IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe SA1 Security Comment Resolutions | | | | |
| Date: 2024-05-13 | | | | |
| 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 22160, 22340

CIDs 22013, 22239, 22242, 22243, 22244, 22245, 22246, 22247, 22101, 22361, 22362, 22363, 22379, 22380

Rev 0. Initial submission

Rev 1. Addressed comments received offline

Rev 2. Reviewed on TGbe teleconference

Rev 3. Update to propose resolutions to 22160 and 22340 and 4-way handshake clarification

Rev 4.

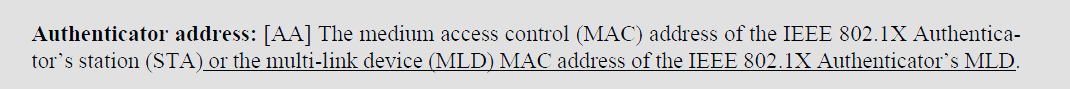
Rev 5.

### Comment

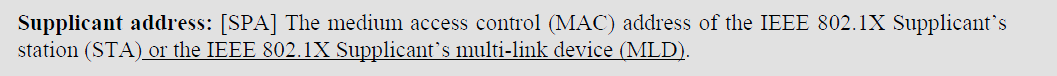
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 22013 | 3.1 | 53.21 | Align the definitions of Authenticator and Supplicant. | Delete "multi-link device (MLD) MAC address of the" from the Authenticator address definition. |

### 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):

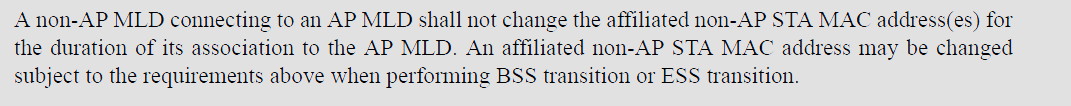
ACCEPTED,

### 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:

* In the previous version of this document, the cited text was incorrect. The cited text in 12.2.10, p408.07



* The proposed change is add the following to the end of the sentence but the grammar could be improved:

“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.”

### Proposed Resolution: (22239)

REVISED. Make the changes proposed by the commenter re-worded as follows. Append the following sentence to the end of the paragraph at the cited p408.07:

“A non-AP MLD may change its affiliated STA MAC 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

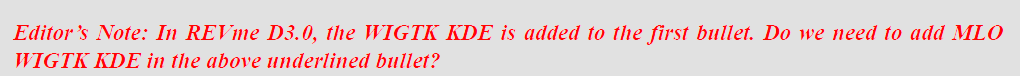
A close up of a text

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)** ACCEPTED

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

**(22101)** REVISED. There is no 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”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 22160 | 11.13 | 394.01 | The security properties of MLO in the current draft are not enough to provide guarantees that OCV provided in baseline. Extend OCV to operate in an MLO context as well. This is vitally important with mechanisms of add/delete AP links becoming more prevalent in later drafts. | As in comment |
| 22340 | 11.13 | 396.30 | [Thomas Derham] OCV is improperly specified in 11be as discussed in this thread: https://grouper.ieee.org/groups/802/11/email/stds-802-11-tgbe/msg08158.html | Provide means for channels of all links to be exchanged during OCV negotiation, such that subsequent frames that do not match those validated channels are properly discarded. |

### Discussion:

* Comments on OCV with MLO have been submitted in multiple rounds of balloting and so far, there hasn’t been an agreed set of updates to the draft to resolve the comments.
* There are two components to the issue:
  1. Is OCV in the 4-way handshake (and similar FT and FILS protocols), and similar security exchange sufficient with MLO.
  2. How does the non-AP MLD verify the operating channel information for each affiliated AP?
* To address issue “1.”, we added a requirement that restricts the Authentication, Association, and 4-way handshake to occur on the same link. We could add a note in the OCVC clause to alert the reader to the requirement.
* “Yes I believe the 4-way handshake, and ML reconfiguration frames (Link Reconfiguration
* The context of this sentence is that the "primary channel... used by the STA to receive PPDUs from the peer STA" is equal to the values in the OCI most recently sent to that peer STA.
* (We had proposed some clarifications on that text a while back - attached again here for reference, minus the discussion on attack vectors which I remove for now).
* Since the OCI only contains information on one of the channels, I think we either need to add OCI so all links are covered, or state this sentence doesn't apply to EHT/MLO or something; otherwise it would imply all frames on the other links should be dropped.
* To address issue 2, Beacon frame protection is required for MLO so the operating channel information can be verified by each affiliated non-AP STA. We could add some requirements on the non-AP MLD validating the operating channel information in beacon frames for each link.
* As discussed earlier, the use of BP for validating the operating channel during operation is not really equivalent to OCV, in particular related to insider attacks where attacker knows the BIGTK. If we decide not to update OCV, then we should probably consider defining an enhancement of BP that is resistant to such attacks...
* 2.2.9 Requirements for Operating Channel Validation
* …
* (#3334)If a STA with OCVC(#3505) receives a frame from (#1414)a peer STA that is not on the same channel used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.
* Perhaps it can be modified, to cover the MLO links better
* (#3334)If a STA with OCVC(#3505) receives a frame from (#1414)a peer STA that is not on the same channel used by the STA to receive PPDUs from the peer STA  (Note: this includes peer STA in the same MLD but different MLO transmitter address in A2),  or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.
* Clause 12.2.9 from REVme D5.0 is shown as follows:

