IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed resolution for miscellaneous LB270 comments – Part 4 |
| Date: 2023-01-09 |
| Author: |
| Name | Affiliation | Address | Phone | Email |
| Edward Au | Huawei Technologies | Ottawa, Ontario, Canada |  | edward.ks.au@gmail.com  |

##### This submission present proposed resolutions for the following 10 ED2 CIDs and 1 GEN CID:

ED2: 3234, 3661, 3727, 3117, 3116, 3686, 3208, 3295, 3241, 3461

GEN: 3613

##### The proposed changes are based on REVme/D2.0.

##### Revision history:

##### R0 – Initial version

##### R1 – Updated the proposed resolution of a few CIDs based on the offline comments received from Mark Rison.

##### R1 – Updated the proposed resolution of a few CIDs during the January 9th teleconference. Proposed resolutions of CIDs 3683 and 3725 are removed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3234 | 12.7.2 | 2901 | 29 | Material on behaviour on reception of an receives an EAPOL-Key request frame should be moved to the subclause on rekeying (12.6.21) | Move lines 29-58 on page 2901 to the end of 12.6.21 |

***Discussion:***

Original text at 2901.29 in subclause 12.7.2 (EAPOL-Key frames) of D2.0:



***Proposed resolution for CID 3234:***

Accepted

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3661 | 12 |  |  | Figure 12-23--CCMP decapsulation block diagram is still fuzzy | De-fuzz it (or take the GCMP one and adapt it for GCMP) |

***Discussion:***

**Original figure at 2843.14:**



IMHO, the figure in D2.0 was not fuzzy but the Editor is willing to generate the emf of the figure again. The commenter is encouraged to provide a new figure by themselves if the figure in the next draft is still fuzzy.

***Proposed resolution for CID 3661:***

Revised.

Editors to regenerate the emf from the visio source of Figure 12-23 and insert the new emf to the draft standards.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3727 | 13.9.3.1 | 2997 | 41 | "PTK= Calc FT-PTK ()" should be "PTK = Calc FT-PTK ()" (space before =) | Add space before = |

***Discussion:***

**Portion of the original figure at 2997.41 in D2.0:**



***Proposed resolution for CID 3727:***

Accepted.

Note to the Editors: The Visio source file is Figure\_13\_14.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3117 | B.4.4.1 | 4639 | 56 | There are locations where the counters are referred to using the field name capitalization. This is not in line with the style of the 802.11 specification. Counters should use lower case names, Fields and elements using the term "Counter' in their name should be capitalized. | Replace: "(#1912)Counter Mode with cipherblock chaining message authentication code protocol (CCMP) data confidentiality protocol using CCMP-128"With: "(#1912)Counter mode with cipherblockchaining message authentication code protocol (CCMP) data confidentiality protocol using CCMP-128"Also the following similar changes should be made:4640.30 Replace: "(#1912)Galois/Counter Mode protocol (GCMP)" with "(#1912)Galois/counter mode protocol (GCMP)" |

***Discussion:***

**Original text at 4639.56 in D2.0:**



**Original text at 4640.30 in D2.0:**



“Galois/Counter Mode” is a specific term from the specification, NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Dworkin, M., Nov. 2007.

***Proposed resolution for CID 3117:***

Rejected.

“Galois/Counter Mode” is a specific term from the specification, NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Dworkin, M., Nov. 2007.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3116 | 29.9.3 | 4568 | 35 | There are locations where the counters are referred to using the field name capitalization. This is not in line with the style of the 802.11 specification. Counters should use lower case names, Fields and elements using the term "Counter' in their name should be capitalized. | Replace "A WUR AP shall maintain a BSS Parameter Update Counter. The WUR AP shall increase the BSS Parameter Update Counter if a critical update ..." with "A WUR AP shall maintain a BSS parameter update counter. The WUR AP shall increase the BSS parameter update counter if a critical update ..."Also the following similar changes should be made:4568.58 Replace "... the current value of the BSS Parameter Update Counter in ..."with "... the current value of the BSS parameter update counter in ..."4568.60 Replace "... if the Counter value in the WUR Operation element ..." with "... if the Counter subfield value in the WUR Operation element ..."4568.63 Replace "A WUR non-AP STA shall maintain a BSS Parameter Update Counter. The WUR non-AP STA shall update its BSS Parameter Update Counter to the Counter subfield contained in the latest WUR Operation element ..." with "A WUR non-AP STA shall maintain a BSS parameter update counter. The WUR non-AP STA shall update its BSS parameter update counter to the Counter subfield contained in the latest WUR Operation element ..."4570.4 Replace "... different from its BSS Parameter Update Counter shall follow ..." with "... different from its BSS parameter update counter shall follow ..." |

***Discussion:***

**Original text at 4568.35 in D2.0:**



Agree with the commenter to

* replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4568.35;
* replace “the BSS Parameter Update Counter” with “the BSS parameter update counter” at 4568.36.

