IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe CC-34 CIDs 2476 and 3133 | | | | |
| Date: 2021-05-10 | | | | |
| 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 comments 2476 and 3133 received in CC34 on Clause 12 of TGbe D0.3

Straw\_poll: Instruct the editor to update the latest TGbe draft with the changes shown in document 11-21/788r1, which address CIDs 2476 and 3133 from CC-34.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 2476 | 131 | 59 | 35.3.5.2 | Change "The PMK, PTK, and the same PN space are used for all the setup links between the ﾠnon-AP MLD and the AP MLD for the PTKSA." to "The PMK, PTK, and PN space are common to all the links set up between the non-AP MLD and the AP MLD for the PTKSA." | As in the comment |
| 3133 | 131 | 56-61 | 35.3.5.2 | This paragraph mixes keys, PN, SA, MAC addresses all together. Consider to rewrite based on the proposed change. | A single PMKSA and a single PTKSA are established between the non-AP MLD and the AP MLD for all the setup links. (and amend the PMKSA and PTKSA definitions to specify MLD MAC addresses) |

### Discussion:

The cited paragraph is as follows:

“After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMK is established and a PTK is derived through a 4-way handshake between the non-AP MLD and the AP MLD (see 12.7.6 (4-way handshake)). The PMK, PTK, and the same PN space are used for all the setup links between the non-AP MLD and the AP MLD for the PTKSA. The non-AP MLD and the AP MLD use their respective MLD MAC addresses to derive the PMK under the SAE method and PTK.”

The PTK is not always derived through a 4-way handshake, it could be derived using FT or FILS protocols. A more general statement would be that the PMKSA and PTKSA are established between the AP MLD and non-AP MLD using their respective MLD MAC addresses.

Cryptographic encapsulation uses the AP MLD and non-AP MLD MAC addresses and is described in detail in 12.5.3.3 and 12.5.5.3. It would be better to simply refer to these clauses.

### Proposed Resolution: (2476, 3133)

Revised. The cited paragraph has been modified to reference the PMKSA, PTKSA and their relationship to the AP MLD and non-AP MLD MAC addresses.

Replace

“After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMK is established and a PTK is derived through a 4-way handshake between the non-AP MLD and the AP MLD (see 12.7.6 (4-way handshake)). The PMK, PTK, and the same PN space are used for all the setup links between the non-AP MLD and the AP MLD for the PTKSA. The non-AP MLD and the AP MLD use their respective MLD MAC addresses to derive the PMK under the SAE method and PTK..”

With  
“After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMKSA and PTKSA are established between the non-AP MLD and the AP MLD (see Clause 12). The PTKSA is used for cryptographic encapsulation across all setup links as described in 12.5.3.3 and 12.5.5.3.”