IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB273 Security Adhoc Comment Resolutions Part 1 | | | | |
| Date: 2023-12-04 | | | | |
| 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 selected REVme SEC adhoc comments from initial SA Ballot.

R0 – Initial version.

R1 –

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6240 |  | 12 |  |  | "group cipher suite" should be "group data cipher suite", or alternatively there should be a statement in 1.4 that it is to be understood as such | Po-Kai HUANG has done some work on this |
| 6241 |  | 12.6.3 |  |  | "It shall also specify the group cipher suite specified by the targeted AP." needs to consider both the data and management cipher suites, if MFP is negotiated | Change to "suite(s)" |

### Discussion:

* This comment was addressed in the resolution to CID 6020.

### Proposed Resolution: (6240, 6241)

REVISED. Incorporate the changes in 11-23/1745r1 <https://mentor.ieee.org/802.11/dcn/23/11-23-1745-01-000m-cr-for-cid-6020.docx>.

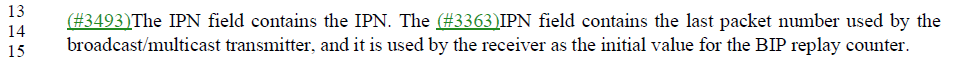
Note to editor: This comment is resolved by the changes in the resolution to CID 6020.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6606 | 2914.00 | 12.7.2 |  |  | "The IPN field contains the IPN. The (#3363)IPN field contains the last packet number used by the broadcast/multicast transmitter, and it is used by the receiver as the initial value for the BIP replay counter." seems garbled. It's clearer for the BIPN version: "The BIPN field contains the BIPN(#1422) that was carried in the MME of the last protected Beacon frame and it is used by the receiver as the initial value for the BIP replay counter for the BIGTK." | Change to "The IPN field contains the last IPN used by the transmitter, and it is used by the receiver as the initial value for the replay counter for the IGTK." At 2916.17/38 change "BIP replay counter" to "replay counter". At 2916.16/37 add a comma before "and it is used". |

### Discussion:

* The text referred to on 2914.13



* The text referred to on 2916

A screenshot of a computer

Description automatically generated

* The proposed text on page 2914 would be changed to: "The IPN field contains the last IPN used by the transmitter, and it is used by the receiver as the initial value for the replay counter for the IGTK."
* This change looks fine.
* The change on 2916 removes “BIP” from “BIP replay counter at two locations and adds a comment before “it is used” around the two locations.

### Proposed Resolution: (6606)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6605 | 2919.00 | 12.7.4 |  |  | "IPN is the current IGTK replay counter value provided by the IGTK KDE" is confusing. It is the value to which the IGTK RC is set to at the receiver, but it contains the IPN at the transmitter, as described in 12.7.2: "The IPN field contains the IPN. The (#3363)IPN field contains the last packet number used by the broadcast/multicast transmitter, and it is used by the receiver as the initial value for the BIP replay counter." | Change to "IPN is the last IPN, as provided by the IGTK KDE" |

### Discussion:

* The cited text where the proposed text changes are:

A close up of text

Description automatically generated

And

A close-up of a text

Description automatically generated

* The comment is requesting the following change:

Change

"IPN is the current IGTK replay counter value provided by the IGTK KDE"

to

“IPN is the last IPN, as provided by the IGTK KDE"

* The proposed change looks OK.
* Should likely change BIPN and WIPN in a similar way
* Note that this CID is similar to CID 6415, but the changes in CID 6415 and not clearly specified.