**Original text at 4568.58 in D2.0:**



Agree with the commenter to

* replace “the BSS Parameter Update Counter” with “the BSS parameter update counter” at 4568.58;

Agree in principle with the commenter to

* replace “the Counter value” with “the Counter subfield value” at 4568.60 but the phrase “value” is not needed, i.e., replace “the Counter value” with “the Counter subfield”.

**Original text at 4568.63 in D2.0** [The commenter cites 4568.63 for the description of the WUR non-AP STA but this paragraph is about the WUR AP STA]:



Agree with the commenter to

* replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4568.58;

**Original text at 4569.63 in D2.0** [The commenter’s proposed changes on the WUR non-AP STA are located at 4569.63, not 4568.63 identified by the commenter]:



Agree with the commenter to

* replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4569.63;
* replace “its BSS Parameter Update Counter” to “its BSS parameter update counter” at 4569.64.

**Original text at 4570.4 in D2.0:**



Agree with the commenter to

* replace “its BSS Parameter Update Counter” to “its BSS parameter update counter” at 4570.4.

***Proposed resolution for CID 3116:***

Revised.

Replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4568.35;

Replace “the BSS Parameter Update Counter” with “the BSS parameter update counter” at 4568.36.

Replace “the BSS Parameter Update Counter” with “the BSS parameter update counter” at 4568.58;

Replace “the Counter value” with “the Counter subfield” at 4568.60.

Replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4568.58;

Replace “a BSS Parameter Update Counter” with “a BSS parameter update counter” at 4569.63;

Replace “its BSS Parameter Update Counter” to “its BSS parameter update counter” at 4569.64.

Replace “its BSS Parameter Update Counter” to “its BSS parameter update counter” at 4570.4.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3686 | 12 |  |  | "Length", including in "KDF-Hash-Length", in 12.7.1.6.3 PMK-R0 should be italic, also in 12.7.1.6.4 PMK-R1, 12.7.1.6.5 PTK, 12.7.8.2 TPK handshake; in .6.4 and .8.2 Length should be explicitly defined too; in .8.2. "that uses Hash to generate a key whose length is TK\_bits + 128" should be "using the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors))" | As it says in the comment |

***Discussion:***

**First item of the comment:**

"Length", including in "KDF-Hash-Length", in 12.7.1.6.3 PMK-R0 should be italic, also in 12.7.1.6.4 PMK-R1, 12.7.1.6.5 PTK, 12.7.8.2 TPK handshake

* In subclause 12.7.1.6.3 of D2.0, “Length”, including in “KDF-Hash-Length”, is already italic (two appearances)
* In subclause 12.7.1.6.4 of D2.0, “Length”, including in “KDF-Hash-Length”, is already italic (two appearances)
* In subclause 12.7.1.6.5 of D2.0, two out of four appearances of “Length”, including in “KDF-Hash-Length”, are already italic. The two non-italic ones are located at 2897.44 and 2897.48.
* In subclause 12.7.8.2 of D2.0, “Length”, including in “KDF-Hash-Length”, is already italic (two appearances)
* In subclause 12.11.2.5.3 of D2.0, which is not a subclause pointed out by the commenter, all appearances of “Length”, including in “KDF-Hash-Length”, are not italic. The locations are 2958.7 and 2958.12.

**Second item of the comment:**

in .6.4 and .8.2 Length should be explicitly defined too;

* In subclause 12.7.1.6.4 of D2.0, “Length” is defined at 2896.26 as follows:



* In subclause 12.7.8.2 of D2.0, “Length” is defined at 2927.60 as follows:



**Third item of the comment:**

in .8.2. "that uses Hash to generate a key whose length is TK\_bits + 128" should be "using the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors))"

* In subclause 12.7.8.2 of D2.0, the phrase “that uses Hash to generate a key whose length is TK\_bits + 128” does not exist. At 2927.60, Hash is defined as the hash algorithm specific to the negotiated AKM (see Table 9-188 (AKM suite selectors)).

***Proposed resolution for CID 3686:***

Revised.

At 2897.44, 2897.48, 2958.7, and 2958.12, replace “KDF-Hash-Length” with “KDF-*Hash*-*Length*” (i.e., change the style of “Hash” and “Length” from non-italic to italic.

