IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TDLS related comment resolutions on REVme draft 0.0 | | | | |
| Date: November 1, 2021 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Menzo Wentink | Qualcomm | Utrecht, The Netherlands | +31-65-183-6231 | mwentink  @qti.qualcomm.com |

Abstract

This document contains comment resolutions for REVme draft 0.0, addressing the following CIDs:

1. 250, 237, 201, 196, 195, 182, 574, 9, 8,
2. 2, 1, 118

The baseline for this document is Draft P802.11REVme D0.0 except when noted otherwise.

|  |  |  |  |
| --- | --- | --- | --- |
| **CID identifiers** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 250  Mark Rison  2318.24  11.20.1 | It is not clear whether a TDLS STA may transmit to a TDLS peer STA a unicast MPDU containing an A-MSDU containing subframes with a group DA | After  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a TDLS or other frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA."  add  "An A-MSDU transmitted over the direct path shall not contain an A-MSDU subframe header with a DA field that is a group address." | Accepted |
| 195  Mark Rison  2318.24  11.20.1 | It is not clear whether the RA can be a group address in a direct-link frame in TDLS (From DS = To DS = 0), and if so which key is used (GTK or TPK).  Since group traffic can and should go via the AP, group-addressed transmissions would be ambiguous if a TDLS STA had more than one TDLS peer STA, and neither the GTK nor the TPK are really appropriate anyway (not GTK because it's a pairwise link and the TA isn't the AP's TA, yes GTK because it's a group RA), just make it clear no, TDLS is for unicast traffic only.  Ah, and "The group cipher suite shall be set to 00-0F-AC:7." for the TPK handshake also nixes use of a group cipher. | After  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a TDLS or other frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA."  add  "A TDLS or other frame transmitted over the direct path shall not be group addressed." | Revised -  After  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a TDLS or other frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA."  add  "Note--This implies that the RA of frames transmitted over the direct path can not be a group address." |
| 237  Mark Rison  11.2 | "TDLS frame" is not defined.  "Transmitting a TDLS frame through the AP"  suggests it just means a frame transmitted by a TDLS STA to a TDLS peer STA, but  "Note that the TDLS Discovery Response frame is not a TDLS frame but a Public Action frame."  and  "tunneled direct-link setup (TDLS): A protocol that uses a specific Ethertype encapsulation to TDLS frames through an access point (AP) to establish a TDLS direct link."  suggest it means specifically a frame used for TDLS signalling and that is carried in an MSDU with a specific Ethertype (so does not include the TDLS Discovery Response frame) | At 199.63 change  "tunneled direct-link setup (TDLS): A protocol that uses a specific Ethertype encapsulation to tunnel TDLS frames through an access point (AP) to establish a TDLS direct link."  to  "tunneled direct-link setup (TDLS): A protocol that uses a specific Ethertype encapsulation to tunnel frames through an access point (AP) to establish a TDLS direct link."  (i.e. s/to TDLS/to tunnel/)  and add a definition:  "tunneled direct-link setup (TDLS) frame: A medium access control (MAC) service data unit (MSDU) with a specific Ethertype encapsulation used for establishing and managing a TDLS direct link."  At 2318.24 change  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA."  to  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a TDLS frame or other frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA." | Revised -  add a definition:  "tunneled direct-link setup (TDLS) frame (TDLS frame): A medium access control (MAC) service data unit (MSDU) with a specific Ethertype encapsulation, used for establishing and managing a TDLS direct link."  At 2318.24 change  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA."  to  "Transmitting a TDLS frame through the AP means that the frame's RA is set to the BSSID. Transmitting a TDLS frame or other frame over the direct path means that the frame's RA is set to the MAC address of the TDLS peer STA." |
