### IEEE P802.11Wireless LANs

|  |
| --- |
| 11be D1.0 CR for CR for Miscellaneous CIDs Part II |
| Date: 2022-04-04 |
| 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:

5303, 5275, 6642, 8338, 6629, 4049, 6359, 6182, 5184, 5356, 7434

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the discussion with Abhi
* Rev 2: Revision based on the discussion in teleconference
* Rev 3: Revision for CID 5303, 5275, 6642, 8338 based on the discussion offline
* Rev 4: Revision for CID 5303 based on the discussion with Mike. Changes are hightlight with green.
* Rev 5: Revision for CID 6642 based on the discussion with Jason and Yongho. Changes are marked with blue.
* Rev 6: Editorial change based on the teleconference discussion.

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** |
| 5303 | Jarkko Kneckt | 35.3.5.3 | 257.35 | Please allow ML element to contain zero or more Per-STA Profiles. It is important that AP MLD does not need to fail ML associations when only a single link is allowed to setup with AP MLD. 802.11be STAs should be able to setup any number of links with ML authenticaton and ML association. Different signaling for single link setup adds delays, complexity and overheads. | Please change:"one or more" to "zero or more" | Revised – For the problem of MLD association with only one link, we note that it is possible that AP MLD only supports 2.4 GHz and 5 GHz, and non-AP MLD only supports 5 GHz and 6 GHz. As a result, the only overlapping link is 5 GHz, and this is a strong reason why you need to enable MLD association with only one link if client prefers to use MLD association for all AP MLDs all the time.We clarify the case of zero or more per-STA profiles, fix a bug, and clarify the corresponding 4-way handshake signaling. TGbe editor to make the changes shown in 11-21/599r6 under all headings that include CID 5303. |
| 5275 | Insun Jang | 35.3.5.4 | 256.33 | Single-link setup cases between MLDs should be considered, e.g., non-AP MLD requests one link or AP MLD accepts one link only | 5275 | Revised – For the problem of MLD association with only one link, we note that it is possible that AP MLD only supports 2.4 GHz and 5 GHz, and non-AP MLD only supports 5 GHz and 6 GHz. As a result, the only overlapping link is 5 GHz, and this is a strong reason why you need to enable MLD association with only one link if client prefers to use MLD association for all AP MLDs all the time.We clarify the case of zero or more per-STA profiles, fix a bug, and clarify the corresponding 4-way handshake signaling. TGbe editor to make the changes shown in 11-21/599r6 under all headings that include CID 5303. |
| 8338 | Zhiqiang Han | 35.3.5.4 | 257.13 | There is a special case. non-AP STA wants to initiate a multi-link setup but the AP can only setup one link. In this case, AP will not include the Basic variant Multi-Link element. The spec shall cover this case. | 8338 | Revised – For the problem of MLD association with only one link, we note that it is possible that AP MLD only supports 2.4 GHz and 5 GHz, and non-AP MLD only supports 5 GHz and 6 GHz. As a result, the only overlapping link is 5 GHz, and this is a strong reason why you need to enable MLD association with only one link if client prefers to use MLD association for all AP MLDs all the time.We clarify the case of zero or more per-STA profiles, fix a bug, and clarify the corresponding 4-way handshake signaling. TGbe editor to make the changes shown in 11-21/599r6 under all headings that include CID 5303. |
| 6642 | Pooya Monajemi | 35.3.5.4 | 256.37 | AP MLD may only accept the link on which the request was sent. Text is not clear about how this case is handled. | 6642 | Revised – For the problem of MLD association with only one link, we note that it is possible that AP MLD only supports 2.4 GHz and 5 GHz, and non-AP MLD only supports 5 GHz and 6 GHz. As a result, the only overlapping link is 5 GHz, and this is a strong reason why you need to enable MLD association with only one link if client prefers to use MLD association for all AP MLDs all the time.We clarify the case of zero per-STA profiles and how AP MLD react to the status code.TGbe editor to make the changes shown in 11-21/599r6 under all headings that include CID 6642. |
| 6629 | Po-Kai Huang | 35.3.5.1 | 254.50 | Clarify that the setup is successful if any link is accepted and a failure if none of the links is accepted. | As in comment. | Revised –Agree in principle with the commenters. We add the sentence to say failure if none of the links are accepted and successful otherwise. TGbe editor to make the changes shown in 11-22/0599r2 under all headings that include CID 6629. |
| 4049 | Abhishek Patil | 35.3.5.1 | 255.10 | What is the reason to limit the links to nonoverlapping channels? A link is defined as a Tuple consisting of <Operating Class, Channel and BSSID>. Therefore, it is possible to have two different BSSIDs operating on the same channel. Also, if there is to be a limit then it should be only for baseline features i.e., tied to dot11EHTBaselineFeaturesImplementedOnly equal to true | As in comment | Rejected - A proposed resolution for this CID was discussed as part of the comment resolutions in 11-22/526r0, however the group could not reach consensus on a proposed change that would resolve the comment. |
