IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe SA2 Security Comment Resolutions | | | | |
| Date: 2024-06-14 | | | | |
| 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 D6.0, mainly on Clause 12. The resolutions will be shown relative to TGbe D6.0 and REVme D6.0.

CIDs 23143, 23144, 23078, 23079, 23105, 23077, 23075, 23169, 23047, 23076

Rev 0. Initial submission

Rev 1.

Rev 2.

Rev 3.

Rev 4.

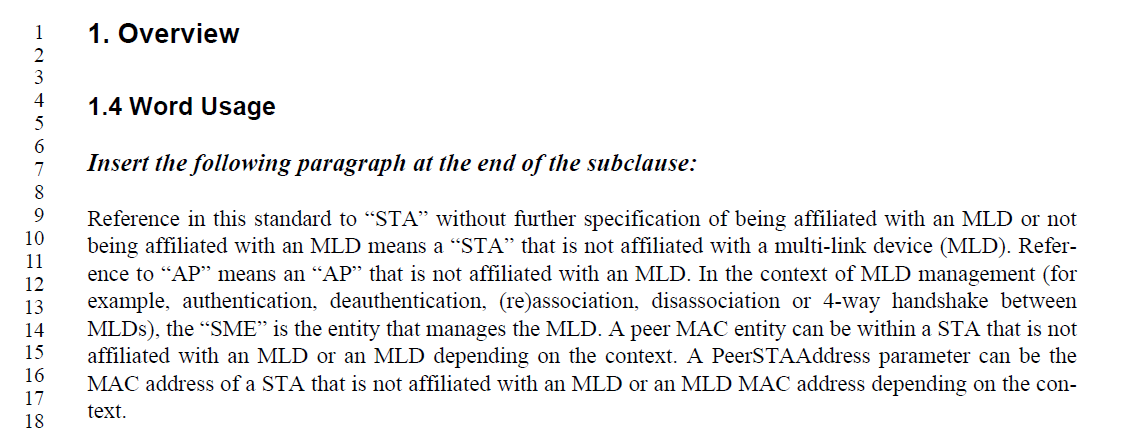
Rev 5.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 23143 | 1 | 51.07 | This does not belong in 1.4. This is not about word usage (shall, may and should). It seems to contain technical details that likely belong in a normative clause. | Delete changes to 1.4 |

### Discussion:

* The cited text (at 51.07) is:



* The cited text clarifies the usage of terms STA, AP, and MLD. Given that this text is important to interpreting requirements described in the amendment, it cannot be removed.

### Proposed Resolution (23143):

REJECTED. The text clarifies the usage of terms STA, AP and MLD and is important to interpreting requirements described in the amendment.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23144 | 2 | 53.09 | RFC 7296 does not appear to be properly cited in normative text. Only reference to [B14] which is correct for informative text e.g.: (page 197, line 51); In 9.4.2.313 (page 244, line 8) in an informative statement (which maybe you meant to be normative?); 12.4.4.1(page 415, line 51) in informative text; 12.10.2 in informative text; 12.11.2.3.2 in informative text; and lastly in Annex C which may be meant to be normative, but the reference is not properly cited. | Remove from clause 2 |

### Discussion:

* The cited text is:

A close-up of a computer code

Description automatically generated

* The reference replaces the normative reference for IKEv1 (RFC 2409) with IKEv2 (RFC 7296).
* The commenter references the following text:A screenshot of a computer code

  Description automatically generated

A close-up of a document

Description automatically generated

A screenshot of a document

Description automatically generated

* In the baseline, the beginning of clause 9 indicates that all format descriptions in the clause are normative:

### Proposed Resolution: (23144)

REJECTED. In the IEEE 802.11 standard, all field format descriptions in clause 9 are normative as indicated in clause 9.1 of the baseline. The normative reference to RFC 7296 replaces the normative reference to RFC 2409 in the baseline.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23078 | 12.2.9 | 411.49 | The note about each affiliated STA advertising OCVC could be misinterpreted to claim that non-AP MLD must have OCVC. | At P411 L49, replace "Each STA affiliated with an MLD advertises OCVC capability in the RSNE" with "When OCVC is present in an MLD, each STA affiliated with the MLD advertises OCVC capability in the RSNE". |
| 23079 | 12.2.9 | 411.49 | The last C in OCVC stands for "capability", so it should not be followed by a separate word "capability". | On P411 L49, replace "OCVC capability" with "OCVC" |

### Discussion:

* Cited text is:

A close-up of a document

Description automatically generated

* The commenter proposes changing the note to the following, which looks reasonable:

“NOTE—When OCVC is present in an MLD, each STA affiliated with the MLD advertises OCVC in the RSNE.”