| 201  Mark Rison  2321.20  11.20.4 | "Subsequent to the successful completion of the TPK handshake, all frames transmitted and received on the TDLS direct link shall be protected using the TPKSA"  -- not Control or (unless PMF) Management frames | Change to  "Subsequent to the successful completion of the TPK handshake, all Data frames transmitted and received on the TDLS link, and all Management frames if management frame protection is in use, shall be protected using the TPKSA" | Revised - change the cited sentence to  "Subsequent to the successful completion of the TPK handshake, all Data frames transmitted on the TDLS direct link, and all Management frames if management frame protection is in use, shall be protected using the TPKSA"  Relative to the proposed change, 'TDLS link' is changed to 'TDLS direct link' and 'and received' is removed because the transmission is where the protection takes place. |
| 196  Mark Rison  2319.46  11.20.2 | "TDLS uses Ethertype 89-0d frames, as defined in Annex H. The TDLS payload contains a TDLS Action field as is specified in 9.6.12 (TDLS Action field formats)."  is far too general. TDLS only uses such frames for TDLS signalling. And "TDLS payload" is not clear | Change to  "TDLS uses Ethertype 89-0d frames, as defined in Annex H, for TDLS signalling. The Payload field of the Ethertype 89-0d frame contains one of the TDLS Action fields specified in 9.6.12 (TDLS Action field formats)." | Accepted |
| 182  Mark Rison | direct link v direct path v TDLS direct link v TDLS link -- it is not clear how these differ.  There aren't many instances of "direct path". A TDLS link is by definition a direct link, otherwise it's not a TDLS link it's a normal infrastructure BSS link going via the DS | Change  "direct path"  to  "direct link" throughout.  Change "TDLS direct link"  to "TDLS link" throughout | Rejected -  The direct path in the context of TDLS is defined at 2318.25:  'Transmitting a TDLS frame through the AP means that the frame’s RA is set to the BSSID. Transmitting a frame over the direct path means that the frame’s RA is set to the MAC address of the TDLS peer STA.'  There are occasional uses of 'direct link' without 'TDLS', but when this happens it is clearly within the context of TDLS and this does not appear to be causing any confusion. |
| 574  Stephen Mc Cann  837.59  9.3.2.1.2 | There is no specific mention of setting the To DS and From DS addressing bits for TDLS Data frames. | Add a new sentence at the end of the paragraph  "The values of the To DS and From DS bits for TDLS Data frames are set to 0."  Note: The settings for TDLS management frames are implied by text in clause 9.3.3.1 (P845L43). | Revised -  At 780.19, after  "A Data frame from one STA to another STA within the same IBSS or the same PBSS, a Data frame direct from one non-AP STA to another non-AP STA within the same infrastructure BSS, or a Data frame outside the context of a BSS."  replace  "This is the only valid combination for Data frames transmitted by an IBSS or PBSS STA, or outside the context of a BSS."  with  "This is the only valid combination for Data frames transmitted by an IBSS or PBSS STA, on the direct path of a TDLS direct link, or outside the context of a BSS."  (Same resolution as for CID 1.) |
| 1  Abhishek Patil  780.14  9.2.4.1.4 | Based on the description, the text applies to a Data frame sent from a TDLS peer STA to another TDLS peer STA over the TDLS direct link. | Clarify that 0,0 applies to Data frames sent over a TDLS direct link | Revised -  Revised -  At 780.19, after  "A Data frame from one STA to another STA within the same IBSS or the same PBSS, a Data frame direct from one non-AP STA to another non-AP STA within the same infrastructure BSS, or a Data frame outside the context of a BSS."  replace  "This is the only valid combination for Data frames transmitted by an IBSS or PBSS STA, or outside the context of a BSS."  with  "This is the only valid combination for Data frames transmitted by an IBSS or PBSS STA, on the direct path of a TDLS direct link, or outside the context of a BSS."  (Same resolution as for CID 574.) |
