IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe SA1 Security Comment Resolutions | | | | |
| Date: 2024-02-16 | | | | |
| 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 SA Ballot on D5.0, mainly on Clause 12, of P802.11be D5.0. The resolutions will be shown relative to D5.0.

CIDs 22013, 22239, 22244, 22245, 22246, 22247, 22101, 22361, 22362, 22363, 22379, 22380

Rev 0. Initial submission

Rev 1.

Rev 2.

Rev 3.

Rev 4.

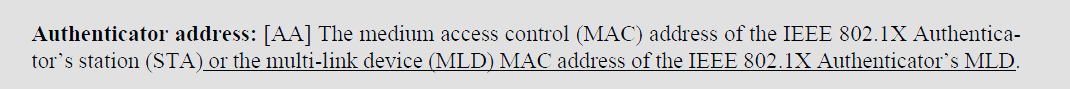
Rev 5.

### Comment

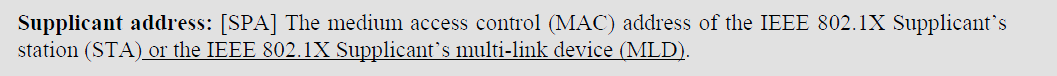
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 22013 | 3.1 | 53.21 | Align the definitions of Authenticator and Supplicant. | Delete "multi-link device (MLD) MAC address of the" from the Authenticator address definition. |

### Discussion:

* The cited text (at 53.21) is:



* The definition of Supplicant address is:



* Agree with the commenter that the proposed change aligns the two definitions and removes duplicative text.

### Proposed Resolution (22013):

ACCEPTED,

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22239 | 12.2.10 | 410.07 | Submitted on behalf of Po-Kai. It is also possible for an affiliated non-AP STA MAC address to be changed when association or reassociation to the same AP MLD. | Add at the end of last paragraph. "An affiliated non-AP STA MAC address may be changed subject to the requirements above when performing association or reassociation to the AP MLD that the non-AP MLD is currently associated with." |

### Discussion:

* The cited text is:

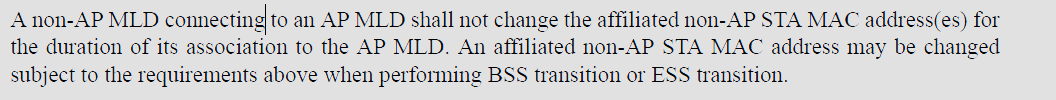
A close-up of a document

Description automatically generated

* The commenter proposes to add the following to the end of the cited paragraph:

“An affiliated non-AP STA MAC address may be changed subject to the requirements above when performing association or reassociation to the AP MLD that the non-AP MLD is currently associated with.”

* The cited text provides the requirements on the identity of SAE entities that perform SAE. The proposed text provides a requirement on, presumably a non-AP MLD, in changing an affiliated STA MAC address when performing association or reassociation to another peer SAE entity.
* Note that this requirement should apply more broadly to a changing affiliated STA MAC address, and should likely be included in 12.2.10.
* Related text in 12.2.10 is as follows at p408.5:



* It would make sense to add a note after this paragraph clarifying the requirement in the last sentence.

### Proposed Resolution: (22239)

REVISED. The proposed change looks to add a requirement related to a non-AP MLD changing its affiliated STA MAC address while performing (re-)association. It applies to more than SAE entities. A note could be added in 12.2.10 to clarify the affiliated STA addresses could be changed on association/re-association to the current AP.

At 410.17, add “NOTE – A non-AP MLD might change its affiliated STA address when performing association or reassociation to the AP MLD that it is currently associated.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22247 | 12.6.19 | 428.27 | Submitted on behalf of Po-Kai. For the editori's note "Editor’s Note: In REVme 3.0, TPKSA is added in the third paragraph. Do we need to add it to this new paragraph for MLO too?", the new paragraph is about group key. TPKSA is not group key at all, so the question is not relevant. | Delete the Editor's note |
| 22101 | 13.4.2 | 450.13 | Address the editor note on including the WIGTK. Also at 468.50. | The WIGTK needs to be addressed and added to the specification. At this point it looks as though the WIGTK is managed at the MLD level. Commnter will provide a contribution to discuss and update the draft. |
| 22244 | 12.7.7.1 | 441.58 | Submitted on behalf of Po-Kai. For the editor's note "Editor’s Note: Do we need to add MLO WIGTK n?" whether to add WUR to MLO is a spearate topic by itself. The answer to the question is no until we decide to expand WUR to MLO. | Delete the Editor's note |
| 22245 | 12.7.7.1 | 441.47 | Submitted on behalf of Po-Kai. For the editor's note "Editor’s Note: Do we need to add MLO WIGTK in the above paragraph?" whether to add WUR to MLO is a spearate topic by itself. The answer to the question is no until we decide to expand WUR to MLO. | Delete the Editor's note |
| 22242 | 13.8.5 | 470.50 | Submitted on behalf of Po-Kai. For the editor's note "Editor’s Note: Do we need to add the MLO WIGTK subelement?" whether to add WUR to MLO is a spearate topic by itself. The answer to the question is no until we decide to expand WUR to MLO. | Delete the Editor's note |
| 22243 | 13.4.2 | 452.13 | Submitted on behalf of Po-Kai. For the editor's note "Editor’s Note: Do we need to add MLO WIGTK?" whether to add WUR to MLO is a spearate topic by itself. The answer to the question is no until we decide to expand WUR to MLO. | Delete the Editor's note |
| 22246 | 12.7.6.4 | 439.01 | Submitted on behalf of Po-Kai. For the editori's note "Editor’s Note: In REVme D3.0, the WIGTK KDE is added to the first bullet. Do we need to add MLO WIGTK KDE in the above underlined bullet?" whether to add WUR to MLO is a spearate topic by itself. The answer to the question is no until we decide to expand WUR to MLO. | Delete the Editor's note |