### Proposed Resolution: (6605)

REVISED. Make the changes proposed by the commenter. Also update BIPN and WIPN

At 2919.38 Change

“BIPN is the current BIGTK replay counter value provided by the BIGTK KDE"

to

“BIPN is the last BIPN, as provided by the BIGTK KDE"

At 2919.40 Change

“WIPN is the current WIGTK replay counter value provided by the WIGTK KDE"

to

“WIPN is the last WIPN, as provided by the WIGTK KDE"

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6386 |  | 12.7.6.4 |  |  | "OCI FTE subelement" -- no such subelement | At 2923.34, 2925.52 change to "OCI KDE or FTE OCI subelement is missing in the message" to "OCI KDE or OCI subelement is missing in the message or FTE respectively". At 4666.49 change "OCI FTE subelement" to "OCI subelement" |

### Discussion:

* The relevant text at 2923

A close-up of a message

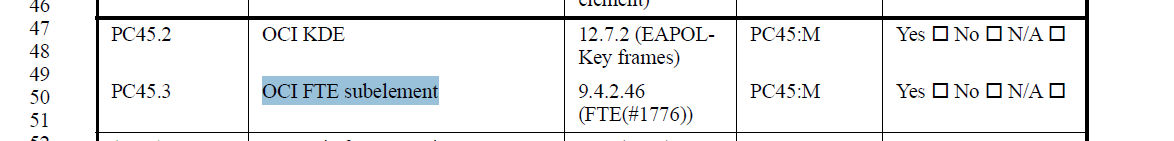
Description automatically generated

and at 2925

A close-up of a message

Description automatically generated

and at 4666



* Here is the OCI sub-element definition for the FTE:

A close-up of a chart

Description automatically generated

* The proposed changes clarify the OCI subelement in the FTE

### Proposed Resolution: (6386)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6308 | 2910.00 | 12.7.2 |  |  | "When replying to a message from the Authenticator, the Supplicant shall use the Key Replay Counter field value from the last valid (#1836)EAPOL-Key PDUs" should be "... PDU" | As it says in the comment |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

* There are two occurrences of EAPOL-Key PDUs in the paragraph and the commenter is referring to the first one. Agree with the recommended change

### Proposed Resolution: (6308)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6301 | 2999.00 | 13.8.1 |  |  | "The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element, and is present in the fourth message if an RSNXE was present in the third message and the target AP set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element." -- missing "otherwise not present" | As it says in the comment |

### Discussion:

* The cited text is the following:

A screenshot of a computer

Description automatically generated

* To be clearer to break this text into multiple paragraphs, see below:

“The RSNXE is present in the first message if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe

Response frame that the FTO has received from the target AP and the

FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element,

The RSNXE is present in the fourth message if an RSNXE was present in the third message and the target AP set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

Otherwise the RSNXE is not present.”

### Proposed Resolution: (6301)

REVISED. Make the changes proposed by the commenter but update the text into multiple paragraphs.

Change

“The RSNXE is present in the first message if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield; otherwise, not present. The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe

Response frame that the FTO has received from the target AP and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element, and is present in the fourth message if an RSNXE was present in the third message and the target AP set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

To

“The RSNXE is present in the first message if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe

Response frame that the FTO has received from the target AP and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element,

The RSNXE is present in the fourth message if an RSNXE was present in the third message and the target AP set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

Otherwise the RSNXE is not present.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6571 |  | 12.6.19 |  |  | "shall discard unprotected individually addressed robust Action frames received from any STA that advertised MFPC = 1" -- is this true for Class 1/2 Action frames? | Add a NOTE to say that there are no robust Class 1/2 Action frames |

### Discussion:

* After searching in the cited clause and the standard, the cited text does not appear. The comment does not give a page or line number in the comment.

### Proposed Resolution: (6571)

REJECTED. The cited text could not be found in the cited clause or anywhere else in the draft.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6084 | 2933.00 | 12.7.7.4 |  |  | The 100 ms retransmit timeout value for the first EAPOL-Key frame timeout is too short for some cases especially when there is a large number of associated or associating STAs. In particular, the group key handshake timeout can result in undesired retries since the AP will not be able to send out potentially hundreds of EAPOL-Key group msg 1/2 and receive the response msg 2/2 in that time. This timeout needs to be relaxed to allow more efficient and robust implementations to be compliant with the requirements. This comment proposes a simple shall-to-should way of doing this, but other approaches and potentially NOTEs to clarify this would be acceptable as well. | At P2933 L60 (group HS) and P2927 L35 (4-way HS) replace "The retransmit timeout value shall be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If there is no listen interval or the listen interval is zero, then 100 ms shall be used for all timeout values." with "The retransmit timeout value should be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If there is no listen interval or the listen interval is zero, then 100 ms should be used for all timeout values.". |

