IEEE P802.11
Wireless LANs

|  |
| --- |
| CIDs related to TDLS operation – Part 2 |
| Date: September 23, 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com  |
| Michael Montemurro | Huawei |  |  | Montemurro.michael@gmail.com  |
| Rojan Chitrakar | Panasonic |  |  |  |
| Tomo Adachi | Toshiba |  |  |  |
| Srinivas Kandala | Samsung Electronics |  |  |  |
| Chunyu Hu | Facebook |  |  |  |
| Insun | LGE |  |  |  |
| Namyeong |  |  |  |

 Abstract

This submission proposes resolutions for following CIDs received for TGbe (CC36): 4031, 8296

***TGbe Editor: Please note, the baseline for this document is REVme D0.3 and TGbe D1.2***

Revisions:

* Rev 0: Initial version

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbe Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Section** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 4031 | Abhishek Patil | 11.20 | 206.23 | Investigate if clause 12.7.8 needs to be updated to cover PTK establishment for a TDLS link involving a STA of a non-AP MLD. | As in comment | **Revised**Based on offline discussions with various members, the spec text is updated to include AP MLD MAC address in the TDLS Discovery and Setup frames. The AP MLD MAC address is used during TPK generation if both peers are STAs affiliated with their respective non-AP MLDs. The AP MLD MAC address is carried in a new variant of Multi-Link element (TDLS variant). Other parts of the spec were updated accordingly. **TGbe editor, please make changes as shown in doc 11-21/1436r0 tagged 4031** |
| 8296 | Zhiqiang Han | 9.6.7.16 | 154.51 | Add Multi-Link element in this frame | as in comment. | **Revised**Resolution to CID 4031 proposes to include Multi-Link element in TDLS Discovery and Setup frames transmitted by a STA affiliated with a non-AP MLD.**TGbe editor, please make changes as shown in doc 11-21/1436r0 tagged 4031** |

**35.3.20 TDLS procedure in multi-link operation**[4031]

**35.3.20.1 General**

***TGbe editor: Please modify the 1st paragraph in this clause as follows:***

When the frames that are exchanged during TDLS discovery or setup do not include a TDLS Multi-Link element or include a TDLS Multi-Link element containing only the Common Info field carrying only the AP MLD MAC Address field, then the TDLS discovery or setup respectively, is for a single link.

**35.3.20.2 TDLS direct link over a single link**

***TGbe editor: Please add the following paragraph after the 4th paragraph in D1.2:***

When attempting to establish a TDLS direct link over a single link, a TDLS STA affiliated with a non-AP MLD shall include a TDLS Multi-Link element containing only the Common Info field carrying only the AP MLD MAC Address field (see 9.4.2.295b.4 (TDLS Multi-Link element)) in the TDLS Discovery Request frame and TDLS Discovery Response frame that it transmits. A TDLS STA affiliated with a non-AP MLD shall not respond to a TDLS Discovery Request frame if the frame carries TDLS Multi-Link element and the MLD MAC address carried in the AP MLD MAC Address field of the TDLS Multi-Link element does not match the MLD MAC address of the AP MLD with which the non-AP MLD has performed multi-link setup.

***TGbe editor: Please add the following paragraph after the 5th paragraph in D1.2:***

When attempting to establish a TDLS direct link over a single link, a TDLS STA affiliated with a non-AP MLD shall include the TDLS Multi-Link element containing only the Common Info field carrying only the AP MLD MAC Address field (see 9.4.2.295b.4 (TDLS Multi-Link element)) in the TDLS Setup Request frame. A TDLS STA affiliated with a non-AP MLD shall not respond to a TDLS Setup Request frame if the frame carries TDLS Multi-Link element and the MLD MAC address carried in the AP MLD MAC Address field of the TDLS Multi-Link element does not match the MLD MAC address of the AP MLD with which the non-AP MLD has performed multi-link setup. A TDLS STA affiliated with a non-AP MLD shall include the TDLS Multi-Link element in the TDLS Setup Response frame if the soliciting TDLS Setup Request frame included TDLS Multi-Link element. A TDLS STA affiliated with a non-AP MLD shall not respond to a TDLS Setup Response frame if the frame carries TDLS Multi-Link element and the MLD MAC address carried in the AP MLD MAC Address field of the TDLS Multi-Link element does not match the MLD MAC address of the AP MLD with which the non-AP MLD has performed multi-link setup. A TDLS STA affiliated with a non-AP MLD shall include the TDLS Multi-Link element in the TDLS Setup Confirm frame if the preceding TDLS Setup Response frame included TDLS Multi-Link element.

