IEEE P802.11
Wireless LANs

|  |
| --- |
| 11be D4.0 CR for 13 |
| Date: 2023-08-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions for the following CIDs:

19231, 19232, 19519, 19058, 19233, 19234, 19388, 19756, 19117, 19196,

19059, 19060, 19061, 19901

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Add header.
* Rev 2: Format change.

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 D4.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D4.0 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** |
| 19231 | John Wullert | 13.2.2 | 441.12 | Text refers to situations where "the R1KH identifies an AP MLD", but it is not clear how a key holder would identify another device. | Change "R1KH" to "R1KH-ID" | Revised – Based on the following spec texts, R1KH is part of the key management for AP or AP MLD.“The R0KH and R1KH are part of AP’s or AP MLD’s SME RSNA key management.”We simplify the texts to “For non-MLO” and “For MLO”.TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19231 |
| 19232 | John Wullert | 13.2.2 | 441.19 | Text refers to situations where "the R1KH identifies an AP MLD", but it is not clear how a key holder would identify a device. | Change "R1KH" to "R1KH-ID" | Revised – Based on the following spec texts, R1KH is part of the key management for AP or AP MLD.“The R0KH and R1KH are part of AP’s or AP MLD’s SME RSNA key management.”We simplify the texts to “For non-MLO” and “For MLO”.TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19232 |
| 19519 | Michael Montemurro | 13.5.3 | 39.43 | [WFA-R] The figure should be updated to keep the text between the lines. | As in comment | Revised – We note that this is a baseline revme issue. However, we try to do the editorial change to move the texts between lines.TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19519 |
| 19058 | Po-Kai Huang | 13.7.1 | 457.45 | Similar to 4-way, we may want to verify AP MAC address during FT exchange. | Add the following after "If the Reassociation Response frame includes the RSNXE, ....": "If FTR is an AP MLD and in the Reassociation Response frame, the affiliated AP MAC address for each link in the Basic Multi-Link element are not identical to the corresponding AP MAC address received in the Beacon and Probe Response frames from the corresponding AP affiliated with the FTR or in the multi-link probe response frame from the FTR, the S1KH of the FTO shall discard the response." | Revised – Agree in principle with the commenter. We tweak the language by moving the location of “received” and add “target” before FTR.TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19058 |
| 19233 | John Wullert | 13.7.1 | 456.44 | Using definite article "the" to refer to two different instances of the Reassociation Request frame is confusing. | Change "the Resassociation Request frame" to "a Reassociation Request frame" at the beginning of both sentences in this paragraph. | Rejected – In the beginning of 13.7.1, a Reassociation Request/Response frame is described for the exchange between FTO and target FTR. In the following, “the” is used to referred to that specific frame for the exchange.  |
| 19234 | John Wullert | 13.7.1 | 457.44 | Using definite article "the" to refer to two different instances of the Reassociation Response frame is confusing. | Change "the Resassociation Response frame" to "a Reassociation Response frame" at the beginning of both sentences in this paragraph. | Rejected – In the beginning of 13.7.1, a Reassociation Request/Response frame is described for the exchange between FTO and target FTR. In the following, “the” is used to referred to that specific frame for the exchange.  |
| 19388 | Thomas Derham | 13.7.1 | 2994.40 | "... in the Reassociation Response frame the RSNE fields other than...".It is unclear \*which\* RSNE this refers to, since one (either implicit/inherited, or explicit) is specified for each link.Similar issue for RSNXE in para starting line 51 | Clarify the matching requirement applies to each link.Clarify that the RSNE/RSNXE being matched (in Reassoc Resp) is the one corresponding to each link, and it needs to match that link's RSNE/RSNXE in beacons/probes. | Revised – We assume the commenter is pointing out the phrases in 457.48.The existing text specifies RSNE fields “of each link”. The intention of the texts does not go and repeat the complicated inheritance rules. We change “of” to “corresponding to” as suggested by the commenter.*if in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field of each link are not identical to the corresponding RSNE fields of the link in the Beacon and Probe Response frames received from any AP affiliated with the FTR if the FTR is an AP MLD*We also tweak the RSNXE texts to follow the RSNE texts although we note that for AP MLD, RSNXE of each AP is actually the same. TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19388 |
| 19756 | Abhishek Patil | 13.7.1 | 457.54 | If the affiliated AP MAC address(es) for each link do not match the MAC address(es) received in Beacon or Probe Response frame from the affiliated AP(s), then the FTO must discard the response. Add a paragraph to that effect (also see 11-23/743r2 bugfix 17616) | As in comment | Revised – Agree in principle with the commenter. TGbe editor to make the changes shown in 11-23/1382r2 under all headings that include CID 19058 |
| 19117 | Akira Kishida | 13.8.1 | 460.01 | Replace "an non-AP MLD" with "a non-AP MLD" in the first sentence. | As in the comment. | Accepted -  |
| 19196 | Yusuke Asai | 13.8.1 | 460.01 | "an non-AP MLD" should be "a non-AP MLD" | As in the comment. | Accepted - |
| 19059 | Po-Kai Huang | 13.8.5 | 463.05 | tweak the language to say RSNEs corresponding to requested links that exists in case that the requested link does not exist and not responded in (re)associaiton response | change "RSNEs corresponding to all requested links" to "RSNEs corresponding to all requested links that exist" | Accepted -  |
| 19060 | Po-Kai Huang | 13.8.5 | 463.17 | tweak the language to say RSNXEs corresponding to requested links that exists in case that the requested link does not exist and not responded in (re)associaiton response | change "RSNXEs (if present) corresponding to all requested links " to "RSNXEs (if present) corresponding to all requested links that exist " | Accepted - |
| 19061 | Po-Kai Huang | 13.8.5 | 463.20 | tweak the language to say AP MAC Addressess corresponding to requested links that exists in case that the requested link does not exist and not responded in (re)associaiton response | change "AP MAC address corresponding to all requested links " to "AP MAC address corresponding to all requested links that exist" | Accepted - |
| 19901 | Liwen Chu | 13.11.2 | 466.23 | Given that TSPEC and BA parameters being carried for resoure request in FT, the SCS and R-TWT parameters should also be added. | As in comment. | Rejected – R-TWT can already be negotiated in (re)association request/response frame exchange. The commenter does not provide enough details on why SCS needs to be added. |