### Proposed Resolution:

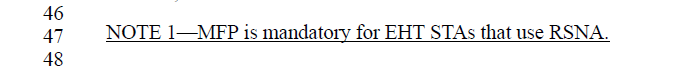
**(23078, 23079)** ACCEPTED.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23105 | 12.6.3.1 | 429.47 | The IEEE SA Standards Board Operations Manual, 6.4, states that notes are informative. Thus this statement is NOT stating a mandatory requirement. I cannot find where this requirement is stated. Is something missing? | Delete note |

### Discussion:

* Cited text in context:



* The cited note is informative as the commenter suggests and is not stating a mandatory requirement. The mandatory requirement is given in 12.12.9. Beacon protection is required to be enabled, which requires MFP to be enabled.

### Proposed Resolution: (23105)

REJECTED. The cited note is informative as the commenter suggests and is not stating a mandatory requirement. The mandatory requirement is given in 12.12.9. Beacon protection is required to be enabled for EHT STAs, and enabling beacon protection requires MFP to be enabled.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23077 | 12.7.6.1 | 437.11 | The changes to the EAPOL-Key contents have not followed the design changes from REVme correctly (and well, even REVme seems to have one issue there). In addition, this does not match the REVme baseline (OCI missing from message 2). | At P437 L12, replace "[,MAC Address])" with "[,MAC Address]})" (i.e., add the missed '}'). At P437 L15, replace "{RSNE [,RSNXE]} [, MAC Address, MLO Link\_n])" with "{RSNE [,RSNXE][, OCI]] [, MAC Address, MLO Link\_n]})" (i.e., move '}' to the end to include all KDEs and elements in Key Data and bring back the OCI from baseline, but move it to the correct location to be within the '{..}' list). |
| 23075 | 12.7.6.1 | 437.13 | The EAPOL-Key notation for Message 2 is incorrect. OCI is missing, the MLO KDE's are not included as part of key data (i.e. in the {…}), and finally, the 11bh KDEs are missing. | Incorporate the changes under "Updates to P802.11be D6.0:" in https://mentor.ieee.org/802.11/revise-document?t=9329800040%7F4 |
| 23169 | 12.7.6.1 | 437.14 | Message 2 should include [, OCI]. | Add [, OCI] to Message 2 |

### Discussion:

* The cited text is

A screenshot of a computer program

Description automatically generated

* As part of aiding the editors of P802.11be and P802.11bh with REVme roll-in prior to the completion of SA ballot recirculation, the following document with updates to the EAPOL-Key notation were posted in: <https://mentor.ieee.org/802.11/dcn/24/11-24-0298-04-00be-tgbe-sa1-eapol-key-notation-cleanup.docx>
* The changes suggested in the proposed change for these comments were already implemented in that document.

### Proposed Resolution: (23077, 23075, 23169)

ACCEPTED.

Note to editor: The text changes are captured in <https://mentor.ieee.org/802.11/dcn/24/11-24-0298-04-00be-tgbe-sa1-eapol-key-notation-cleanup.docx> after “***Updates to P802.11be D6.0:***”

### Comment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23047 | 12.7.6.1 | 437.45 | It would be better to put the "[, a]" notation at the end of the bulleted list so it stands out more. | Move the cited bullet to the end of the list. |

### Discussion:

* The cited text is:

A document with text on it

Description automatically generated

* It would be better to include the EAPOL-Key notation statement at the end of the list.

### Proposed Resolution: (23047)

ACCEPTED.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 23076 | 12.7.7.1 | 444.42 | EAPOL-Key notation is used incorrectly here (both in REVme baseline and for the new additions in 802.11be). All KDEs and elements are supposed to be within the { .. } block. | At P444 L42, replace "{[GTK(N)] [, OCI} [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)][, WIGTK(R, WIPN)] [, MLO GTKn] [, MLO IGTKn] [, MLO BIGTKn])" with "{[GTK(N)] [, OCI] [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)][, WIGTK(R, WIPN)] [, MLO GTKn] [, MLO IGTKn] [, MLO BIGTKn]})", i.e., move '}' to the correct place at the end of the list (and use ']' with OCI correctly to fix the REVme issue). |

### Discussion:

* The cited text is

A close-up of a computer code

Description automatically generated

* The proposed changes suggested by the commenter would change the cited text to:

EAPOL-Key(1,1,1,0,G,0,Key RSC,0, MIC, {GTK(N) [, OCI] [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, MLO GTKm] [, MLO IGTKn] [, MLO BIGTKn])

### Proposed Resolution: (23076)

ACCEPTED