When both STAs that are involved in a single link TDLS setup include a TDLS Multi-Link element carrying the AP MLD MAC Address field in the frames exchanged during the TDLS setup phase, the TDLS TPK generation shall include the AP MLD MAC address in addition to the MAC address of the affiliated AP where the TDLS direct link is being established, as defined in Equation (12-0b). When at least one of the STAs that are involved in a single link TDLS setup, does not include TDLS Multi-Link element, in the frames exchanged during TDLS setup phase, the STAs shall derive the TPK as defined in Equation (12-0a).

***TGbe editor: Please update the following two paragraphs after as shown below:***

Figure 35-20 (Example A of TDLS discovery initiated by a non-AP MLD) and Figure 35-21 (Example B of TDLS discovery initiated by a non-AP MLD) illustrate the scenario where the TDLS discovery is initiated by a non-AP MLD (MLD\_S). MLD\_S has performed multi-link setup with an AP MLD (MLD\_A). MLD\_S has two affiliated STAs, STA1 and STA2. STA3 is not capable of performing multi-link operation and is not affiliated with a non-AP MLD. MLD\_A has two affiliated APs, AP1 and AP2, where AP1 operates on link 1 and AP2 operates on link 2. STA1 and STA3 operate on link 1 and are associated with AP1. STA2 operates on link 2 and is associated with AP2. In the example, MLD\_S initiates TDLS discovery by transmitting two TDLS Discovery Request frames (which are Data frames) as it does not know which link STA3 is operating on and whether STA3 is an MLD or a STA not affiliated with an MLD. The first TDLS Discovery Request frame (shown on Figure 35-20 (Example A of TDLS discovery initiated by a non-AP MLD)) has the BSSID field in the Link Identifier element set to the BSSID of AP1 and the second TDLS Discovery Request frame has this field set to the BSSID of AP2 (shown on Figure 35-21 (Example B of TDLS discovery initiated by a non-AP MLD)). Both the frames have their A3 (DA) set to the STA3 MAC address and the To DS subfield of the Frame Control field set to 1. The TDLS Discovery Request frame can be transmitted over either link 1 (through STA1 as represented by solid line) or link 2 (through STA2 as represented by dotted line). When the TDLS Discovery Request frame is received at the AP MLD (i.e., through AP1 or AP2), it routes the frame to STA3, through AP1 by setting the From DS subfield of the Frame Control field to 1 and A3 (SA) to the non-AP MLD Address (i.e., MLD\_S). STA3 discards the TDLS Discovery Request frame that had the BSSID field of Link Identifier element set to BSSID of AP2 as it does not recognize the BSSID. STA3 recognizes the BSSID set to AP1 and responds with a TDLS Discovery Response frame, which is a Management frame, with the RA set to the MLD\_S and both To DS and From DS subfields set to 0. STA3 ignores the TDLS Multi-Link element as it does not recognize this element. The TDLS STA affiliated with MLD\_S receives the TDLS Discovery Response frame, which is sent on the TDLS direct link (see Table 11-11a (Frame type and their pathway in a TDLS setup)). The TDLS initiator STA Address field and the TDLS responder STA Address field contained in the Link Identifier element (denoted as LI in the figure) are carried in the TDLS Discovery Request frame and in the TDLS Discovery Response frame and are set to MLD\_S and STA3, respectively.

The same considerations apply for setting the fields in the Link Identifier element when the TDLS discovery is initiated by STA3 to establish a single link TDLS direct link with the non-AP MLD. In this scenario, since STA3 is not affiliated with a non-AP MLD and is not aware of MLD, the BSSID field of the Link Identifier element is set to the BSSID of AP1 and the TDLS Discovery Request frame does not carry a TDLS Multi-Link element.