### Discussion:

* The cited text at p2933.60

A close-up of a text

Description automatically generated

* And the cited text at 2927.35

A close-up of a message

Description automatically generated

* The proposed resolution adds the following to the cited text:

“The retransmit timeout value should be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. *If there is no listen interval or the listen interval is zero, then 100 ms should be used for all timeout values*."

* The behaviour does need to be clarified since a STA can set the listen interval to 0 when it associates. However, the listen interval always must be specified in the (re)association request frame. It would be better to say “If the listen interval is zero, then 100 ms should be used for all timeout values.”

### Proposed Resolution: (6084)

REVISED. Make the changes in line with the Proposed Change noting that there is always a listen interval but it can be set to 0.

At P2933.60 (group HS) and P2927.35 (4-way HS) replace

"The retransmit timeout value shall be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If there is no listen interval or the listen interval is zero, then 100 ms shall be used for all timeout values."

with

"The retransmit timeout value should be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If the listen interval is zero, then 100 ms should be used for all timeout values."

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6170 |  | 12 |  |  | Rules or at least guidance is needed for channel switch across bands, to cover constraints in the new band (e.g. that certain security procedures are not allowed) | At the end of 11.8.8.1 add a "NOTE---The non-extended channel switching procedure does not allow switching to a different operating class, and hence does not allow switching to a different band." At the end of 11.9.1 add a "NOTE---The RSN configuration does not change across a channel switch. This means, for example, that a switch from the 2.4 GHz or 5 GHz band to the 6 GHz band is only possible if the RSNE advertised in the old band is also valid in the 6 GHz band." |

### Discussion:

* This comment has nothing to do with clause 12. It is asking for notes added to clause 11 with respect to the extended channel switch announcement.
* Clause 11.8.8.1 on page 2495:

A screenshot of a news

Description automatically generated

* The comment proposes to add this note to the above clause:

“NOTE---The non-extended channel switching procedure does not allow switching to a different operating class, and hence does not allow switching to a different band.”

* It would be better to express the note with respect to the extended channel switch announcement:

“NOTE---Only the extended channel switching procedure allows switching to a different operating class, and hence allows switching to a different band.”

* Clause 11.9.1 on page 2503:

A screenshot of a computer

Description automatically generated

* The comment proposes to add this note to the above clause:

“NOTE---The RSN configuration does not change across a channel switch. This means, for example, that a switch from the 2.4 GHz or 5 GHz band to the 6 GHz band is only possible if the RSNE advertised in the old band is also valid in the 6 GHz band.”

* The BSS configuration does not change across a channel switch. Although the RSNE has further constraints. Perhaps modify the note as follows:

“NOTE---The BSS configuration does not change across a channel switch. This means, for example, that a switch from the 2.4 GHz or 5 GHz band to the 6 GHz band is only possible if the BSS configuration in the old band is also valid in the 6 GHz band.”

### Proposed Resolution: (6170)

REVISED. The BSS configuration, other than the operating channel does not change as a result of channel switching procedures.

At the end of clause 11.8.8.1 at 2945.51, insert the following note:

“NOTE---Only the extended channel switching procedure allows switching to a different operating class, and hence allows switching to a different band.”

At the end of clause 11.9.1 at 2503.54, insert the following note:

“NOTE---The BSS configuration does not change across a channel switch. This means, for example, that a switch from the 2.4 GHz or 5 GHz band to the 6 GHz band is only possible if the BSS configuration in the old band is also valid in the 6 GHz band.”

