### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11be D1.0 CR for CID 5919 | | | | |
| Date: 2021-11-29 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation | 2200 Mission College Blvd, Santa Clara, CA 950542200 |  | po-kai.huang@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

5919

Revisions:

* Rev 0: Initial version of the document.

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 D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D1.0 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** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 5919 | Li-Hsiang Sun | 11.3.3 | 187.64 | MLD should transmit class 1, 2,3 frames at the same link because before 4-way handshake, the supplicant has not proved to the authenticator the MAC address of other links are authentic | add the requirement of sending frames on the same link before state 4 | Revised –  We note that class 1 frame (ex probe request, beacon, public action) can be transmitted before association without the need of any security consideration. Hence, it is not reasonable to limit the exchange this way. Similarly, control frame is transmitted without security consideration, so limiting the exchange of control frame this way is not reasonable either. As for data frame and management frame, data frame exchange under RSNA has control port blocked before state 4, and protected management requires PTK, which is only available after state 4 anyway.  However, we note that there are various texts in the spec assume that the exchange of 4-way handshake should happen on the same link used to exchange (re)association request/response frame. For example, in message 2, the link information KDE only includes the information that is carried in the multi-link element of the (re)assocaiton request, which only makes sense if the 4-way handshake happens at the same link as the one used for (re)association request/response exchange.  Offline discussion indicates that non-AP MLD can control this by having the link they want to exchange set to active mode. We then only adjust the texts of 4-way and TID to link mapping to make sure that if non-AP MLD wants, then it is possible to control 4-way all in the same link. If they do not want to, then data frame can be sent in any link.  Finally, we ensure that the 4 message exchange for the FT over-the air protocol will also use the same AP-STA pair because that is the same authentication frame exchange and follows the rule agreed for the normal 2 way exchange of authentication.  We add texts toward this direction to close the gap in the spec.  TGbe editor to make the changes shown in 11-21/1770r0 under all headings that include CID 5919. |

**Discussion:**

We note that there are various texts in the spec assume that the exchange of 4-way handshake should happen on the same link used to exchange (re)association request/response frame. For example, in message 2, the link information KDE only includes the information that is carried in the multi-link element of the (re)assocaiton request, which only makes sense if the 4-way handshake happens at the same link as the one used for (re)association request/response exchange.

*An MLO Link KDE is included for each affiliated STA link of an MLD. When included in  
message 2, an MLO Link KDE is included for each link and contains the LinkId field and  
corresponding affiliated STA MAC address received in the Multi-Link element by the AP MLD in  
the (Re)Association Request frame.*

Having 4-way handshake happens at the same link is also helpful for non-AP MLD to prepare the 4-way exchange message without considering the case that the peer MLD is jumping link for the exchange. Offline discussion indicates that non-AP MLD can control this by having the link they want to exchange set to active mode. We then only adjust the texts of 4-way and TID to link mapping.

In the same spirit, we ensure that FT 4-way also happens in the same link. Finally, we ensure that the 4 message exchange for the FT over-the air protocol will also use the same AP-STA pair because that is the same authentication frame exchange and follows the rule agreed for the normal 2 way exchange of authentication.

*For a destination MLD, an Authentication frame that is constructed using the appropriate procedure to complete the authentication procedure shall have the Address 1 field equal to the MAC address of the STA affiliated with the originating MLD that sends the Authentication frame with authentication transaction sequence number equal to 1.*

We add texts toward this direction to close the gap in the spec.

**Propose:**

***TGbe editor: Add the following bullet at the end of the third paragprah in 12.7.6.1 General 4-way handshake* *as follows: (track change on)***

**12.7.6 4-way handshake**

**12.7.6.1 General**

***Change the third paragraph as follows:***

The following apply:

(..existing bullets…)

* (#2290)For MLO, each message of the 4-way handshake contains an MAC Address KDE  
  containing the MLD MAC address of the Authenticator or Supplicant that is sending the message.

(#2290)An MLO Link KDE is included for each affiliated STA link of an MLD. When included in message 2, an MLO Link KDE is included and contains the LinkId field and corresponding affiliated STA MAC address for each requested link except the link used to send message 2(#5919). When included in message 3, an MLO Link KDE is included for each affiliated AP link and contains the LinkId field, corresponding affiliated AP MAC address, RSNE, and RSNXE for each affiliated AP that was sent by the Authenticator in Beacons, Probe Response, and ML Probe Response frames.