* **TPK handshake[4031]**

***TGbe editor: Please make changes to the 4th paragraph and add NOTEs after the paragraph as shown below:***

The TDLS initiator STA and the TDLS responder STA perform the following exchange to set up a TPK:

TDLS PMK handshake message 1: TDLS initiator STA ® TDLS responder STA:

Link Identifier element, RSNE, Timeout Interval element, FTE, TDLS Multi-Link element (optionally included if the transmitting STA is affiliated with a non-AP MLD (see 35.3.20 (TDLS procedure in multi-link operation)))

TDLS PMK handshake message 2: TDLS responder STA ® TDLS initiator STA:

Link Identifier element, RSNE, Timeout Interval element, FTE, TDLS Multi-Link element (optionally included if the transmitting STA is affiliated with a non-AP MLD (see 35.3.20 (TDLS procedure in multi-link operation)))

TDLS PMK handshake message 3: TDLS initiator STA ® TDLS responder STA:

Link Identifier element, RSNE, Timeout Interval element, FTE, TDLS Multi-Link element (optionally included if the transmitting STA is affiliated with a non-AP MLD (see 35.3.20 (TDLS procedure in multi-link operation)))

where

…

***TGbe editor: The rest of the content in this paragraph is unchanged***

…

***TGbe editor: Please update the 8th paragraph in this subclause as shown below:***

The TPK shall be derived as follows when the TDLS setup frames transmitted by at least one of the participating STA does not include the TDLS Multi-Link element carrying the AP MLD MAC Address:

TPK-Key-Input = Hash(min (SNonce, ANonce) || max (SNonce, ANonce))

TPK = KDF-Hash-Length(TPK-Key-Input, “TDLS PMK”, min (MAC\_I, MAC\_R) || max (MAC\_I, MAC\_R) || BSSID) (12-0a)

where

Hash is the hash algorithm specific to the negotiated AKM (see Table 9-151 (AKM suite selectors))

KDF-Hash-Length is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF))

Length is TK\_bits + 128

TK\_bits is cipher-suite dependent and specified in Table 12-7 (Cipher suite key lengths)

MAC\_I and MAC\_R are the MAC addresses of the TDLS initiator STA and the TDLS responder STA, respectively

SNonce and ANonce are the nonces generated by the TDLS initiator STA and TDLS responder STA, respectively, for this instance of the TPK handshake.

BSSID is the BSSID of the BSS of which the TDLS initiator STA is a member.

***TGbe editor: Please add a new paragraph as the 9th paragraph in this subclause as shown below:***

The TPK shall be derived as follows when the TDLS setup frames transmitted by both peers include the TDLS Multi-Link element carrying the AP MLD MAC Address and the setup is for a single link TDLS:

TPK-Key-Input = Hash(min (SNonce, ANonce) || max (SNonce, ANonce))

TPK = KDF-Hash-Length(TPK-Key-Input, “TDLS PMK”, min (MAC\_I, MAC\_R) || max (MAC\_I, MAC\_R) || BSSID || AP MLD MAC) (12-0b)

where

Hash, KDF-Hash-Length, Length, TK\_bits, MAC\_I, MAC\_R, SNonce, ANonce and BSSID are as defined above.

AP MLD MAC is the MLD MAC address of the AP MLD with which the initiating non-AP MLD has performed multi-link setup.

* TPK handshake message 2[4031]

***TGbe editor: Please update the 1st paragraph in this subclause as shown below:***

If the TDLS responder STA validates the TPK handshake message 1 for this TDLS instance, the TDLS responder STA may respond with TPK handshake message 2. To do so, the TDLS responder STA shall add an RSNE, FTE, and Timeout Interval element to its TDLS Setup Response frame. The elements shall be formatted as follows:

…

***TGbe editor: The contents in between remain unchanged***

…

The FTE shall include the following:

ANonce shall be set to a value chosen randomly by the TDLS responder STA, see 12.7.5 (Nonce generation) for a recommended procedure.

SNonce shall be same as that received in message 1 of this sequence

The MIC shall be calculated on the concatenation, in the following order, of:

TDLS initiator STA MAC address (6 octets)

TDLS responder STA MAC address (6 octets)

Transaction Sequence number (1 octet) which shall be set to the value 2

Link Identifier element

RSNE

Timeout Interval element

FTE, with the MIC field of the FTE set to 0.

 TDLS Multi-Link element (when present)

The MIC shall be calculated using the TPK-KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.

All other fields shall be set to 0.

