently tracked PN.
* The SN is managed by the AP MLD so SN would be the same for each link.
* If the non-AP MLD detects that a GTK associated with a link is compromised, it could send an EAPoL-Request frame to trigger a new group-key handshake.
* For CID 14105, The comment discusses a scenario when a non-AP MLD switches between links with beacon protection enabled, it does not know the most recent BIPN associated with the beacon frame. The comment claims that the beacon frame could be transmitted with a forged timestamp.
* As long as the BIPN received on the updated link for the beacon frame has a BIPN that is greater than the last received beacon, the beacon frame should be valid.
* Legacy STAs can miss multiple beacon frames and receive frames with a BIPN greater than its configured BIPN.
* If a frame can be replayed with a forged timestamp, the BIGTK is compromised.
* Assuming the BIPN is incremented by one for each beacon frame transmitted, the BIPN will be increased by one at each TBTT.
* It the non-AP MLD detects that the BIGTK is compromised, it can trigger a new group key handshake to refresh the keys.

### Proposed Resolution: (14104, 14105)

REVISED. The PN is managed by each affiliated AP and affiliated STA link independently and s PN is received for each link, securely, as part of the 4-way handshake or group key handshake and prevents replay detection. It’s not uncommon for a legacy non-AP MLD to miss reception of group-addressed frames so as long as the PN in the received frame is greater than the maintained PN, the non-AP STA can determine that the frame has not been replayed. If a non-AP MLD detects that a GTK may be compromised, it can trigger a new group-key handshake with the AP MLD.

At 423.48, insert the following note:

"NOTE - When a non-AP MLD changes the link used for group-addressed frame reception, the non-AP MLD supplicant is able to request a group-addressed handshake by sending an EAPOL-Key frame to the AP MLD authenticator with the Key Type set to Group (0) and the Request bit set to 1 (see 12.7.7.1 General) to refresh Key RSC/BPN/IPN. “.