### Comment

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** | |
| 6167 | 2937.00 | 12.7.8.4 |  |  | The TPK handshake allows the TDLS initiator STA to propose multiple cipher suites. However, it was asserted during a TGme session at the September 2023 F2F that existing TDLS responder STA implementations would not cope with more than one proposed cipher suite. Furthermore, integrity validation of the full list of pairwise cipher suite selectors is not performed and that could potentially result in the AP (or anyone else who is able to decrypt and inject frames on the AP links) being able to do a downgrade attack for the direct link by selectively removing cipher suite selectors from the list | | At 2937.42 change "The (#3240)(#3241)Pairwise Cipher Count and Pairwise Cipher Suite List fields (#1420)shall indicate the pairwise cipher suites the TDLS initiator STA is willing to use with the TPKSA. (#3056)TKIP shall not be included in this list." to "The Pairwise Cipher Suite List field shall indicate the pairwise cipher suite to be used with the TPKSA, and the Pairwise Cipher Suite Count field shall be set to 1." At 2938.49 delete "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." |

### Discussion:

* The cited text on 2937 isA close-up of a message

  Description automatically generated
* The first proposed change is:
* At 2937.42 change

"The (#3240)(#3241)Pairwise Cipher Count and Pairwise Cipher Suite List fields (#1420)shall indicate the pairwise cipher suites the TDLS initiator STA is willing to use with the TPKSA. (#3056)TKIP shall not be included in this list."

to

"The Pairwise Cipher Suite List field shall indicate the pairwise cipher suite to be used with the TPKSA, and the Pairwise Cipher Suite Count field shall be set to 1."

* Based on the review of document 11-23/1546r1 and the minutes from the September interim and the minutes, the only comment I could find is:

“Jouni: change would not be interoperable. Would need capability negotiation. "Nobody" does PMF with TDLS and "nobody" pays attention to the number of replay counters advertised -- so RSN capabilities not useful in current deployments”

* In IEEE 802.11-2020, the original text is “The pairwise cipher suite list field indicating 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 cited text on 2398

A close up of a message

Description automatically generated

* The proposed change is:

At 2938.49 delete "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."

* In IEEE 802.11-2020, the text is “Include a pairwise cipher suite from one of those presented in RSNE of message 1 of this sequence in the pairwise cipher suite list, and set the pairwise cipher suite count to 1.”
* Note that the cited text to be changed was added in REVme.
* Also note that the Resolution to CID 4229 (on a similar topic was):

“REJECTED. The purpose of the RSNE used in the TPK handshake is to negotiate a secure TDLS link. The TDLS Responder STA is required to evaluate the RSN Capabilities received in TPK handshake message one and include the same value in message 2.”

* The comment points out that an AP (or any entity that can may be able to decrypt and inject frames) can compromise the TPK handshake. However, the TPK handshake is derived based on the assumption that the TDLS initiator and TDLS responder trust the AP.
* With respect to the number of cipher suites included in the RSNA for TPK message 1, a note could be added to reflect current implementations on sending message 1 include only a single cipher suite.

### Proposed Resolution: (6167)

Multiple options here:

ACCEPTED

or

REVISED. Add a note to indicate that some TDLS responder STA implementations expect a single cipher suite in TPK handshake message 1. No changes are required for TPK handshake message 2.

At 2937.45, change

“TKIP shall not be included in this list.’

to

“NOTE---Some deployed TDLS responder STAs implementations expect to receive a single pairwise cipher suite in the RSNE in TPK handshake message 1.”

