IEEE P802.11
Wireless LANs

|  |
| --- |
| LB236 additional comment resolutions  |
| Date: 2019-07-04 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Michael Montemurro | BlackBerry Ltd | 4701 Tahoe Blvd, Mississauga, ON. CANADA. L4W 0B4 | +1-289-261-4183 | mmontemurro@blackberry.com  |

##

**Abstract**

This document contains some proposed resolutions to REVmd LB236 comments. The proposed resolutions incorporate review comments from Dan Harkins and Jouni Malinen.

# Comments

### CID 2198

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2198 | 456.00 | 6.3.31.3.2 |  |  | What information is in the dot11RMNeighborReportTable is not clearly defined. How the information gets into the table and what information should be put into the table is not defined. The actual allowed content of the table seems to only be defined by a list of MIB variables in the MIB. In "11.10.10 Usage of the neighbor report" the ot11RMNeighborReprotTable is not mentioned and the specification states "The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS." I assume the table referred to above is the dot11RMNeighborReportTable but it is not named. Outside of the MIB dot11RMNeighborReportTable is only used in "4.3.11.10 Neighbor report" and "6.3.31.3 MLME-NEIGHBORREPRESP.indication". Hence, this reference needs to be clarified in 4.3.11.10 and 6.3.31.3. | In 6.3.31.3.2 remove the reference to dot11RMNNeighborReport.Replace:A set of Neighbor List elements derived from theMIB table dot11RMNeighborReportTable, eachrepresenting a neighboring AP being reported asdefined in the Neighbor Report element format.With:A set of Neighbor List elements for each for the neighboring APs being reported on as described in 11.10.10.3 and defined in the Neighbor Report element format.If this deletion of this MIB variable is of concern, it should probably be introduced into section 11.10.10 where the Neighbor report details are. |

#### Discussion:

* The commenter is correct in stating that the primitive indicates that the NeighborListSet appears to be derived from the dot11RMNeighborReportTable.
* Populating the neighbor list using a network management interface is valid and there are implementations that make use of that method.
* The text in 11.10.10 “The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.”
* Propose to adopt the alternative in the Proposed resolution.
* Assign to Joseph Levy.

#### Proposed Resolution:

Revised. Relative to D2.0,

In 6.3.31.3.2 remove the reference to dot11RMNNeighborReport.
Replace:
“A set of Neighbor List elements derived from the MIB table dot11RMNeighborReportTable, each representing a neighboring AP being reported as defined in the Neighbor Report element format.”
With:
“A set of Neighbor List elements for each for the neighboring APs being reported on as described in 11.10.10.3.”

At p2282.10, replace:

“The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.”

With:

“The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information provisioned in dot11RMNeighborReportTable, or the DS.”

### CID 2436

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2436 |  |  |  |  | It is not clear whether Robustness of Management frames is a capability (MMPDU \*can\* be protected if PMF was negotiated) or a stated (PMF was negotiated and MMPDU is protected). E.g. the definition "A Management frame that is eligible for protection." suggests the former, while 4.3.8's "Enhanced cryptographic encapsulation mechanisms for robust Management frames" suggests the latter. Some places use expressions like "protected robust Management frame", which both suggests the former and provides a way to distinguish the capability ("robust") from the actuality ("protected robust") | Add "protected" before "robust Management" throughout where not already present |

#### Discussion:

* There are 163 occurences of “robust management frame in the standard.
* There are 9 occurences of “protected robust management frame” (relative to D2.0):
	+ 269.40: “Unprotected Data frames and unprotected robust Management frames received at a STA configured for mandatory data confidentiality, as well as protected Data frames and protected robust management frames are discarded…”
	+ 270.4: “a STA that receives a Data or protected robust Management frame can determine …”
	+ 270.17: “STA that receives a Data or protected robust Management frame from …”
	+ 2568.9: “The transmitter shall preserve the order of protected robust Management frames that are…”
	+ 2572.27: “The transmitter shall preserve the order of protected robust Management frames that are…”
	+ 2576.51: “The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected robust Management frames. …”
	+ 2585.20: The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected robust Management frames.”
	+ 2587.12: “The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow data traffic and protected robust Management frames.
	+ These occurences refer to frames that are encrypted.
* PMF includes two features: encryption of unicast management frames using the IGTK, and integrity protection of group addressed management frames using BIP.
* The usage of “protected robust Management frames” refers to frames that have been encrypted. That’s why “protected” is used to indicate encryption. Encrypted frames have the “protection” field set in the header.
* Assign to Jouni Malinen

#### Proposed Resolution:

Rejected. PMF negotiation supports integrity protection of group-addressed MMPDUs and encryption of unicast MMPDUs. The term “protected robust Management frames” refers to MMPDUs that have been encrypted. “robust Management frames” refers to both unencrypted and encrypted MMPDUs.

