IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIDs related to TDLS operation – Part 2 | | | | |
| Date: September 23, 2021 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | Montemurro.michael@gmail.com |
| Abhishek Patil | Qualcomm Inc |  |  | appatil@qti.qualcomm.com |
| George Cherian |  |  |  |
| Jouni Malinen |  |  |  |
| Duncan Ho |  |  |  |

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 1.0 and TGbe D1.4***

Revisions:

* Rev 0: Initial version
  + Updates the TPK generation steps to include MLD MAC Address of the associated AP MLD when both parties are identified to be STAs affiliated with (their respective) non-AP MLDs.
  + Added TDLS variant to Multi-Link element
  + Updates to other portions of the spec for consistency
* Rev 1: Updates based on several offline discussions with Po-Kai, Liwen, Mike, Jouni, Abhi, George, Duncan
  + The resolutions are updated to disallow the formation of a TDLS link between two non-AP MLDs and undo all changes to the TPK generation steps
  + Baseline updated to REVme D1.0 and 11be D1.4

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**  Agree with the comment. When both parties are non-AP MLDs, the common authenticator is the AP MLD (and not the AP operating on the link). The TPK generation steps need to be updated to include the MLD MAC address of the associated AP MLD (as proposed in 11-21/1436r0).  However, several months of offline discussions have not produced a mutually acceptable outcome. As a result, the members involved in the discussion have decided to keep the TPK generation steps unchanged and instead disallow TDLS between two non-AP MLDs. In other words, from security point of view, TDLS between non-AP MLDs must be disallowed if no changes are made to the TPK generation process.  The proposed change in the contribution (11-21/1436r1) requires a non-AP MLD to include TDLS Multi-Link element in the TDLS discovery frames that it transmits and not initiate TDLS setup or respond to a TDLS Setup Request frame if the other peer is determined to be a STA affiliated with a non-AP MLD.  Furthermore, clause 12.7.8.2 is updated to clearly state the assumption that the ‘common’ authenticator in case of a TDLS between a non-AP MLD and legacy STA is the intermediate AP operating on the link and hence the existing TPK generation steps require no change.  **TGbe editor, please make changes as shown in doc 11-21/1436r1 tagged 4031** |
| 8296 | Zhiqiang Han | 9.6.7.16 | 154.51 | Add Multi-Link element in this frame | as in comment. | **Revised**  Agree with the comment.  The proposed change requires a non-AP MLD to include TDLS Multi-Link element in the TDLS discovery frames that it transmits. Also see resolution to CID 4031  **TGbe editor, please make changes as shown in doc 11-21/1436r1 tagged 4031** |

**Discussion (rev 1)**

TGbe D1.4 provides rules for establishing single link TDLS between a STA of a non-AP MLD and a legacy (non-EHT) STA. In such a setup, the baseline mechanism for generating the encryption key (TPK) is applicable. Specifically, the associated AP (operating on the link) is considered as the ‘common’ authenticator for the two peers and the AP’s MAC address is included as part of the TPK generation.

TGbe D1.4 is also proposing to use the same rules for establish a single link TDLS between two non-AP MLDs. However, the mechanism for generating TPK is left unchanged and needs to be updated. Since the ‘common’ authenticator for two non-AP MLDs is the associated AP MLD (not the AP operating on the link), the TPK generation procedure needs to also include the associated AP MLD’s MAC address.

Over the past several months, there have been numerous offline discussions and debates on the topic of updating TPK generation when both sides are non-AP MLDs. However, the offline discussions have not helped come to a mutually agreeable outcome. To make progress and to meet the March 2022 deadline for producing TGbe draft 2.0, the concerned parties have agreed to explicitly disallow single link TDLS between two non-AP MLDs.

The proposed change requires a non-AP MLD to include TDLS Multi-Link element in the discovery frames that it transmits. If it is determined that both parties are non-AP MLDs, then neither side can initiate a TDLS setup or respond to a TDLS Setup Request frame from the other.