Or

REJECTED. The purpose of the RSNE used in the TPK handshake is to negotiate a secure TDLS link. The security properties of the TPK handshake required the TDLS initiator STA and TDLS responder STA to trust the AP. The TDLS Responder STA is required to evaluate the RSN Capabilities received in TPK handshake message one and include the same value in message 2.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6166 |  | 12 |  |  | Determination of the TDLS responder's RSN capabilities is problematic, because in the TPK handshake the TDLS responder echoes the TDLS initiator's RSNE, so the TDLS initiator does not receive the TDLS responder's RSN capabilities. The TDLS responder's RSN capabilities are present in the TDLS Discovery Response frame, but TDLS discovery is not mandatory, and anyway this frame is not protected. In turn, this means that the number of replay counters supported by the TDLS responder is not always known, nor is its MFP support. It was asserted during a TGme session at the September 2023 F2F that "nobody" does PMF with TDLS and "nobody" pays attention to the number of replay counters advertised. | In Table 9-189—PTKSA/GTKSA/TPKSA replay counters usage delete "/TPKSA" (5x inc. caption) At 4974.17 delete "and the number of TPKSA replay counters per (#2152)TDLS direct link" At 2852.52 and 2862.47 change "subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE))." to "subject if not for a TPKSA to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE)). A TDLS STA shall support 16 replay counters per TPKSA and shall ignore the PTKSA Replay Counter field in RSNEs received from a TDLS peer STA." At 2874.36 change "(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS peer STA during TDLS discovery or in the RSNEs exchanged in the 3-way handshake with the TDLS peer STA to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0." to "(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS responder STA during TDLS discovery, if performed, or in the RSNE received from the TDLS initiator STA in the TPK handshake to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0. If TDLS discovery was not performed, the TDLS initiator STA shall set the MFPC and MFRP bits in its RSNE to the same value; if the TDLS initiator STA set them to 0 in its RSNE it shall behave as if the MFPC and MFPR bits from the TDLS responder STA were 0, and as if those bits were 1 otherwise. NOTE---This means that if a TDLS initiator STA requires MFP but does not know whether the TDLS responder is MFP-capable, it assumes it is (any mismatch will be discovered when a Management frame exchange is performed); otherwise MFP is not used. The TDLS responder STA might preemptively tear down the TDLS link if this assumption is wrong, i.e. the TDLS initiator STA requires MFP but the TDLS responder STA is not MFP-capable or vice-versa, or it might hope Management frames are not used (e.g. there is no attempt to set up a block ack agreement)." At 2875.37 change "3-way handshake" to "TPK handshake". |

### Discussion:

* [p985.9] In Table 9-189—PTKSA/GTKSA/TPKSA replay counters usage delete "/TPKSA" (5x inc. caption) A screenshot of a computer

  Description automatically generated
  + Deleting all occurrences of TPKSA in this table does not seem like the right approach here since the TPKSA includes these fields and could affect deployed implementations
* At 4974.17 delete "and the number of TPKSA replay counters per (#2152)TDLS direct link"
  + Deleting this text does not seem like the right approach here since the TPKSA includes these fields in the RSNE and would affect interoperability between peer TDLS STAs
* At 2852.52 and 2862.47 change

"subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE))."

to

"subject if not for a TPKSA to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.23 (RSNE)). A TDLS STA shall support 16 replay counters per TPKSA and shall ignore the PTKSA Replay Counter field in RSNEs received from a TDLS peer STA."

* + Adding an explicit requirement for the TDLS STA to support 16 repla counters for TPKSA and ignore the field in the RSNE does not seem to make sense here.
* At 2874.36 change

"(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS peer STA during TDLS discovery or in the RSNEs exchanged in the 3-way handshake with the TDLS peer STA to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0."

to

"(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS responder STA during TDLS discovery, if performed, or in the RSNE received from the TDLS initiator STA in the TPK handshake to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0. If TDLS discovery was not performed, the TDLS initiator STA shall set the MFPC and MFRP bits in its RSNE to the same value; if the TDLS initiator STA set them to 0 in its RSNE it shall behave as if the MFPC and MFPR bits from the TDLS responder STA were 0, and as if those bits were 1 otherwise.

NOTE---This means that if a TDLS initiator STA requires MFP but does not know whether the TDLS responder is MFP-capable, it assumes it is (any mismatch will be discovered when a Management frame exchange is performed); otherwise MFP is not used. The TDLS responder STA might preemptively tear down the TDLS link if this assumption is wrong, i.e. the TDLS initiator STA requires MFP but the TDLS responder STA is not MFP-capable or vice-versa, or it might hope Management frames are not used (e.g. there is no attempt to set up a block ack agreement)."