**Discussion:**

*TGbe editor: Change Clause 13.2.2 as follows (track change on):*

* + 1. **Authenticator key holders**

***Change the seventh paragraph as follows:***

The R1KH shall meet the following requirements:

* The R1KH-ID shall be set to a MAC address of the physical entity that stores the PMK-R1 and uses it to generate the PTK. That same MAC address shall be used to advertise the PMK-R1 identity to the STA or non-AP MLD and the R0KH.
* For non-MLO, the R1KH shall derive and distribute the GTK and IGTK to all connected STAs. For MLO, the R1KH shall distribute the GTKs and IGTKs for setup links to all connected non-AP MLDs.(#19231)
* If WUR frame protection is enabled, the R1KH shall derive and distribute the IWGTK and WIPN to all WUR non-AP STAs with which the R1KH has negotiated WUR frame protection.
* For non-MLO, if beacon protection is enabled, the R1KH shall derive and distribute the BIGTK and BIPN to all connected STAs. For MLO, the R1KH shall derive and distribute the BIGTKs and BIPNs for setup links to all connected non-AP MLDs.(#19232)
* When the PMK-R1 lifetime expires, the R1KH shall delete the PMK-R1 PMKSA and shall revoke all PTKSAs derived from the PMK-R1 using the MLME-DELETEKEYS primitive.
* The R1KH shall not expose the PMK-R1 to other parties.

*TGbe editor: Change Figure 13-6—Over-the-DS FT protocol in an RSN as follows (track change on):(#19519)*



*TGbe editor: Change Clause 13.7.1 as follows (track change on):*

* 1. **FT reassociation**
		1. **FT reassociation in an RSN**

***Change the first three paragraphs as follows:***

If the FTO does not send a Reassociation Request frame to the target ~~AP~~FTR within the reassociation deadline interval received during the FT initial mobility domain association, the target ~~AP~~FTR may delete the PTKSA, and the FTO shall abandon this transition attempt.