| 9  Abhishek Patil  2320.1  11.20.3 | What is the TDLS Initiator STA Address and TDLS Responder STA Address fields of the Link Identifier element set to when the TDLS Discovery Response frame is sent unsolicited? In addition, what are the values carried in this field when a STA responds to an unsolicited TDLS Discovery Response frame with a TDLS Discovery Response frame? | As in comment | Revised -  A regular (solicited) Discovery Response frame has the responder STA address in the TDLS responder STA Address field contained in the Link Identifier element:  "The TDLS responder STA Address field contained in the Link Identifier element of the TDLS Discovery Response frame shall be set to the MAC address of the STA sending the TDLS Discovery Response frame."  It makes sense that the unsolicted Discovery Response does the same, and also the Discovery Response frame that is the response to an unsollicited Discovery Response frame.  This implies that the addresses in the Link Identifier element of these TDLS Discovery Response frames are swapped, but this is not an issue, because the Link Identifier element used for the setup of the TDLS direct link will be set by the STA sending the TDLS Setup Request frame (the Link Identifier element of any preceding Discovery frames is not relevant anymore at this stage.)  At 2503.9 (D0.1), add  "The TDLS responder STA Address field contained in the Link Identifier element of these TDLS Discovery Response frames shall be set to the MAC address of the STA sending the TDLS Discovery Response frame.  Note--This implies that the addresses in the Link Identifier element of the received and transmitted TDLS Discovery frames are swapped, but the Link Identifier element for the TDLS direct link will be defined the Link Identifier element of the TDLS Setup Request anyway." |
| 8  Abhishek Patil  2319.59  11.20.3 | The responder should not blindly set the TDLS Responder STA Address to the one that was carried in the TDLS Discovery (or Setup) Request frame. It needs to verify that the Address matches its address. | As in comment | Rejected -  The TDLS Responder STA address should not be different from the MAC address of the STA. This might be different in 11be, but it should be handled there.  This change may cause issues with legacy TDLS devices in the field when they do not check this field. |
| 2  Abhishek Patil  1149.53  9.4.2.47 | This FTE is also used for TDLS authentication. | Add TDLS authentication to the list | Revised -  At 1150.23, replace  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithm specified in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message). Otherwise, the MIC field is set to 0."  with  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithms specified in 13.8.4 (FT authentication sequence: contents of third message), 13.8.5 (FT authentication sequence: contents of fourth message), 12.7.8.4.3 (TPK handshake message 2), and 12.7.8.4.4 (TPK handshake message 3). Otherwise, the MIC field is set to 0."  (Same resolution as for CID 118.) |
| 118  Jouni Malinen  1150.25  9.4.2.47 | FTE description in Clause 9 covers only the FT and FILS cases while this element is used also with TDLS. In particular, the rules for setting the MIC for TDLS setup exchange are missing. | Add the needed references for the rules on how MIC field is set for TDLS setup frames. At minimum, this should reference 12.7.8.4.3 and 12.7.8.4.4 for MIC calculation in TPK handshake messages 2 and 3.  Please also note that this may end up getting resolved as a related change in P802.11be, so potential REVme edits should be coordinated with that effort. These edits would likely include following:  Replace  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithm specified in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message). Otherwise, the MIC field is set to 0."  with  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithm specified in 13.8.4 (FT authentication sequence: contents of third message), 13.8.5 (FT authentication sequence: contents of fourth message), 12.7.8.4.3 (TPK handshake message 2), and 12.7.8.4.4 (TPK handshake message 3). Otherwise, the MIC field is set to 0." | Revised -  At 1150.23, replace  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithms specified in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message). Otherwise, the MIC field is set to 0."  with  "When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithm specified in 13.8.4 (FT authentication sequence: contents of third message), 13.8.5 (FT authentication sequence: contents of fourth message), 12.7.8.4.3 (TPK handshake message 2), and 12.7.8.4.4 (TPK handshake message 3). Otherwise, the MIC field is set to 0."  (Same resolution as for CID 2.) |