| 6359 | Morteza Mehrnoush | 35.3.5.1 | 255.11 | Do we need to add "shall" as below?"An MLD that requests or accepts multi-link (re)setup for any two links shall ensure that each link is located on different nonoverlapping channels." | as in comment | Rejected - A proposed resolution for this CID was discussed as part of the comment resolutions in 11-22/526r0, however the group could not reach consensus on a proposed change that would resolve the comment. |
| 6182 | Michael Montemurro | 12.5.3.3.1 | 214.61 | Since the PTKSA is between the non-AP MLD and the AP MLD, unicast management frame exchanges will have to be encapsulated by the MLD entities. The link for the management frame can be identified by the BSSID of the affiliated AP by both the AP MLD and the non-AP MLD. A solution like this would allow a unicast management frame to be transmitted between the affilaited STA and the affiliated AP across any available link through the AP MLD and non-AP MLD. | Update clauses 12.5.3.3, 12.5.5.3, and the appropriate clauses in 35 to specify that unicast management frames use A3 set to the affiliated AP MAC to identify the link and are encapsulated by the MLD prior to transmission.The commenter is willing to create a contribution to update the draft with these changes. | Revised - Due to the reason that MLD MAC address maybe the same as the MAC address of an affiliated AP, and not all the management frame are intended for a specific link, A3 is not a proper choice for the signaling. We introduce the signaling in the framebody.TGbe editor to make the changes shown in 11-21/1877r12 under all headings that include CID 6244. |
| 5184 | Guogang Huang | 12.5.3.3.1 | 215.41 | Define how to construct AAD for individually addressed management frame | As in comment. | Rejected – It has been defined in clause 12 that only individual addressed data frame between AP MLD and non-AP MLD needs AAD swap. For other cases, baseline procedure is used. |
| 5356 | Jarkko Kneckt | 11.13 | 205.55 | The current channel validation information contains channel information and procedure only for a single link. This is not suitable setup for multi-link operation, where a non-AP MLD may have more than 1 link with the AP MLD. The operating channel validation should be done in association, fast transition, SA Query, AP channel Switch, ML Reconfiguration, | Please add channel validation information for more than 1 link and add the procedure how to validate more links. | Rejected –There is no consensus during offline discussion.One argument is that there is a way to validate channel information of other links using beacon protection since EHT has mandated beacon protection on EHT AP as shown below.An EHT AP shall have dot11BeaconProtectionEnabled set to 1.                Specifically, for AP MLD, all the operating channel information for each affiliated AP (operating class and primary channel) are already included in reduced neighbor report (see 35.3.4.1 AP behavior), and during channel switch, channel switch announcement or extended channel switch announcement, channel information are also included in all beacons of sent by APs affiliated with the AP MLD (see 35.3.11 Multi-link procedures for channel switching, extended channel switching, and channel quieting). For ML reconfiguration, we only have link deletion, which is also announced in all beacons and can be verified with BIP. For SA Query, the OCI element for the transmitting STA is included and can be verified.                 Another argument is that Beacon protection is still not enough, and we need more mechanism on top of that.                   |
| 7434 | Thomas Derham | 11.13 | 0.00 | The MLD engages in procedures such as SA Query that involve OCV, however it is not defined how operating channel(s) are validated when an MLD is using multiple links | Add support to OCI for multiple links, or define an alternative mechanism with equivalent security for MLDs | Rejected –There is no consensus during offline discussion.One argument is that there is a way to validate channel information of other links using beacon protection since EHT has mandated beacon protection on EHT AP as shown below.An EHT AP shall have dot11BeaconProtectionEnabled set to 1.                Specifically, for AP MLD, all the operating channel information for each affiliated AP (operating class and primary channel) are already included in reduced neighbor report (see 35.3.4.1 AP behavior), and during channel switch, channel switch announcement or extended channel switch announcement, channel information are also included in all beacons of sent by APs affiliated with the AP MLD (see 35.3.11 Multi-link procedures for channel switching, extended channel switching, and channel quieting). For ML reconfiguration, we only have link deletion, which is also announced in all beacons and can be verified with BIP. For SA Query, the OCI element for the transmitting STA is included and can be verified.                 Another argument is that Beacon protection is still not enough, and we need more mechanism on top of that.                   |

