IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution for CIDs related to TDLS (CC34) | | | | |
| Date: Feb 11, 2021 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |
| George Cherian |  |  |  |
| Duncan Ho |  |  |  |
| Alfred Asterjadhi |  |  |  |
| Yanjun Sun |  |  |  |
| Gaurang Naik |  |  |  |
| Menzo Wentink |  |  |  |
| Jouni Malinen |  |  |  |
| Michael Montemurro | Huawei |  |  |  |
| Stephen McCann |  |  |  |
| Guogang Huang |  |  |  |
| Po-Kai | Intel |  |  |  |
| Liwen | NXP |  |  |  |
| Srinivas Kandala | Samsung |  |  |  |
| Mark Rison |  |  |  |
| Tomo Adachi | Toshiba |  |  |  |
| Ryuichi Hirata | Sony |  |  |  |
| Jarkko Kneckt | Apple |  |  |  |
| Morteza | Facebook |  |  |  |
| Kumail |  |  |  |
| Insun | LGE |  |  |  |
| Rojan | Panasonic |  |  |  |

Abstract

This submission proposes resolutions for following CIDs received for TGbe (CC34): 1032, 1029

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: contribution was revised based on feedback received from several members (added as co-authors)
  + Special thanks to Mike M. & Jouni for their inputs on the TDLS discovery and security aspects
* Rev 2: Updated based on feedback from Stephen McCan and Guogang
* Rev 3: updates based on feedback from Stephen and Rojan
* Rev 4: updated based on additional feedback from Rojan and Menzo
  + Includes TDLS variant ML IE in the computation of MIC
  + Deleted text on setting of Responder STA MAC address since the rules are covered in baseline
  + Since all TDLS frame carry Link Identifier element, the text for setting the fields of the element is generalized

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** | **Pg/Ln** | **Section** | **Comment** | **Proposed Change** | **Resolution** |
| 1032 | Abhishek Patil | 125.51 | 35.3 | TDLS operation between a STA of a non-AP MLD and a (legacy) non-AP STA is broken. Furthermore, there are other issues that need to be addressed - for example: issue1: when the intermediate AP is an AP MLD, the frame can cross over and be received on the wrong link. issue 2: TDLS operation on an nSTR link.  These topics are discussed in doc 11-20/1692. | The commenter will provide a contribution | **Revised**  Agree in principle with the comment. Without any rules in 11be spec, legacy TDLS operation is broken – i.e., a STA affiliated with a non-AP MLD cannot form a TDLS link with a legacy STA. In addition, during TDLS discovery, a non-AP MLD cannot differentiate if the peer device on the other side is a legacy STA or a non-AP MLD. Furthermore, a non-AP MLD can’t determine which link a legacy STA is operating on. Therefore, additional considerations need to be applied during TDLS discovery such what values to set for the fields carried in the Link Identifier element. The TPK generation for TDLS also needs to be updated to consider the case when both parties are non-AP MLDs. The security rules are updated to consider AP MLD MAC address when TDLS is established between two non-AP MLDs. Several examples with figures are provided to draw attention to the various problems that are possible when establishing TDLS that involves non-AP MLD on at least one end. A separate contribution addressing CID 1490 will address NSTR handling.  **TGbe editor, please make changes as shown in doc 11-21/0240r4 tagged 1032** |
| 1029 | Abhishek Patil | 118.34 | 12.7.8 | Update 12.7.8 to cover PTK establishment for a TDLS link involving a STA of a non-AP MLD | Commenter will provide a contribution (also see details in 11-20/1692) | **Revised**  Spec text is updated to clarify the addresses used as inputs during the generation of TPK. The TPK generation is updated to cover the case when both sides are non-AP MLD. The new rules propose to include AP MLD’s MAC address in the generation of TPK in addition to the link AP’s MAC address.  **TGbe editor, please make changes as shown in doc 11-21/0240r4 tagged 1029** |

***TGbe Editor: Please note, the baselines for this document are REVmd D5.0 and 11be D0.4***

***TGbe editor: Please add the following (new) subclause after 35.3.17:***

**35.3.xx TDLS handling with multi-link operation**[1032, 1029]

**35.3.xxx.1 General**

When the frames exchanged during TDLS discovery or setup include a TDLS variant Multi-Link element without a Link Info field, the TDLS direct link discovery or setup respectively, is for a single link. When the frames exchanged during TDLS discovery or setup include a TDLS variant Multi-link element with a Link Info field, the operation is for TDLS direct link over more than one link.