* + This change seems reasonable and clarifies TDLS protocol behavior.
* At 2875.37 change "3-way handshake" to "TPK handshake".
  + This change seems reasonable

### Proposed Resolution: (6166)

REVISED. The purpose of the RSNE used in the TPK handshake is to negotiate a secure TDLS link. The TDLS Responder STA is required to evaluate the RSN Capabilities received in TPK handshake message 1. The negotiation of replay counters and MFP may be “ignored” by implementations, but that does not mean that the standard needs to be changed. Make the following changes as suggested by the commenter.

At 2874.36 change

"(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS peer STA during TDLS discovery or in the RSNEs exchanged in the 3-way handshake with the TDLS peer STA to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0."

to

"(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#199)) and the values of the MFPC and MFPR bits advertised in the RSNE received from the TDLS responder STA during TDLS discovery, if performed, or in the RSNE received from the TDLS initiator STA in the TPK handshake to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled. If either STA does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0. If TDLS discovery was not performed, the TDLS initiator STA shall set the MFPC and MFRP bits in its RSNE to the same value; if the TDLS initiator STA set them to 0 in its RSNE it shall behave as if the MFPC and MFPR bits from the TDLS responder STA were 0, and as if those bits were 1 otherwise.

NOTE---This means that if a TDLS initiator STA requires MFP but does not know whether the TDLS responder is MFP-capable, it assumes it is (any mismatch will be discovered when a Management frame exchange is performed); otherwise MFP is not used. The TDLS responder STA might preemptively tear down the TDLS link if this assumption is wrong, i.e. the TDLS initiator STA requires MFP but the TDLS responder STA is not MFP-capable or vice-versa, or it might hope Management frames are not used (e.g. there is no attempt to set up a block ack agreement)."

At 2875.37 change "3-way handshake" to "TPK handshake".

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6163 | 2938.00 | 12.7.8.4.3 |  |  | "The version number shall be the minimum of the maximum version supported by the TDLS responder STA and the version number received in the RSNE of message 1." seems to duplicate the text 2 paras above | Delete the cited text |

### Discussion:

* This is the cited text:

A close-up of a message

Description automatically generated

* The text at lines 47 and 53 are duplicated.

### Proposed Resolution: (6163)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6150 | 2937.00 | 12.7.8.4 |  |  | The number of replay counters supported by a TDLS responder is not known (T2's RSN Capabilities field is a copy of T1's), and though the number supported by the TDLS responder is advertised in T1's RSN Capabilities field, in practice existing deployments just assume this will always be 16, i.e. one per TID. See other comment for more expansive proposed change | At 2937.50 change "In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1." to "In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1, the PTKSA Replay Counter field in the shall be set to 3 (to indicate 16 replay counters for the TPKSA) and the GTKSA Replay Counter field shall be reserved." At 2939.17 add a para "The RSN capabilities of the TDLS responder STA are not communicated to TDLS initiator STA during the TPK handshake. A TDLS initiator STA shall assume that a TDLS responder STA supports 16 replay counters for the TPKSA." |

### Discussion:

* This is the cited text in context:

A screenshot of a computer message

Description automatically generated

* The first change proposed by the commenter are:

At cited location, change “In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1.”

to

“In the RSN Capabilities field, (#3056)the PeerKey Enabled subfield shall be set to 1, the PTKSA Replay Counter field in the shall be set to 3 (to indicate 16 replay counters for the TPKSA) and the GTKSA Replay Counter field shall be reserved”

* Before message 2, the TDLS Responder STA evaluates message 1. If the number of replay counters or any other parameter from message 1 is not acceptable to the TDLS Responder STA, it would not transmit message 2.
* This proposed change introduces a new requirement for the negotiation of a TDLS link.
* There is no justification for requiring 16 replay counters advertised by the RSNE.
* The second change is as follows: At 2939.17 add a para

"The RSN capabilities of the TDLS responder STA are not communicated to TDLS initiator STA during the TPK handshake. A TDLS initiator STA shall assume that a TDLS responder STA supports 16 replay counters for the TPKSA."