A screenshot of a computer

Description automatically generated

A close-up of a document

Description automatically generated

### Proposed Resolution: (22160, 22340)

**REVISED. Incorporate the changes under “Proposed Resolution: (22160, 22340)” into <this> document.**

***Insert clause 12.2.9 into the TGbe draft with the following modifications:***

* Requirements for Operating Channel Validation

When OCVC(#3505) is present, a STA, or MLD shall advertise this capability in (#6299)the RSNE and shall include operating channel information and validate the Operating Channel Information (OCI) received from an OCVC(#3505) peer in certain protected messages used for key establishment and confirmation. The MLD advertises this capability through all of its affiliated STAs.

NOTE – Each STA affiliated with an MLD advertises OCVC capability in the RSNE.

A STA with OCVC determines channel information from received OCI. An MLD with OCVC determines operating channel information from received OCI on the link used for the establishment of a security association (for example, the 4-way handshake). After a security association has been established, an MLD with OCVC determines operating channel information from the receipt of the channel information included in the Supported Operating Classes element of protected Beacon frames on each setup link.

A STA or STA affiliated with an MLD with OCVC(#3505) validates that the channel information matches its current operating channel parameters by:

* Verifying that the maximum bandwidth used by the STA to transmit or receive PPDUs to/from the peer STA from which the channel information was received is no greater than the bandwidth of the operating class specified in the Operating Class field of the received channel information
* Verifying that the primary channel used by the STA to transmit or receive PPDUs to/from the peer STA from which the channel information was received is equal to the Primary Channel Number field (for the corresponding operating class)
* Verifying that, when 40 MHz bandwidth is used by the STA to transmit or receive PPDUs to/from the peer STA from which the channel information was received, the nonprimary 20 MHz used matches the operating class (i.e., upper/lower behavior) specified in the Operating Class field of the received channel information
* Verifying that, if operating an 80+80 MHz operating class, the frequency segment 1 channel number used by the STA to transmit or receive PPDUs to/from the peer STA from which the channel information was received is equal to the Frequency Segment 1 Channel Number field of the channel information.

If the NT-MLME of a STA with OCVC(#3505) processes an MMPDU containing OCI received in an MLME-OCTunnel.indication primitive (see 11.31.5 (On-channel Tunneling (OCT) operation)):

* The above validation is performed with respect to the expected or current channel used by the STA to transmit or receive PPDUs to/from the peer STA over the WM (i.e., not using the OCT procedure), and
* In addition, the STA verifies that the OCI contains the OCT Operating Class, OCT Primary Channel Number and OCT Frequency Segment 1 Channel Number fields, and uses the OCT information in those fields to perform the above validation with respect to the channel used by the STA corresponding to the TR-MLME from which the MLME-OCTunnel.indication primitive was received to transmit or receive PPDUs containing On-channel Tunnel Request frames to/from the STA corresponding to the TR-MLME used by the peer STA.

(#3334)If a STA or STA affiliated with an MLD with OCVC(#3505) receives a frame from (#1414)a peer STA that is not on the same channel used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.

### Comment

Not related to a CID, but I received comments offline asking to clarify the text describing Supplicant verification of Message 3 of the 4-way handshake.

### Discussion:

* Here is the text describing the content of EAPOL-Key Message 3 for the Authenticator:

A close-up of a white background

Description automatically generated

A screenshot of a computer program

Description automatically generated

….

A close-up of a computer screen

Description automatically generated

* Here is the text for Supplicant processing:

A close up of a document

Description automatically generated

* It would be good to clarify that the Authenticator provides a MLO Link KDE for all of its affiliated APs, and the Supplicant verifies the RSNE and RSNXE for all of the links that it has discovered to confirm that the Authenticator sending message 3 is the MLD that is advertising the RSNE and RSNXE.

### Proposed Text Changes not related to a CID:

Instruct the Editor to update the P802.11be draft to clarify the 4-way handshake message 3 processing for MLO. Update the draft with the following changes relative to D5.0:

At 437.38 change:

"For MLO, an MLO Link KDE containing the LinkID field, the affiliated AP MAC address, and the RSNE and RSNXE (if present)"

to

"For MLO, an MLO Link KDE for each affiliated AP containing the LinkID field, the affiliated AP MAC address, and the RSNE and RSNXE (if present)"

At 438.1, change

"For MLO, verify that the RSNE and if present, RSNXE for each setup link:"

to

"For MLO, verifies that"

At 438.3, change "If this message 3..." to "If message 3..."

At 438.14, change "If the message 3..." to "If message 3..."

At 438.18, change "The Supplicant verities that the affiliated..." to "The affiliated..."