### Discussion:

* These CIDs relate to the Editor’s note questioning whether there are updates to the text to support WIGTK. Searching for Editors’s Note with respect to the WIGTK: The text at these locations are as follows:
* P 426.26 – missing TPKSA in the first sentence. Update the list to include PTKSA and TPKSA

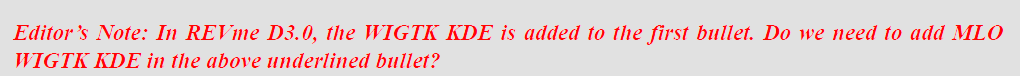
A close up of a text

Description automatically generated

* p.437.1 – There is no MLO WIGTK KDE. No Change

A close up of a document

Description automatically generated



* p.439.38 – There is no MLO WIGTK KDE. No change

A screenshot of a computer

Description automatically generated

* p.450.13 – There is no MLO WIGTK KDE. No change

A screenshot of a computer

Description automatically generated

* p468.50

A close up of a text

Description automatically generated

### Proposed Resolution:

**(22247)** REVISED. In the baseline for re-keying, the list of security associations was expanded to include the PTKSA and the TPKSA.

Delete the “Editor’s Note” at 426.27.

At 426.20, change

“For MLO, the AP MLD’s Authenticator manages packet number assignment for the PTKSA with a non-AP MLD.”

to

“For MLO, the AP MLD’s Authenticator manages packet number assignment for the PTKSA and TPKSA with a non-AP MLD.”

**(22242, 22243, 22244, 22245, 22246)** ACCEPTED

**(22101)** REVISED. There is not requirement for an MLO WIGTK. Delete the “Editor’s Note” at 450.13.

Note to Editor: This is the same resolution as 22243.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22361 | 12.3.3.2.1 | 408.23 | [Al Petrick] The affiliation is for a non-AP STA and AP STA | Change "affiliated STA" to "affiliated non-AP STA" Change "affiliated AP" to "affiliated AP-STA" |

### Discussion:

* Cited text in context:

A close-up of a document

Description automatically generated

* The usage of affiliated STA and affiliated AP and how they relate to the non-AP MLD and AP MLD are clear in the cited text. There is no ambiguity caused by the use of the terms “affiliated STA” or “affiliated AP”
* In the draft, there are 40 occurrences of affiliated non-AP STA
* There are 97 occurrences of affiliated STA
* There are 355 occurrences of affiliated AP
* There are no occurrences of affiliated AP-STA

### Proposed Resolution: (22361)

REJECTED. The usage of terms “affiliated STA” and “affiliated AP” in the cited text clearly indicate the components of the MLD. There is no ambiguity caused in the use of “affiliated STA” and “affiliated AP” in this cited location.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22362 | 12.2.10 | 409.51 | [Al Petrick] BSS transition to and AP is to an AP STA. Change AP to AP STA | Change "AP" to "AP STA" as commented |
| 22363 | 12.2.10 | 409.56 | [Al Petrick] Note is discussing non-AP STA transitions to AP. In this case, the transition is to a AP-STA. | Change "AP" to "AP STA" |

### Discussion:

* Page number looks to be 407, not 409. Here is the cited text in context:

A close up of a text

Description automatically generated

* The cited paragraph deals with BSS transition which be definition refers to the transition between APs in an ESS. So the term “AP” in this context is clear.

### Proposed Resolution: (22362, 22363)

REJECTED. The usage of the term AP in the cited text clearly refers to an AP operating in a BSS. There is no ambiguity caused in the use of “AP” in this cited location.