Furthermore, clause 12.7.8.2 is updated to clearly state the assumption that the ‘common’ authenticator in case of a TDLS between a non-AP MLD and legacy STA is the intermediate AP operating on the link and hence the existing TPK generation steps require no change.

----- End of discussion -----

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

**35.3.21.1 General**

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

**35.3.21.2 TDLS direct link over a single link**

***TGbe editor: Please modify the 4th paragraph as follows:***

When a non-AP MLD initiates a TDLS discovery operation, it may need to transmit more than one TDLS Discovery Request frame with the BSSID field of the Link Identifier element set to a different BSSID in each attempt. In each instance, the attempted BSSID corresponds to a different AP affiliated with the AP MLD. Since the TDLS Discovery Response frame is received over the direct link, the initiating non-AP MLD shall be able to determine the link(s) on which the peer STA is operating on.

***TGbe editor: Please add the following paragraphs after the 4th:***

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 9.4.2.312.5 (TDLS Multi-Link element)) in the TDLS Discovery Request frame, TDLS Discovery Response frame and TDLS Setup Request frame that it transmits. A TDLS STA affiliated with a non-AP MLD that has dot11EHTBaseLineFeaturesImplementedOnly equal to true shall not respond to a TDLS Discovery Request or TDLS Setup Request frame if the frame carries a TDLS Multi-Link element.

When a STA affiliated with a non-AP MLD determines that the peer STA is affiliated with a non-AP MLD, it shall not initiate a TDLS setup by transmitting a TDLS Setup Request frame to that peer STA or respond to a TDLS Setup Request frame received from that peer STA.

***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 MAC address and both To DS and From DS subfields set to 0. STA3 ignores the 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 MAC address field and the TDLS responder STA MAC 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 the MLD\_S and STA3 MAC addresses, 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 Multi-Link element.

***TGbe editor: Please delete the following paragraph as well as figures 35-23 and 35-24:***

***TGbe editor: Please update the following paragraph as shown below and delete figure 35-26:***

Figure 35-25 (TDLS direct link involving a STA affiliated with a non-AP MLD and a STA that is not affiliated with a non-AP MLD) provide examples of a single link TDLS direct link where at least one of the peer STAs is a TDLS STA affiliated with a non-AP MLD. The TA field of Data frames transmitted by the TDLS STA that is affiliated with an MLD over the direct link is set to its non-AP MLD’s MAC address. The To DS and From DS subfields of the Frame Control field of the Data frame are set to 0.

9.4.2.312 Multi-Link element**[4031]**

9.4.2.312.1 General

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

Table 9-401b—Type subfield encoding

|  |  |
| --- | --- |
| **Type Subfield value** | **Multi-link element variant name** |
| 3 | TDLS (see 9.4.2.312.5 (TDLS Multi-Link element)) |
| 4-7 | Reserved |

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

9.4.2.312.5 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 9-1002xx (Format of Common Info field of the TDLS Multi-Link element).

|  |  |  |
| --- | --- | --- |
|  | Common Info Length | AP MLD MAC Address |
| Octets: | 1 | 6 |
| **Figure 9-1002xx – 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.

The 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 9-457 (TDLS Discovery Response Action field):***

**Table 9-457—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 9-497 (Information for TDLS Setup Request Action field):***

**Table 9-497—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 Discovery Request Action field format[4031]**

***TGbe Editor: Please insert the following row into Table 9-507 (Information for TDLS Discovery Request Action field):***

**Table 9-507—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. |

* **TPK handshake security assumptions [4031]**

***TGbe editor: Please add the following new bullet to the list in this subclause:***

g) A TDLS direct link between a STA affiliated with a non-AP MLD and a STA that is not affiliated with a non-AP MLD assumes that the AP affiliated with an AP MLD operating on the link is the common authenticator and binds the AP’s MAC address for TPK generation.