* TPK handshake message 3[4031]

***TGbe editor: Please update the 1st paragraph in this subclause as shown below:***

If the TDLS initiator STA responds to message 2 for this TDLS instance, the TDLS initiator STA shall add an RSNE, FTE, and Timeout Interval element to its TDLS Setup Confirm frame. The elements shall be formatted as follows:

…

***TGbe editor: The contents in between remain unchanged***

…

The MIC shall be calculated on the concatenation, in the following order, of:

TDLS initiator STA MAC address (6 octets)

TDLS responder STA MAC address (6 octets)

Transaction Sequence number (1 octet), which shall be set to the value 3

Link Identifier element

RSNE

Timeout Interval element

FTE, with the MIC field of the FTE set to 0.

 TDLS Multi-Link element (when present)

The MIC shall be calculated using the TPK-KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.

All other fields shall be set to 0.

9.4.2.295bMulti-Link element**[4031]**

9.4.2.295b.1 General

***TGbe editor: Please add a new entry and update the last entry in Table 9-33am as shown below:***

Table 9-322am—Type subfield encoding

|  |  |
| --- | --- |
| **Type Subfield value** | **Multi-link element variant name** |
| 2 | TDLS (see 9.4.2.295b.4 (TDLS Multi-Link element)) |
| 3-7 | Reserved |

***TGbe editor: Please add a new subclause shown below:***

9.4.2.259b.4 TDLS Multi-link element

The usage of TDLS Multi-Link element is described in 35.3.20 (TDLS procedure in multi-link operation).

The Presence Bitmap subfield of the Multi-Link Control field is reserved in TDLS Multi-link element when TDLS direct link discovery or setup is for a single link (see 35.3.20.2 (TDLS direct link over a single link)).

The format of the Common Info field of the TDLS Multi-Link element is defined in Figure 9-788xx1 (Format of Common Info field of the TDLS Multi-Link element).

|  |  |  |
| --- | --- | --- |
|  | Common Info Length | AP MLD MAC Address |
| Octets: | 1 | 6 |
| **Figure 9-788xx1 – Format of Common Info field of the TDLS Multi-Link element** |

The Common Info Length subfield indicates the number of octets in the Common Info field.

The AP MLD MAC Address subfield carries the MAC address of the AP MLD with which the non-AP MLD, affiliated with the transmitting STA, has performed multi-link setup.

Link Info field is not present when TDLS direct link discovery or setup is for a single link (see 35.3.20.2 (TDLS direct link over a single link)).

**9.6.7.16 TDLS Discovery Response frame format[4031]**

***TGbe Editor: Please insert the following row into*** [***Table 9-448 (TDLS Discovery Response Action field***](#bookmark143)***):***

**Table 9-448—TDLS Discovery Response Action field format**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Multi-Link | The TDLS Multi-Link element is present if the STA is affiliated with a non-AP MLD; otherwise, it is not present. |

* + - 1. **TDLS Setup Request Action field format[4031]**

***TGbe Editor: Please insert the following row into Table 9-488 (Information for TDLS Setup Request Action field):***

**Table 9-488—Information for TDLS Setup Request Action field**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Multi-Link | The TDLS Multi-Link element is present if the STA is affiliated with a non-AP MLD; otherwise, it is not present. |

* + - 1. **TDLS Setup Response Action field format[4031]**

***TGbe Editor: Please insert the following row into Table 9-489 (Information for TDLS Setup Response Action field):***

**Table 9-489—Information for TDLS Setup Response Action field**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Multi-Link | The TDLS Multi-Link element is present if the STA is affiliated with a non-AP MLD and the TDLS Setup Request frame soliciting a response carried TDLS Multi-Link element; otherwise, it is not present. |

* + - 1. **TDLS Setup Confirm Action field format[4031]**

***TGbe Editor: Please insert the following row into Table 9-490 (Information for TDLS Setup Confirm Action field):***

**Table 9-490—Information for TDLS Setup Confirm Action field**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Multi-Link | The TDLS Multi-Link element is present if the STA is affiliated with a non-AP MLD and the preceding TDLS Setup Response frames carried TDLS Multi-Link element; otherwise, it is not present. |

* + - 1. **TDLS Discovery Request Action field format[4031]**

***TGbe Editor: Please insert the following row into Table 9-498 (Information for TDLS Discovery Request Action field):***

**Table 9-498—Information for TDLS Discovery Request Action field**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Multi-Link | The TDLS Multi-Link element is present if the STA is affiliated with a non-AP MLD; otherwise, it is not present. |