The FTO shall perform a reassociation directly with the target ~~AP~~FTR via the following exchange:

FTOTarget ~~AP~~FTR: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request, RSNXE, Basic Multi-Link element)

Target ~~AP~~FTRFTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N], IGTK[M], BIGTK[Q], WIGTK[R], MLO GTKn, MLO

IGTKn, MLO BIGTKn], RIC-Response, RSNXE, Basic Multi-Link element)

where

* MLO GTK is the MLO GTK subelement for the AP affiliated with the AP MLD for the link speci- fied by the value in the Link ID field,
* MLO IGTK is the MLO IGTK subelement for the AP affiliated with the AP MLD for the link speci- fied by the value in the Link ID field,
* MLO BIGTK is the MLO BIGTK subelement for the AP affiliated with the AP MLD for the link specified by the value in the Link ID field.
* The GTK[N], IGTK[M], and BIGTK[Q] are present when the FTR is an AP.
* The MLO GTKn, MLO IGTKn, MLO BIGTKn, and the Basic Multi-Link element are present when the FTR is an AP MLD.

The SME of the FTO initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the ~~AP~~FTR responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.6 (Association, reassociation, and disassociation).

***Change the fourth paragraph, including splitting it into two paragraphs as follows:***

In the Reassociation Request frame that does not include the Basic Multi-Link element, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS. In the Reassociation Request frame that includes the Basic Multi- Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.2 (Multi-link device addressing).

The elements in the frame, the element contents, and the MIC calculation shall be as given in [13.8.4 (FT](#bookmark10) [authentication sequence: contents of third message).](#bookmark10)

***Change the now-shifted sixth, seventh, eighth, ninth, and tenth paragraphs as follows:***

The R1KH of the target ~~AP~~FTR verifies the MIC in the FTE in the Reassociation Request frame and shall discard the request if the MIC is incorrect.

If the target ~~AP~~FTR is an AP that includes an RSNXE in its Beacon and Probe Response frames and the RSNXE Used subfield of the MIC Control field of the FTE is set to 1 or if the target FTR is an AP MLD and any AP affiliated with the AP MLD includes an RSNXE in its Beacon and Probe Response frames and the

RSNXE Used subfield of the MIC Control field of the FTE is set to 1, but the Reassociation Request frame does not include an RSNXE, the R1KH of the target ~~AP~~FTR shall discard the request.

If dot11RSNAOperatingChannelValidationActivated is true and the FTO indicates OCVC, the target ~~AP~~FTR shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true:

* OCI subelement is present
* Channel information in the OCI matches the current operating channel parameters of the link where the (Re)Association Request/Response frames are exchanged (see 12.2.9 (Requirements for Operat- ing Channel Validation))

Otherwise, the ~~AP~~target FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE.

If the contents of the MDE received by the target ~~AP~~FTR do not match the contents advertised in the Beacon and Probe Response frames if the FTR is an AP or in the Beacon and Probe Response frames of any APs affiliated with the FTR if the FTR is an AP MLD, the target ~~AP~~FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE. If the FTE in the Reassociation Request frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce, the ~~AP~~FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE. If the RSNE in the Reassociation Request frame contains an invalid PMKR1Name, the ~~AP~~FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_PMKID.

***Change the now-shifted 11th paragraph, including splitting it into two paragraphs as follows:***

In the Reassociation Response frame that does not include the Basic Multi-Link element, the SA field of the message header shall be set to the BSSID of the target AP’s BSS, and the DA field of the message header shall be set to the MAC address of the FTO. In the Reassociation Response frame that includes the Basic Multi-Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.2 (Multi-link device addressing).

The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, the element contents, and the MIC calculation shall be as given in [13.8.5 (FT authentication](#bookmark11) [sequence: contents of fourth message).](#bookmark11)

***Change the now-shifted 14th, 15th, 16th, and 17th paragraphs as follows:***

If in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field are not identical to the corresponding RSNE fields in the Beacon and Probe Response frames received from the target ~~AP~~FTR if the target FTR is an AP or if in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field corresponding to(#19388) each link are not identical to the corresponding RSNE fields of the link in the Beacon and Probe Response frames received from the corresponding AP affiliated with the target FTR or in the multi-link probe response frame received from the target FTR if the target FTR(#19388) is an AP MLD, the S1KH of the FTO shall discard the response. If the PMKID List field does not include the correct PMKR1Name value, the S1KH of the FTO shall discard the response.

If the Beacon and Probe Response frames received from the target ~~AP~~FTR if the target(#19388) FTR is an AP or Beacon and Probe Response frames received from an AP affiliated with the target FTR if the target(#19388) FTR is an AP MLD did not include an RSNXE, but the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, the S1KH of the FTO shall discard the response.