At 2818.38, 2889.37, 2889.42, 2889.46, 2895.42, 2896.26, 2897.6, 2897.52, 2927.60, 2928.24, 2958.16, and 3041.27, replace “Length” with “*Length*” (i.e., change the style of “Length” from non-italic to italic).

At 2896.24 and 2927.55, replace “Hash” with “*Hash*” (i.e., change the style of “Hash” from non-italic to italic).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3208 | 12.4.8.1 | 2827 | 37 | "Zero(Rc)" should be "zero(Rc)" in Figure 12-15--SAE finite state machine. Ditto "Big(" should be lowercase | As it says in the comment |

***Discussion:***

**Original figure at 2827.4 in D2.0:**

“Zero(Rc)” is located at 2827.12. “Big(Rc)” is located at 2827.30. Agree with the commenter on the proposed changes.



***Proposed resolution for CID 3208:***

Accepted.

Note to the Editors: The Visio source file is Figure\_12\_4.

Note to the Editors: The locations are 2827.12 and 2827.30 in D2.0

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3295 | 11.20.3 | 2555 | 29 | MLME-DLSSETUP in Figure 11-35--TDLS direct-link establishment should be MLME-TDLSSETUP | As it says in the comment |

***Discussion:***

**Original figure at 2555.1 in D2.0:**

Agree with the commenter on the proposed change at 2555.29 to replace “MLME-DLSSETUP” with “MLME-TDLSSETUP”.



***Proposed resolution for CID 3295:***

Accepted.

Note to the Editors: The Visio source file is Figure\_11\_30c.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3241 | 12.7.8.4 |  |  | RSNE fields should be referred to by their name, not by paraphrasing | As it says in the comment |

***Discussion:***

None.

***Proposed resolution for CID 3241:***

Revised. Incorporate the changes as shown in CID 3241 in https://mentor.ieee.org/802.11/dcn/22/11-22-2210-02-000m-proposed-resolution-for-miscellaneous-lb270-comments-part-4.docx.

At 2929.7 (in subclause 12.7.8.4.2), changes as follows:

The Version field shall be set to 1.

The Pairwise Cipher Suite Count and Pairwise Cipher Suite List fields shall indicate the pairwise cipher suites the TDLS initiator STA is willing to use with the TPKSA. WEP-40, WEP-104, and TKIP shall not be included in this list.

The Group Data Cipher Suite field shall be set to 00-0F-AC:7.

The AKM Suite Count field shall be set to 1.

The AKM Suite List field shall be set to indicate TPK handshake (00-0F-AC:7).

In the RSN Capabilities field, the No Pairwise subfield shall be set to 0 and the PeerKey Enabled subfield shall be set to 1.

The PMKID Count field, if present, shall be set to 0.

The PMKID List field shall not be present.

The Group Management Cipher Suite field, if present, shall be set to 00-0F-AC:7.

At 2930.15 (in subclause 12.7.8.4.3), changes as follows:

Version fieldset to

The Pairwise Cipher Suite List field shall indicate one of the pairwise cipher suites presented in the RSNE of message 1 in the pairwise cipher suite list, and the Pairwise Cipher Suite Count field shall be set to 1.

All other RSNE fields shall be same as those received in message 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3461 | 11.20.6.1 | 2560 | 36 | The "DL"s in Figure 11-35--Events occurring for a TDLS direct link channel switch(#1356) are confusing because they don't mean downlink, they mean direct link | Change to "direct link"s at lines 36 and 52 |

***Discussion:***

**Portion of the original figure at 2560.36 in D2.0:**

Agree with the commenter on the proposed changes at 2560.36 and 2560.52 to replace “DL” with “direct link”.



***Proposed resolution for CID 3461:***

Accepted. Note to the Editor: It is Figure 11-36, not Figure 11-35.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 3613 | 4 |  |  | "A DMG BSS is a QoS BSS." might be better (a) not just in Clause 4 and (b) with a tie-in to dot11QoSOptionImplemented | Add a statement to that effect in Clause 10, mentioning dot11QoSOptionImplemented |

***Discussion:***

Original text at 265.63 in subclause 4.3.10 (QoS BSS) of D2.0:



***Proposed resolution for CID 3613:***

Revised.

Insert the following sentence as the first paragraph of subclause 10.14 (DMG A-PPDU and EDMG A-PPDU operation) at 1873.18 in D2.0:

A DMG STA is a QoS STA and shall set dot11QosOptionImplemented to true.