IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed resolution for miscellaneous LB258 comments |
| Date: 2022-06-10 |
| Author: |
| Name | Affiliation | Address | Phone | Email |
| Edward Au | Huawei Technologies | Ottawa, Ontario, Canada |  | edward.ks.au@gmail.com  |

##### This submission present proposed resolutions based on the offline comments received from Mark Rison for the following 8 CIDs:

1441, 1442, 1774, 1831, 1909, 1912, 2137, 2164

##### The proposed changes are based on REVme/D1.0.

##### Revision history:

##### R0 – initial version

R1 – Proposed resolution for CIDs 1441, 1442, 1831, and 2164 are updated based on further offline comments from Mark.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 1441 | 12.6.21 | 3186 | 43 | “authenticator” should be uppercase | Change to “Authenticator” at the referenced location and at 3152.50 |
| 1442 | 12.6.21 | 3186 | 43 | “authenticator” should be uppercase | Change to “Authenticator” in all locations where it is improperly lowercase |

***Discussion:***

From Mark Rison’s message: locations are 191.27 (discuss), 250.15/60 (discuss), 1339.30 (2x), 1580.14, 3152.46/49/52, 3180.38, 3186.43, 5387.14/16/17.

At 191.27:

**authenticator address (AA):** The medium access control (MAC) address of the IEEE 802.1X Authenticator’s station (STA).

At 250.15/60:

AA authenticator address

ANonce authenticator nonce

From Mark Rison’s additional offline message, we also change “supplicant” to “Supplicant” for the sake of consistency.

***Proposed resolution for CID 1441:***

Revised.

Change “authenticator” to “Authenticator” at 191.27, 250.15/60, 1339.30 (2x), 1580.14, 3152.46/49/52, 3180.38, 3186.43, 5387.14/16/17.

Change “supplicant” to “Supplicant” at 261.51/55, 3186.43, 3295.44, and 6028.37/41/52.

***Proposed resolution for CID 1442:***

Revised.

Change “authenticator” to “Authenticator” at 191.27, 250.15/60, 1339.30 (2x), 1580.14, 3152.46/49/52, 3180.38, 3186.43, 5387.14/16/17.

Change “supplicant” to “Supplicant” at 261.51/55, 3186.43, 3295.44, and 6028.37/41/52.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 1774 | J |  |  | CCMP nonce (3x) and CCMP-256 Nonce should be just CCM Nonce. Ditto GCMP Nonce should be GCM Nonce | As it says in the comment |

***Discussion:***

From Mark Rison’s review: locations are 5945.14, 5946.5/59, 5947.29, 5959.49.

***Proposed resolution:***

Accepted.

Note to the Editors: The locations of D1.0 are 5945.14, 5946.5/59, 5947.29, and 5959.49.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 1831 | 12 |  |  | “When the negotiated AKM is 00-0F-AC:14, 00-0F-AC:15, 00-0F-AC:16, or00-0F-AC:17, this Key MIC bit is set to 0 regardless of the M parameter value.” -- other places refer to “using an AEAD cipher” -- be consistent | Change to saying “using an AEAD cipher” -- I can provide locations |

***Discussion:***

From Mark Rison’s review: locations are 3208.1 (in 22/0353 for CID 1823), 3214.41/58.

For the location at 3208.1, it will be resolved by 22/0353.

***Proposed resolution:***

Revised.

Change “When the negotiated AKM is 00-0F-AC:14, 00-0F-AC:15, 00-0F-AC:16, or 00-0F-AC:17, this Key MIC bit is set to 0 regardless of the M parameter value.” to “When using an AEAD cipher” at 3214.41/58 in D1.0.

Note to the commenter: The main reason it is revised because the commenter asked to replace the identified text with “using an AEAD cipher” without “When”.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 1909 |  |  |  | “uncontrolled port”, “controlled port”, “Uncontrolled port”, “Controlled port” should have initial caps (~20x) | I can provide locations |

***Discussion:***

From Mark Rison’s review: locations are 269.31 (2x), 339.22, 340.15 (2x), 341.31, 343.12 (2x), 355.19 (2x), 356.15 (2x), 357.30, 359.19 (2x), 3087.1, 3176.43, 6040.56,

***Proposed resolution:***

Accepted.

Note to the Editors: The locations of D1.0 are 269.31 (2x), 339.22, 340.15 (2x), 341.31, 343.12 (2x), 355.19 (2x), 356.15 (2x), 357.30, 359.19 (2x), 3087.1, 3176.43, and 6040.56.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 1912 |  |  |  | “counter mode” (or “Counter mode”) is an external reference so should be “Counter Mode” | I can provide locations |

***Discussion:***

From Mark Rison’s review: locations are 2.12, 193.15/16 (discuss), 223.37/38/52/53, 239.42/43, 252.36 (discuss), 272.51/52, 4939.56, 4940.29.

At 193.15/16:

**counter mode with cipher-block chaining message authentication code (CCM):** A symmetric key block cipher mode providing confidentiality using counter mode (CTR) and data origin authenticity using cipherblock chaining message authentication code (CBC-MAC).

NOTE—See IETF RFC 3610.

At 252.36:

CTR counter mode

***Proposed resolution:***

Revised.

Note to the Editors: The locations of D1.0 are locations are 2.12, 193.15/16 (discuss), 223.37/38/52/53, 239.42/43, 252.36 (discuss), 272.51/52, 4939.56, 4940.29.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 2137 |  |  |  | “a NDP” should be “an NDP” | I can provide locations |

***Discussion:***

From Mark Rison’s review - location are 2353.25, 3537.49, 3603.7/9, 3988.1, 4096.51, 4097.39.

***Proposed resolution:***

Accepted.

Note to the Editors: The locations of D1.0 are 2353.25, 3537.49, 3603.7/9, 3988.1, 4096.51, and 4097.39.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| 2164 |  |  |  | “the Interworking capabilities of STA” (multiple) should be “the interworking capabilities of the STA” | I can provide locations |

***Discussion:***

From Mark Rison’s review - locations are 399.41, 469.19. Also 5079.12 should be lowercase “information” and 5676.58 lowercase “interworking”.

***Proposed resolution:***

Revised.

At 399.41 and 469.19 in D1.0, replace “the Interworking capabilities of STA” with “the interworking capabilities of the STA”.

At 5079.12, replace “Information” with “information”.

At 5676.58, replace “Interworking capabilities” with “interworking capabilities”.

At 5676.59, replace “Interworking Capability” with “Interworking capability”.