A non-AP MLD that intends to establish a single link TDLS direct link with a peer STA on one of its links follows the procedures defined in 11.20 (Tunneled direct-link setup), with additional rules as defined in 35.3.xxx.2 (TDLS over a single link).

**35.3.xxx.2 TDLS direct link over a single link**

When a non-AP MLD that has performed multi-link setup with an AP MLD establishes a single link TDLS direct link on one of its links, it prepares the context (i.e., security, SN/PN, BA) for the TDLS direct link with the non-AP MLD MAC address. For ease of description, this TDLS direct link context is referred to as TDLS STA affiliated with the non-AP MLD in the rest of this subclause.

TDLS discovery and setup between a non-AP MLD and a peer STA involves frames that are sent and received via an intermediate AP (MLD) or sent and received through the direct communication (see Table 11-11a). Frames that traverse the intermediate AP (MLD) are sent or received by a STA affiliated with the non-AP MLD that is part of the multi-link setup with the AP MLD. Frames sent over the direct link are sent or received by the TDLS STA affiliated with the non-AP MLD. The TDLS direct link, when successfully established, is between the TDLS STA affiliated with the non-AP MLD and a TDLS peer STA at the other end of the direct link.

If the TDLS initiator is a non-AP MLD, then the TDLS initiator STA Address field contained in the Link Identifier element of the TDLS frames shall be set to the MLD MAC address of the non-AP MLD.

When a non-AP MLD initiates a TDLS discovery, 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. Each attempted BSSID corresponds to that of a different affiliated AP of the AP MLD that is part of the multi-link setup. 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) where the peer STA or non-AP MLD is operating on.

NOTE - Due to the nature of multi-link operation, when a Data frame traverses an AP MLD, it can be relayed on any available link. Furthermore, when a frame that was transmitted by a STA of a non-AP MLD traverses an AP MLD, the AP MLD sets the SA field to the transmitting STA’s non-AP MLD MAC address. Therefore, when an affiliated STA of a non-AP MLD receives a frame from its corresponding associated AP that is affiliated with an AP MLD, it cannot determine the link where the frame originated from and it cannot determine if the initiating STA is affiliated with a non-AP MLD or not. Consequently, the non-AP MLD initiating a TDLS discovery doesn’t know the BSSID of the link where the intended peer STA is operating on.

If the TDLS initiator STA is a non-AP MLD, then the BSSID field contained in the Link Identifier element of the TDLS frames shall be set to the BSSID of the corresponding affiliated AP of the AP MLD that is operating on the link where the TDLS direct link was established.

If a TDLS STA affiliated with a non-AP MLD transmits a TDLS frame over the direct link, then the BSSID field contained in the Link Identifier element shall be set to the BSSID of the corresponding affiliated AP of the AP MLD where the TDLS direct link was negotiated.

When both STAs, involved in TDLS setup, include the TDLS variant Multi-Link element, carrying the AP MLD MAC Address field, in the frames exchanged during 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). Otherwise, the STAs shall derive the TPK as defined in Equation (12-0a).

After a TDLS direct link is successfully established between the TDLS STA affiliated with a non-AP MLD and a TDLS peer STA at the other end of the TDLS direct link, TDLS STA and other affiliated STA(s) of the non-AP MLD shall cease transmitting MSDUs to the TDLS peer, at the other end, through their associated AP that is affiliated with the AP MLD to which the non-AP MLD has performed multi-link setup.

NOTE – The STAs affiliated with the non-AP MLD can transmit/receive frames to/from other STAs or the DS via the AP MLD.