### Comment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22379 | 12.4.4.1 | 410.57 | CID 19516 was addressed by removing the reference to IETF RFC 2409 from Clause 2 (P51 L4) without updating all locations that reference IETF RFC 2409 in the baseline. As such, this would break the standard once IEEE 802.11be gets incorporated in the next maintenance round. Referencing IETF RFC 4306 feels strange because that RFC was obsoleted by RFC 5996 which itself was obsoleted by RFC 7296. In other words, if we are moving from IKE v1 to IKE v2, we should reference RFC 7296. In addition, the only actual change from RFC 2409 to RFC 4306 in 12.4.4.1 (P412 L57) looks incorrect since it would now be pointing to an IANA registry that does not exist. Before this change, we were referencing this registry: https://www.iana.org/assignments/ipsec-registry/ipsec-registry.xml#ipsec-registry-10 If we were to want to move to using the IANA IKE v2 registry that contains the same values and additional updates, the reference should be to registry called "Transform Type 4 - Key Exchange Method Transform IDs" for IETF RFC 7296 (IKEv2). https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8 CID 19516 does not include any justification for the proposed change, so this comment is proposing the incomplete and incorrect changes to be reverted. This comment could be addressed by fixing the changes to be complete (i.e., cover all instances of IETF RFC 2409 in the baseline) and correct (i.e., use RFC 7296 and update the IANA registry name). | In Clause 2, replace the reference to IETF RFC 4306 with reference to IETF RFC 7296. In 12.4.4.1, reference IETF RFC 7296 instead of IETF RFC 4306 and replace "Group Description" with "Transform Type 4 - Key Exchange Method Transform IDs". Update all other references to IETF RFC 2409 in the baseline: REVme/D4.2 (in 9.4.1.10, 12.10.2, 12.11.2.3.2, Annex C - dot11RSNAConfigDLCGroupIdentifier) to point to IETF RFC 7296 and the "Transform Type 4 - Key Exchange Method Transform IDs" attributes. |

### Discussion:

* The comment points out that the changes made as a resulted in a reference to an obsolete RFC.
* The commenter is proposing that the up-to-date RFC and IANA registry replace the changes that were made by CID 19516.

### Proposed Resolution: (22379)

REVISED. Make the changes proposed by the commenter. The specific changes are:

At 51.9 Change

“IETF RFC 4306, Internet Key Exchange (IKEv2) Protocol, C. Kaufman, Ed., Dec. 2005”

to

“IETF RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2), C. Kaufman, Ed., Oct. 2014”

At 410.56, change

“Group Description”

to

“Transform Type 4 - Key Exchange Method Transform IDs”

At 410.57, replace “IETF RFC 4306” with “IETF RFC 7296”

Relative to REVme D5.0,

At 827.46 replace

“maintained by IANA as “Group Description” attributes for IETF RFC 2409 (IKE)”

with

“maintained by IANA as “Transform Type 4 - Key Exchange Method Transform IDs” attributes for IETF RFC 7296”

At 1561.20, replace

“from the “Group Description” registry maintained by IANA for IETF RFC 2409 (IKE)”

with

“from the “Transform Type 4 - Key Exchange Method Transform IDs” registry maintained by IANA for IETF RFC 7296”

At 3135.53, 3141.53, and 5557.38 replace

“maintained by IANA as “Group Description” attributes for IETF RFC 2409 (IKE)”

with

“maintained by IANA as “Transform Type 4 - Key Exchange Method Transform IDs” attributes for IETF RFC 7296”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22380 | 12.7.1.6.5 | 0.00 | The MLD design for PTK derivation was modified by defining AA/SPA to be the MLD MAC addresses. This ends up updating the rules for deriving PTK in 4-way handshake. However, this is not sufficient to cover the FT case where PTK derivation in 12.7.1.6.5 is defined to use BSSID and STA-ADDR (non-AP STA's MAC address) instead of AA/SPA. 12.7.1.6.5 needs to be modified to be consistent with the MLD MAC address use and also to be consistent with known FT with MLO implementations. | Modify 12.7.1.6.5 to change STA-ADDR definition from "is the non-AP STA's MAC address" to "is the MLD MAC address of the non-AP MLD when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the non-AP STA's MAC address" and BSSID definition from "is the BSSID of the target AP's BSS" to "is the MLD MAC address of the target FTR when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the BSSID of the target AP's BSS". |

### Discussion:

* The cited text in REVme D5.0 at 3086.14 is as follows:

A screenshot of a computer

Description automatically generated

* The proposed changes update the PTK derivation for FT to align with the changes made for RSN.
* Relative to REVme D5.0, the changes are:

At 3086.14, (STA definition) change

“is the non-AP STA’s MAC address”

to

“is the MLD MAC address of the non-AP MLD when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the non-AP STA's MAC address”

At 3086.26, change

“is the BSSID of the target AP’s BSS”

to

“is the MLD MAC address of the target FTR when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the BSSID of the target AP's BSS”

### Proposed Resolution: (22380)

ACCEPTED.

Note to Editor, the changes relative to REVme D5.0 are as follows:

At 3086.14, (STA definition) change

“is the non-AP STA’s MAC address”

to

“is the MLD MAC address of the non-AP MLD when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the non-AP STA's MAC address”

At 3086.26, change

“is the BSSID of the target AP’s BSS”

to

“is the MLD MAC address of the target FTR when the S1KH is a non-AP MLD and the R1KH is an AP MLD; otherwise, is the BSSID of the target AP's BSS”