### IEEE P802.11Wireless 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 |
| Duncan Ho | Qualcomm |  |  |  |
| Mike Montemurro | Huawei |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

5919

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the comments received offline.
* Rev 2: Another bug fix to clarify one RSNE and one RSXNE from non-AP MLD
* Rev 3: Editorial fix

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 the latest (re)association request/response exchange. As a result, we provide text to clarify this point and adjust texts for TID to link mapping to make this possible.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.We also explicitly clarify that there is only one RSNE and one RSNXE inserted into (re)association request frame initiated by non-AP MLD.TGbe editor to make the changes shown in 11-21/1770r3 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. As a result, we add texts to clarify this point.

*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.*

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 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…)

**----------------------------------------------------------start option 1---------------------------------------------------**

***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 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. 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.For MLO, if RSNA has not been established, each message of the 4-way handshake shall be sent in the same link used by the latest exchange of successful (Re)Association Request/Response frame. (#5919)

***TGbe editor: Add the following sentence in 13.4.2 FT initial mobility domain association in an RSN as follows: (track change on)***

**13.4.2 FT initial mobility domain association in an RSN**

 (….existing texts…)

Between a non-AP MLD and an AP MLD, the FT 4-way handshake is as follows:

 R1KHS1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {MAC Address})

S1KHR1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE[PMKR1Name], MDE, FTE,

RSNXE, MAC Address, MLO Linkn})

R1KHS1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {MAC Address, MLO Linkn with

 RSNE[PMKR1Name], MDE, MLO GTKn, MLO IGTKn, MLO BIGTKn, FTE, TIE[Reassociation- Deadline], TIE[KeyLifetime]})

12

 S1KHR1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {MAC Address})

where MLO GTKn is the MLO GTK KDE for link n, MLO IGTKn is the MLO IGTK KDE for link n, and

16

MLO BIGTKn is the MLO BIGTK KDE for link n.

NOTE—MAC Address KDE is the MLD MAC address of the MLD with which the transmitting STA is affiliated. See

12.7.4 (EAPOL-Key frame notation). 21

Between a non-AP MLD and an AP MLD, if RSNA has not been established, each message of the FT 4-way handshake shall be sent in the same link used by the latest exchange of successful (Re)Association Request/Response frame. (#5919)

***TGbe editor: Modify* 12.6.21 RSNA rekeying *as follows: (track change on)***

**12.6.21 RSNA rekeying**(M117)When a PTKSA is deleted, a non-AP and non-PCP STA may reassociate with the same AP or PCP and/
or establish a new RSNA with the AP or PCP. When a PTKSA is deleted, a non-AP MLD may reassociate with the same AP MLD and/or establish a new RSNA with the AP MLD. (#5919)… (existing texts)….

(#2500)An Authenticator may initiate a 4-way handshake for the purpose of renewing the key associated with
a PTKSA. A supplicant may send an EAPOL request message to the authenticator to request rekeying. In
addition, if both the Authenticator and the Supplicant support multiple keys for individually addressed traffic, a
smooth switchover to the new key is possible using the following procedure.

Between a non-AP MLD and an AP MLD, if RSNA has been established, each message of the 4-way handshake or FT 4-way handshake shall be sent in the same link. (#5919)

… (existing texts)….

(#2500)A PTKSA has a limited lifetime, either in absolute time or due to exhausting the PN space. To maintain
an uninterrupted security association, a STA or MLD should establish a new PTKSA prior to the expiration of the old PTKSA. (#5919)

… (existing texts)….

***TGbe editor: Modify 12.6.3 RSNA policy selection in an infrastructure BSS as follows: (track change on)***

**12.6.3 RSNA policy selection in an infrastructure BSS**

 ***Insert a new subclause General before the beginning of the first paragraph (“The requirements
in this subclause”):***

**12.6.3.1 General**

 ***Change the fourth paragraph as follows:***

An SME initiating an association shall insert an RSNE into its (Re)Association Request via the MLMEASSOCIATE.request or MLME-REASSOCIATE.request primitive, when the targeted AP indicates RSNA
support. The initiating STA’s RSNE shall include one authentication and pairwise cipher suite from among
those advertised by the targeted AP in its Beacon and Probe Response frames. It shall also specify the group
cipher suite specified by the targeted AP. For MLO, there shall be only one RSNE and RSNXE inserted into the (Re)Association Request frame initiated by the non-AP MLD.(#5919)

(#6596)(#1578)(#2482)For MLO, the initiating non-AP MLD’sRSNE shall include one AKM suite selector, one pairwise cipher suite selector, and one group cipher suite
selector that are common among those advertised by the APs affiliated with the targeted AP MLD. A non-AP
MLD would determine the appropriate AKM suite selector and pairwise cipher suite selector during MLO
discovery by monitoring Beacon frames transmitted by APs affiliated with the AP MLD or performing basic
probing with each AP affiliated with the AP MLD or by performing ML probing with one or more APs
affiliated with the AP MLD. If at least one RSNE field from the AP’s RSNE fails to overlap with any value the
STA supports, the STA shall decline to associate with that AP. An HT STA shall eliminate TKIP as a choice for
the pairwise cipher suite if CCMP-128 or CCMP-256 is advertised by the AP or if the AP included an HT
Capabilities element in its Beacon and Probe Response frames. The elimination of TKIP as a choice for the
pairwise cipher suite may result in a lack of overlap of the remaining pairwise cipher suite choices, in which
case the STA shall decline to create an RSN association with that AP.