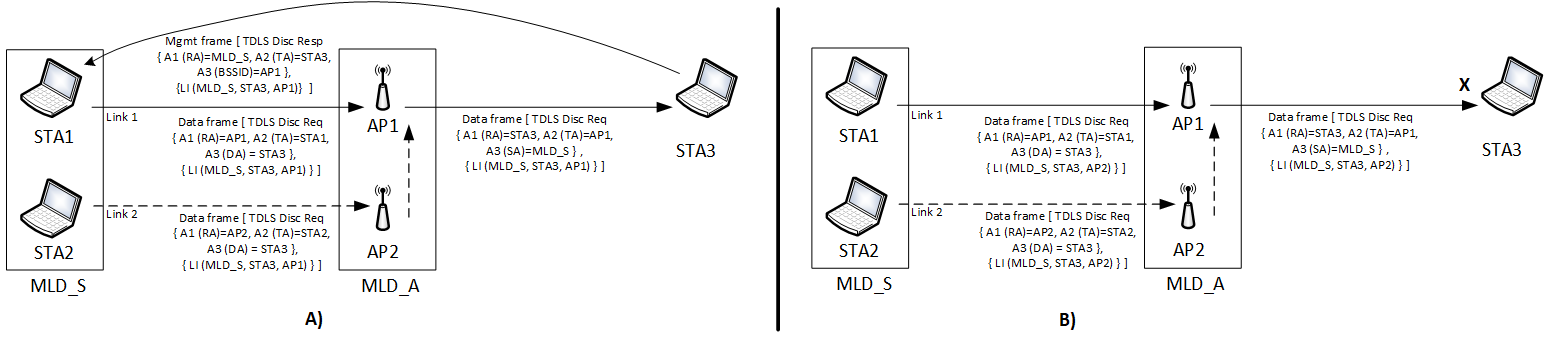


Figure 35-xx1 – Example of TDLS discovery initiated by a non-AP MLD

Figure 35-xx1 illustrates 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 the left side A) 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 the right side B). Both the frames have their A3 (DA) set to the STA3 MAC address and the ToDS 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 FromDS 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 ToDS and FromDS subfields set to 1. STA3 ignores the TDLS variant 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). 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 variant Multi-Link element.

Due to the nature of multi-link operation, it is possible that a Data frame sent by a STA is relayed on a different link when it traverses the AP MLD. As a result, it is possible that the TDLS Discovery Request frame (which is a Data frame) sent by STA3 is received on link 2. Figure 35-xx2 illustrates this case. The capabilities of each device is same as that described in Figure 35-xx1.

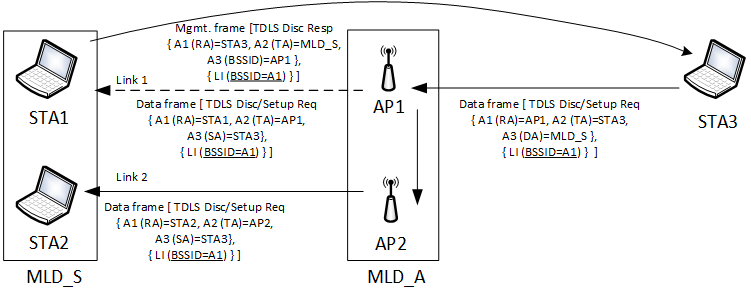


Figure 35-xx2 – Example of TDLS discovery initiated by a STA to a non-AP MLD

In Figure 35-xx2, the TDLS Discovery Request frame transmitted by STA3 has the ToDS subfield of the Frame Control field set to 1 and A3 (DA) set to non-AP MLD address (MLD\_S) since STA3 is only aware of MLD\_S and not the link addresses of STA1 or STA2 as the AP MLD sets the SA to non-AP MLD’s MAC address. In this example, when the TDLS Discovery Request frame (which is a Data frame) is received by AP1 and routed to the non-AP MLD, the AP MLD sets the FromDS subfield of the Frame Control field to 1 and the A3 (SA) to STA3 and transmits the frame either on link 2 (solid line) or link 1 (dotted line). The non-AP MLD receives the TDLS Request Discovery frame and identifies the intended TDLS direct link using the BSSID field of the Link Identifier element. In this case, the BSSID is set to AP1 (i.e., link 1), so the non-AP MLD enables the TDLS STA affiliated with the non-AP MLD on link 1. The TDLS STA affiliated with the non-AP MLD responds by transmitting a TDLS Discovery Response frame on the direct link to STA3 with the ToDS and FromDS subfields of the Frame Control field set to 0, and A1 set to STA3 (i.e. RA=STA3, TA=MLD\_S, A3=AP1). In both the TDLS Discovery Request and TDLS Discovery Response frames, the BSSID, the TDLS initiator STA Address and the TDLS responder STA Address fields in the Link Identifier element (represented as LI in the figure) are set to AP1, STA3 and MLD\_S, respectively