***TGbe editor: Add the following bullet at the end of the third paragprah in 12.7.6.3 4-way handshake message 2 as follows: (track change on)***

**12.7.6.3 4-way handshake message 2  
*Change the first paragraph as follows:***

(..existing texts…)

Key Data =

(..existing bullets…)

* (#2290)For MLO, a MAC Address KDE containing the MLD MAC address of the  
  Supplicant.
* (#2290)For MLO, an MLO Link KDE for each affiliated STA link containing the  
  affiliated STA MAC address for each requested link except the link used to send message 2 (#5919).

***Change the last paragraph as follows:***

Otherwise, the Authenticator:

Otherwise, the Authenticator:  
 a) Derives PTK.  
 b) Verifies the message 2 MIC or AEAD decryption operation result.  
 1) If the calculated MIC does not match the MIC that the Supplicant included in the EAPOL-Key  
 frame or the AEAD decryption operation returns failure, the Authenticator silently discards  
 message 2.  
 2) If the MIC or AEAD decryption is valid and this message 2 is part of a fast BSS transition  
 initial mobility domain association or an association started through the FT protocol, the  
 Authenticator checks that all fields of the RSNE other than the PMKID List field and, if  
 present, the RSNXE bitwise matches the fields from the (Re)Association Request frame and  
 that the FTE and MDE are the same as those provided in the AP’s (Re)Association Response  
 frame. If the MIC or AEAD decryption is valid and this message 2 is not part of a fast BSS  
 transition initial mobility domain association and this message 2 is not part of an association  
 started through the FT protocol, the Authenticator checks that the RSNE and, if present, the  
 RSNXE bitwise matches that from the (Re)Association Request frame. (#2290)For MLO,  
 validates that the affiliated STA MAC addresses are the same for each affiliated STA MAC  
 address of the requested

link(#5919).

(..existing texts…)

***TGbe editor: Add the following sentence in 13.7.1 FT reassociation in an RSN* *as follows: (track change on)***

***13.8 FT authentication sequence  
13.8.1 Overview***

(…existing texts…)

1. The first message is used by the FTO to initiate a fast BSS transition. When RSNA is enabled, the FTO shall
2. include the R0KH-ID and the SNonce in the FTE and the PMKR0Name in the RSNE. The target

46

1. (#5070)~~AP~~FTR can use the PMKR0Name to derive the PMKR1Name, and if the target (#5070)~~AP~~FTR does
2. not have the PMK-R1 identified by PMKR1Name, it may attempt to retrieve that key from the R0KH
3. identified by R0KH-ID. See [13.2 (Key holders).](#bookmark0) The FTO includes a fresh SNonce as its contribution to the
4. association instance identifier and to provide key separation of the derived PTK; it is selected randomly to

serve as a challenge that demonstrates the liveness of the peer in the fourth message.

52

1. The second message is used by the target (#5070)~~AP~~FTR to respond to the requesting FTO. The target
2. (#5070)~~AP~~FTR provides the key holder identifiers and key names used to generate the PTK. The target
3. (#5070)~~AP~~FTR also includes a fresh ANonce as its contribution to the association instance identifier and to
4. provide key separation of the derived PTK. The response includes a status code.

58

59

1. In an RSN, the third message is used by the FTO to assert to the target (#5070)~~AP~~FTR that it has a valid
2. PTK. If no resources are required, then the FTO omits inclusion of the RIC.

62

63 The fourth message is used by the target (#5070)~~AP~~FTR to respond to the requesting FTO. This message

64

1. serves as final confirmation of the transition, establishes that the (#5070)~~AP~~FTR possesses the PMK-R1 and is participating in this association instance, and protects against downgrade attacks. Note, however, that the RIC is absent if no resources were requested in the third message. This also includes a status code and may include a reassociation deadline.

If the requesting FTO is an non-AP MLD, the target FTR is an AP MLD, and the first message is sent over the air, the following apply:

* the third message sent over the air shall have the value of the Address 1 field equal to the value of the Address 1 field of the first message and the value of the Address 2 field equal to the value of the Address 2 field of the first message
* the second and fourth message sent over the air shall have the value of the Address 1 field equal to the value of the Address 2 field of the first message and the value of the Address 2 field equal to the value of the Address 1 field of the first message. (#5919)

(…existing texts…)

***TGbe editor: Modify 35.3.6.1.3 Negotiation of TID-to-link mapping as follows: (track change on)***

***35.3.6.1.3 Negotiation of TID-to-link mapping***

(…existing texts…)

After the multi-link (re)setup is successful and 4-way handshake is complete (if RSNA is required) (#5919), to negotiate a new TID-to-link mapping, an initiating MLD with dot11TIDtoLinkMappingActivated equal to true shall send an individually addressed TID-to-link Mapping Request frame to a responding MLD that has indicated support of TID-to-link mapping negotiation.

(…existing texts…)