* This places a requirement on the TDLS initiator STA to assume a capability of the TDLS responder STA.
* The TDLS initiator STA can obtain the capabilities of the TDLS responder STA during TDLS discovery. The TDLS initiator STA could infer the capabilities of the TDLS responder STA from a previous TDLS connection with the TDLS responder STA, or the capabilities advertised by the AP.

### Proposed Resolution: (6150)

REJECTED. The TDLS initiator STA can obtain the capabilities of the TDLS responder STA using TDLS discovery. Alternatively, the TDLS initiator STA can infer the TDLS capabilities of the TDLS responder STA from a previous connection or the capabilities advertised by the AP. The TDLS responder STA evaluates the parameters receives in message 1 and if any parameter, including the number of replay counters is not acceptable, the TDLS responder STA may refrain from sending message 2. There is not need to provide additional restrictions on the TDLS handshake.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6114 | 2870.00 | 12.7.9.3 |  |  | Missing shall - and correct grammar "deletes" to "delete" | Insert "shall" correcting the text to read: "… the Supplicant shall also delete ... " |

### Discussion:

* This is the cited text in context and is in clause 12.6.1.2.2:

A close-up of a computer screen

Description automatically generated

* This behavior requirement is covered in clause 11.3.5 (Association, reassociation, and disassociation) and the key deletion is invoked by calling MLME-DELETEKEYS primitive. A reference to that subclause could be made a this location.
* Also “roams from” should be “transitions from”

### Proposed Resolution: (6114)

REVISED. At 2870.40, change

“but its Supplicant also deletes the PTKSA when it roams from the old AP. The Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all BSSIDs in the ESS.”

To

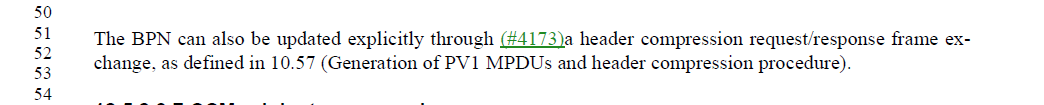
“but its Supplicant also deletes the PTKSA when it transitions from the old AP. The Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all BSSIDs in the ESS (see 11.3.5).”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6102 | 2850.00 | 12.5.2.3.7 |  |  | [HP] Incorrect reference | Change reference to 12.5.2.3.4 Construct CCM nonce |

### Discussion:

* This is the cited text in context is: A close up of text

  Description automatically generated:
* The comment is correct in noting that b) on the bulleted list should cross reference 12.5.2.3.4

### Proposed Resolution: (6102)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6101 | 2804.00 | 12.3.4.1.2 |  |  | [HP] Incorrect reference | Change reference to 9.2.4.9 FCS field |
| 6100 | 2800.00 | 12.3.2.2.1 |  |  | [HP] Incorrect reference | Change reference to 9.2.4.9 FCS field |

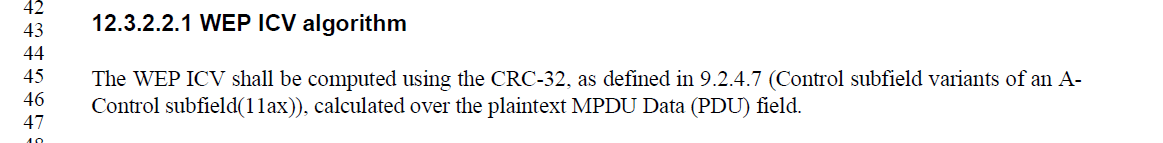
### Discussion:

* This is the cited text in clause 12.3.4.1.2:

A black text on a white background

Description automatically generated

* This is the cited text in clause 12.3.2.2.1:



* The text in 12.3.4.1.2 in 802.11-2020 looks like:

A close up of text

Description automatically generated

* Clause 9.2.4.7 in IEEE 802.11-2020 is the “Frame Body field” which was renumbered to clause 9.2.4.8 in D4.0