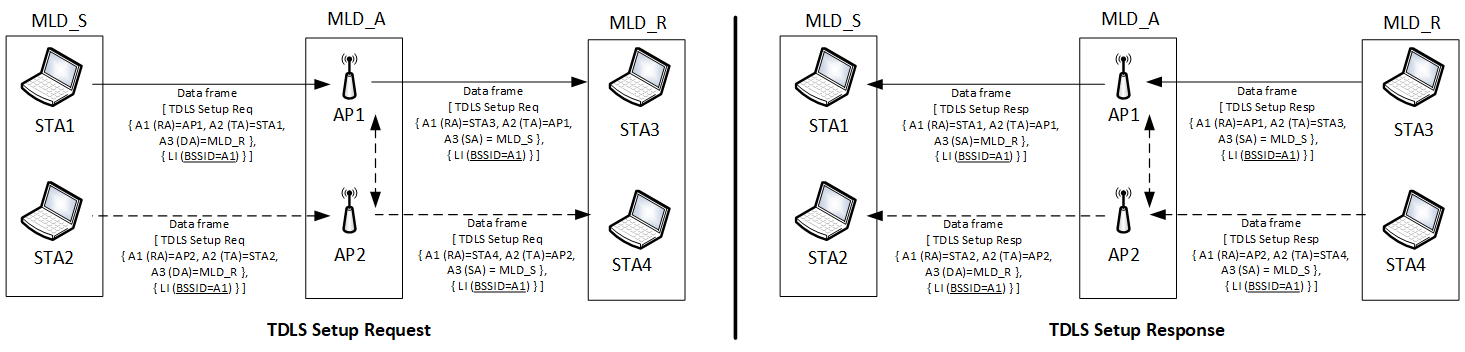


Figure 35-xx3 – TDLS Setup exchange between two STAs each affiliated with a different non-AP MLD

Figure 35-xx3 illustrates the case where a single link TDLS direct link is set up between two non-AP MLDs that have performed multi-link setup with the same AP MLD. The example assumes that the two non-AP MLDs have performed TDLS discovery and that the initiating non-AP MLD (in this example, MLD\_S) has decided to perform single link TDLS setup for link 1. As shown in the figure, the TDLS Setup Request frame is transmitted by the non-AP MLD, MLD\_S, through affiliated STA1 to MLD\_R through affiliated STA3. The BSSID field in the Link Identifier element identifies the intended link for establishing the TDLS direct link.

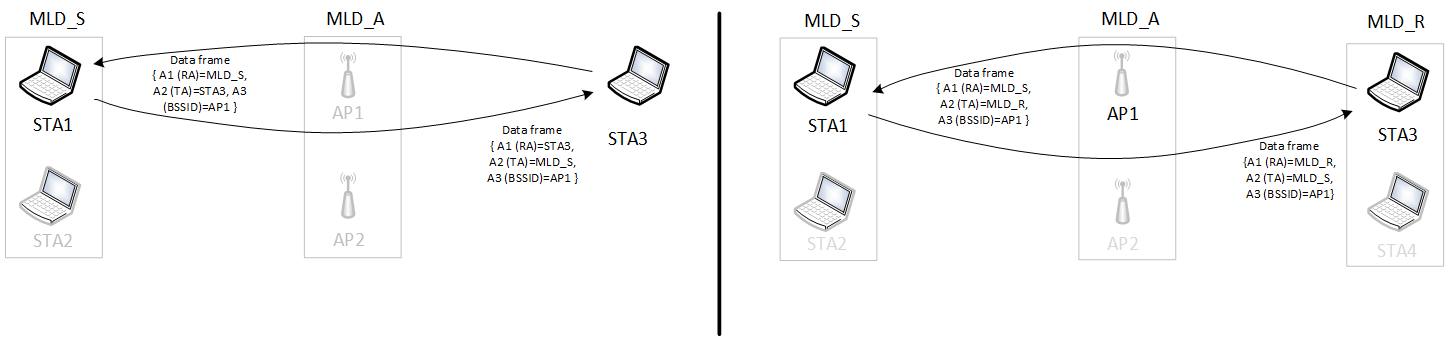


Figure 35-xx4 – Example of TDLS direct link involving a non-AP MLD

Figure 35-xx4 provides 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 ToDS and FromDS subfields of the Frame Control field are set to 0.

* **Tunneled direct-link setup**
* **General[1032]**

***TGbe editor: Please update the 14th paragraph (including adding the table) as shown below:***

TDLS frames shall use the formatting specified in 11.20.2 (TDLS payload) when they are transmitted through the AP and when they are transmitted over the TDLS direct link. A STA shall not transmit a TDLS Action field in a frame with the Type field of the frame set to Management. A received TDLS Action field in a frame with the Type field equal to Management shall be discarded. Note that the TDLS Discovery Response frame is not a TDLS frame but a Public Action frame. Table 11-11a shows the frames that can be exchanged between the TDLS peer STAs and the path taken by each of them.