### CID 2440

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2440 |  | 12.7 |  |  | Key Data Length can't be 0 if there is something in the Key Data field. And if you list the contents it should cover all the possible contents | Delete "Key Data Length = length of Key Data field in octets" in 12.7.6.2/3/5, "Key Data Length = length of Key Data field in octets of included RSNEs and GTK" in 12.7.6.4, "Key Data Length = Cipher-suite dependent(#1408); see Table 12-5 (Cipher suite key lengths)" in 12.7.7.2, "Key Data Length = 0" in 12.7.7.3 |

#### Discussion:

* The cited sections document the contents of each of the IEEE 802.1X EAPol-Key fields in the 4-way handshake and the GTK handshake.
* The information on each field contents (including the Key Data Length value) has proved to be extremely useful in the past in implementing and debugging the 4-way handshake and group key handshake.
* There is an error in 12.7.6.5 (p2632.19) because there are no KDEs included in MSG 4.

*Key Data Length = length of Key Data field in octets*

*Key Data = none required*

* There is also an error in 12.7.7.3 (p2638.9):

*Key Data Length = 0*

*Key Data = (M58)*

 *— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator(M58)*

* Feedback from Jouni:

“Regarding CID 2440, I don't like the direction of forcing EAPOL-Key msg 4/4 to have an empty Key Data field. While the standard does not define any specific use for that field, a vendor specific KDE or a Vendor-Specific element is allowed in the Key Data field of any EAPOL-Key messages, including EAPOL-Key msg 4/4. As such, the current text is correct (Key Data Length = length of Key Data field in octets, Key Data = none required) and I would not make the proposed change. I would have no objections to clarifications pointing out that vendor specific KDE/elements can be present, but the comment does not propose those, so I'd go with minimal changes here. The change on Group msg 2/2 looks correct, so that would remain.”

#### Proposed Resolution:

Revised. The cited clauses include the value of all fields of the IEEE 802.1X EAPoL key frame and provide guidance on the implementation of the key exchanges.

Relative to D2.0,

In clause 12.7.7.3, (p2638.10), replace:

“Key Data Length = 0

Key Data = (M58)

 — OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator(M58*)*”

With:

“Key Data Length = length of Key Data field in octets

Key Data = OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator”

At 2629.62, replace:

“Key Data Length = length of Key Data field in octets of included RSNEs and GTK”

With

“Key Data Length = length of Key Data field in octets”

At 2637.3, replace:

“Key Data Length = Cipher-suite dependent(#1408) ; see Table 12-5 (Cipher suite key lengths)”

With

“Key Data Length = length of Key Data field in octets”

### CID 2505

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2505 |  | 12 |  |  | "IPN integer value" -- it can hardly be a real complex value | Delete "integer" in "integer value" throughout Clause 12 |

#### Discussion:

* The locations are 2573.12, 2573.14, 2573.18, 2573.20, 2573.41, 2573.44
* At 2629.18, “initializes the SA Query Transaction Identifier to an implementation-specific non-negative integer value, …”, “integer” is required.

#### Proposed Resolution:

* Revised. Make the proposed change at the following locations: “2573.12, 2573.14, 2573.18, 2573.20, 2573.41, and 2573.44”

### CID 2509

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2509 |  | 12 |  |  | There are occasional references to "wrapped" keys, but it's not clear how these keys differ from keys elsewhere | In 9.4.2.47 change "wrapped IGTK" to "encrypted IGTK" and "AES-Key-wrapped IGTK" to "IGTK". In 12.6.1.1.10 change "wrapped MGTK" to "MGTK". In 9.4.2.47 change "Key Length field is" to "The Key Length field is" and "RSC field contains" to "The RSC field contains" |

#### Discussion:

* “Key-wrap algorithms” are cryptographic algorithms that are used to encrypt and integrity protect key material. Therefore the proposed change from “wrapped” to “encrypted” is incorrect.
* The second proposed change modifies this text:

“The Wrapped Key field contains the wrapped IGTK being distributed. The length of the resulting AES-Keywrapped IGTK in the Wrapped Key field is Key Length + 8 octets.(#102)”

* The two sentences are correct.
* A Key-wrap algorithm provides encryption as well as integrity protection
* At 1148.1, the “Wrapped key” field does contain the wrapped IGTK.
* The two editorial changes look to be correct.

#### Proposed Resolution:

Revised. Relative to D2.0,

Key-wrap algorithms are cryptographic algorithms that encrypt and integrity protect key material. Therefore the use of the term “wrapped” is correct.

The Key Wrap field does contain wrapped keying material so the current text is correct.

At p1148.1, change "Key Length field is" to "The Key Length field is" and "RSC field contains" to "The RSC field contains"

### CID 2565

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2565 |  |  |  |  | "packet number" should not be used as the term "packet" is imprecise | Change "packet number" to "frame number" throughout |

#### Discussion:

* There are 22 occurences of “packet number” in the draft and they all refer to cryptographic encapsulation.
* The use of “packet number” is precise when it refers to CCMP and GCMP encapsulation.
* CCMP uses CBC-MAC (RFC 3610) which uses the term “packet”. RFC 3610 is a normative reference to IEEE Std 802.11
* GCM encapsulation refers to NIST Special Publication 800-38D which uses the term packet. NIST Special Publication 800-38D is a normative reference to the IEEE Std 802.11.

#### Proposed Resolution:

Rejected. The term packet is precise when used in the context of cryptographic encapsulation. The term used consistently and is in line with normative references RFC3610 and NIST Special Publication 800-38D.