### Proposed Resolution: (6101, 6100)

REVISED. At 2804.14 and 2800.45, change “(see 9.2.4.7 …” to “(see 9.2.4.8 …”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6089 | 2835.00 | 12.4.8.1 |  |  | The Figure 12-4 (SAE finite state machine) transition Confirmed->Confirmed based on the Com event lacks the condition for the group differing from the last valid received SAE Commit message that is describe in the text (P2841 L54: "if the finite cyclic group differs from the finite cyclic group in the most recently received valid SAE Commit message". Because of this, the current state machine figure would indicate incorrect behavior for a SAE confirm message where the group has changed (it would be result in SAE Commit message and SAE Confirme message being transmitted with the new Sc value while the received message should have been discarded without transmitting these new messages). | In Figure 12-4 (P2835 L33; the text a bit right and up from the Confirmed state), replace Confirmed->Confirmed transition case "(Com,!big(Sync)/(inc(Sc), inc(Sync), 1(0 or 126),2,set(t0))" with "(Com,!big(Sync),!ChangedGrp/(inc(Sc),inc(Sync),1(0 or 126),2,set(t0))". At P2838 L3 (12.4.8.5.2), add a new entry to the list after DiffGrp: "ChangedGrp. The group specified in an SAE Commit message is supported but differs from the one received in the most recently received valid SAE Commit message." |

### Discussion:

* Note that the figure referenced by the comment is Figure 12-14 and is shown below:

A diagram of a diagram

Description automatically generated

* And referenced in the proposed change on pages 2837-2838:

**A close up of text

Description automatically generated**

**A close-up of a message

Description automatically generated**

* The first change is to Figure 12-14 and is:

“In Figure 12-**14**(P2835 L33; the text a bit right and up from the Confirmed state), replace

Confirmed->Confirmed transition case

"(Com,!big(Sync)/(inc(Sc), inc(Sync), 1(0 or 126),2,set(t0))"

with

"(Com,!big(Sync),!ChangedGrp/(inc(Sc),inc(Sync),1(0 or 126),2,set(t0))".

* The second change is:

At P2838 L3 (12.4.8.5.2), add a new entry to the list after DiffGrp:

"ChangedGrp. The group specified in an SAE Commit message is supported but differs from the one received in the most recently received valid SAE Commit message."

* The change updates the state machine for the case where the finite cyclic group has changed. The second change updates the list of state variables with ChangedGrp”

### Proposed Resolution: (6089)

REVISED. Make the changes suggested by the commenter noting that the Figure to be changed is 12-14, not 12-4.

Note to editor: The commenter will supply an updated figure which includes the change.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 6266 |  | 12.7.2 |  |  | "In other words, the Supplicant (#1822)shall not update the Key Replay Counter field for message 1 in the 4-way handshake, as it includes no MIC." is confusing since the Supplicant does not tx M1 | Reword for better clarity |

### Discussion:

* This is the cited text on page 291- in context:

A close-up of a text

Description automatically generated

A close-up of a text

Description automatically generated

* The cited text begins with “in other words” which implies that it is simply clarifying another requirement already specified for the Supplicant.
* The requirements for the Supplicant:
  + The Supplicant tracks the key replay counter per SA.
  + The Supplicant uses the last received key replay counter value received from the Authenticator.
  + The Supplicant ignores a EAPOL-Key PDU with a replay counter smaller or equal to any received in a valid message.
* The sentence seems to be clarifying that the Supplicant does not update the key replay counter after it has received a message 3 with a valid MIC.
* After a valid message 3 is received with a valid MIC, the SA would be in place. The requirements preceding the cited text seem to clearly articulate the requirements on the Supplicant.

### Proposed Resolution: (6266)

REVISED. The cited text attempts to clarify the requirements that are stated earlier and can be removed.

At 2910, delete:

“In other words, the Supplicant (#1822)shall not update the Key Replay Counter field for message 1 in the 4-way handshake, as it includes no MIC. This implies the Supplicant needs to allow for retransmission of message 1 when checking for the key replay counter of message 3.”