If the Reassociation Response frame includes the RSNXE, the S1KH of the FTO shall verify that this element matches information included in the Beacon and Probe Response frames received from the target ~~AP~~FTR if the target(#19388) FTR is an AP or the S1KH of the FTO shall verify that the RSNXE corresponding to each link is identical to the corresponding RSNXE of the link in the Beacon and Probe Response frames received from the corresponding AP affiliated with the target FTR or in the multi-link probe response frame received from the target FTR if the target FTR is an AP MLD. (#19388) If those frames did not include the RSNXE or if the RSNXEs are not identical, the S1KH of the FTO shall discard the response.

If the target FTR is an AP MLD and in the Reassociation Response frame, the affiliated AP MAC address for each link in the Basic Multi-Link element are not identical to the corresponding AP MAC address in the Beacon and Probe Response frames received from the corresponding AP affiliated with the target FTR or in the multi-link probe response frame received from the target FTR, the S1KH of the FTO shall discard the response.(#19058)

(…existing texts…)

*TGbe editor: Change Clause 13.8.1 as follows (track change on):*

* 1. **FT authentication sequence**
		1. **Overview**

***Insert the following paragraph as the last paragraph of the subclause as follows:***

(…existing texts…)

If the requesting FTO is a(#19117) 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.

*TGbe editor: Change Clause 13.8.5 as follows (track change on):*

* + 1. **FT authentication sequence: contents of fourth message**

***Change the second paragraph as follows:***

If present, the RSNE(s) shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR1Name
* All other fields of the Information field shall be identical to the contents of the RSNE advertised by the target ~~AP~~FTR if the FTR is an AP or an AP affiliated with the target FTR if the FTR is an AP MLD in Beacon and Probe Response frames.

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

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the target AP or an AP affiliated with the target AP MLD includes an RSNXE in its Beacon and Probe Response frames; otherwise, this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC, the Authenticator shall include FT OCI subelement in FTE.
* When this message of the authentication sequence appears in a Reassociation Response frame, the Optional Parameter(s) field in the FTE may include the GTK, IGTK, BIGTK, and WIGTK subelements or MLO GTK, MLO IGTK, and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK, ~~or~~ WIGTK, an MLO GTK, an MLO IGTK, or an MLO BIGTK are included, the Key field of the subelement shall be wrapped using PTK-KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-11 (Integrity and key wrap algorithms) and 12.7.2 (EAPOL-Key frames). The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received message, the receiver shall ignore this trailing padding. Addition of padding does not change the value of the Key Length field. Note that the length of the encrypted Key field can be determined from the length of the GTK, IGTK, BIGTK, ~~or~~ WIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.

***Editor’s Note: Do we need to add the MLO WIGTK subelement?***

* When the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9, the MIC shall be calculated using the PTK-KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC algorithm shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:13, the MIC shall be calculated using the PTK-KCK and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:16, the MIC shall be calculated using the KCK2 and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:17, the MIC shall be calculated using the KCK2 and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:25, the MIC shall be calculated using the PTK-KCK and the HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 algorithm when the length of the PTK- KCK in bits in 128/192/256. The output of the HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA- 512 shall be truncated to 128/192/256 bits.
* The MIC shall be calculated on the concatenation of the following data, in the order given here:
	+ FTO’s MAC address (6 octets)
	+ Target ~~AP’s~~FTR’s MAC address (6 octets)
	+ Transaction sequence number (1 octet), which shall be set to the value 6 if this is a Reassociation Response frame or, otherwise, set to the value 4
	+ RSNE if Basic Multi-Link element is not included in the Reassociation Response frame
	+ RSNEs corresponding to all requested links that exist(#19059) in increasing order of link ID if Basic Multi-Link element is included in the Reassociation Response frame
	+ MDE
	+ FTE and corresponding Fragment element(s) (if FTE is fragmented), with the MIC field of the FTE set to 0
	+ Contents of the RIC-Response (if present)
	+ RSNXE (if present) if Basic Multi-Link element is not included in the Reassociation Response frame
	+ RSNXEs (if present) corresponding to all requested links that exist(#19060) in increasing order of link ID if Basic Multi-Link element is included in the Reassociation Response frame
	+ AP MAC address corresponding to all requested links that exist(#19061) in increasing order of link ID if Basic Multi-Link element is included in the Reassociation Response frame
* All other fields shall be set to 0.

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

The RSNXE shall be present if an RSNXE was present in the third message and the target ~~AP~~FTR if the FTR is an AP or an AP affiliated with the target FTR if the FTR is an AP MLD set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.