**Table 11-11a – Frame type and their pathway in a TDLS setup**

|  |  |  |  |
| --- | --- | --- | --- |
| **Frame** | **Pathway (link)** | **Frame type** | **Description** |
| TDLS Discovery Request frame | Via AP | Data frame |  |
| TDLS Discovery Response frame | Direct | Public Action (Management frame) | Can be sent unsolicited (i.e., without receiving a TDLS Discovery Request frame) |
| TDLS Setup Request frame  TDLS Setup Response frame  TDLS Setup Confirm frame | Via AP | Data frame |  |
| TDLS Teardown frame | Both allowed | Data frame | The frame is sent via the AP if the TDLS peer is not reachable |
| TDLS Channel Switch Request frame  TDLS Channel Switch Response frame | Direct | Data frame |  |
| TDLS Peer PSM Request frame | Both allowed | Data frame | See 11.2.3.12 (TDLS peer power-save mode) |
| TDLS Peer PSM Response frame | Direct | Data frame |
| TDLS Peer Traffic Indication frame  TDLS Peer Traffic Response frame | Direct | Data frame |  |
| Data frame  Control frame | Direct |  | Data and Control frames exchange after TDLS session is successfully established |
| GAS frame carrying TDLS Capability ANQP-element | Direct | Public Action (Management frame) | Discovery of TDLS peer STAs. See 11.22.3.3.10 |

* **TDLS Capability procedure[1032]**

***TGbe editor: Please add the following NOTE after the last paragraph in this subclause:***

The mechanism shall work as follows:

…

***TGbe editor: The contents of the last paragraph remain unchanged***

…

NOTE – The TA field of the frame carrying a TDLS Capability ANQP-element is the non-AP MLD’s MAC address (see 35.3.xx.2 (TDLS over a single link)) when the STA transmitting the frame is affiliated with a non-AP MLD.

* **Link Identifier element[1032]**

***TGbe editor: Please modify Figure 9-388 and the 3rd, 4th and 5th paragraph in this subclause as follows:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | BSSID | TDLS initiator STA Address | TDLS responder STA Address |
| Octets: | 1 | 1 | 6 | 6 | 6 |
| Figure 9-388 – Link Identifier element format | | | | | | |

[1032]The BSSID field is set to the BSSID of the BSS of which the TDLS initiator STA is a member when the frame carrying the element is transmitted by a STA that is not affiliated with a non-AP MLD. Otherwise the BSSID field is set to the BSSID of the AP that is operating on the link where the non-AP MLD intends to establish a single link TDLS direct link.

[1032]The TDLS initiator STA Address field is set to the TDLS initiator STA’s MAC address if the STA is not affiliated with a non-AP MLD. Otherwise, the TDLS initiator STA Address field is set to the MAC address of the initiating non-AP MLD.

9.4.2.295bMulti-Link element**[1032]**

9.4.2.295b.1 General

***TGbe editor: Please add a new in Table 9-33am as shown below:***

Table 9-322am—Type subfield encoding

|  |  |
| --- | --- |
| **Type Subfield value** | **Multi-link element variant name** |
| 2 | TDLS |
| TBD | Reserved |

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

9.4.2.259b.4 TDLS variant Multi-link element

The TDLS variant Multi-link element is included in frames transmitted by a STA of a non-AP MLD during TDLS discovery and setup.

The format of the Common Info field of the TDLS variant Multi-link element is defined as in Figure 9-xxx (Common Info field of the TDLS variant Multi-link element format).

|  |  |
| --- | --- |
|  | AP MLD MAC Address |
| Octets: | 6 |
| **Figure 9-788xxx – Common Info field of the TDLS variant Multi-link element format** | |

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

* **TPK handshake[1029]**

***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 variant Multi-Link element (see NOTE)

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

Link Identifier element, RSNE, Timeout Interval element, FTE, TDLS variant Multi-Link element (see NOTE)

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

Link Identifier element, RSNE, Timeout Interval element, FTE, TDLS variant Multi-Link element (see NOTE)

where

…

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

…

The MIC field of the FTE is 0 for message 1 and computed as described in 12.7.8.4.3 (TPK handshake message 2) and 12.7.8.4.4 (TPK handshake message 3) for messages 2 and 3 respectively

NOTE – TDLS variant Multi-Link element is carried in the TDLS setup frames if it is determined, during TDLS discovery, that both sides are non-AP MLDs; Otherwise the element is not present.

***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 variant Multi-Link element carrying 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 includes the TDLS variant 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[1029]

***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 variant 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[1029]

***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 variant 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.