**Discussion:**

**Propose:**

**TGbe editor: Modify 35.3.5.4 Usage and rules of Basic Multi-Link element in the context of multi-link (re)setup as follows (track change on):**

(#6752)(#8234)(#6360)A non-AP MLD may initiate a multi-link setup with an AP MLD to (#2478)(re)set up one or more links with AP(s) affiliated with the AP MLD. When a non-AP MLD initiates a multi-link (re)setup with an AP MLD, a STA that is affiliated with the non-AP MLD shall transmit an (Re)Association Request frame on the link that it desires to use as part of the multi-link (re)setup(#3153). An AP that is affiliated with the AP MLD shall transmit an (Re)Association Response frame on the link on which it received the (Re)Association Request frame. (#5293)

……………(existing texts)………………………

The (#6700)Basic Multi-Link element carried in the (Re)Association Request frame shall include the Common Info field and may include the Link Info field.(#5293)

(#6624)NOTE 1—When a (Re)Association Request frame is sent from a non-AP EHT STA that does not support the
multi-link operation, the Basic Multi-Link element is not carried in the (Re)Association Request frame.

(#1747)(#1789)(#2348)The Common info field of the (#6700)Basic Multi-Link element carried in the
(Re)Association Request frame shall include the MLD MAC address, the MLD Capabilities, and the EML Capabilities subfields, and shall not include the Link ID Info, the BSS Parameters Change Count, and the
Medium Synchronization Delay Information subfields.

(#1747)(#1789)(#2348)NOTE—The presence of the subfields in the Common Info field is signaled via the Multi-Link
Control field of the (#6700)Basic Multi-Link element as defined in 9.4.2.312.2 (Basic Multi-Link element(#6700)).

(#2125)(#2479)For each requested link in addition to the link on which the (Re)Association Request frame
is transmitted, the Link Info field (#6729)of the Basic Multi-Link element carried in the (Re)Association
Request frame shall contain the corresponding Per-STA Profile subelement(s). If there is no other requested link in addition to the link on which the (Re)Association Request frame is transmitted, the Basic Multi-Link element carried in the (Re)Association Request frame shall not include the Link Info field.(#5303)

For each Per-STA Profile subelement included in the Link Info field, the Complete Profile subfield of the STA Control field shall be set to 1 (see 35.3.2.2 (Advertisement of complete or partial per-link information(#1859))).

……………(existing texts)………………………

The (#6700)Basic Multi-Link element carried in the (Re)Association Response frame shall include the Common Info field and may include the Link Info field. (#5293)

(#6624)NOTE 2—When a (Re)Association Response frame is sent to a non-AP EHT STA that does not support the
multi-link operation, the Basic Multi-Link element is not carried in the (Re)Association Response frame.

(#1747)(#1789)(#2348)The Common info field of the (#6700)Basic Multi-Link element carried in the
(Re)Association Response frame shall include the MLD MAC address, the MLD Capabilities, the EML
Capabilities, the Link ID Info, and the BSS Parameters Change Count subfields.

(#1747)(#1789)(#2348)NOTE 3—The presence of the subfields in the Common Info field is signaled via the Multi-Link
Control field of the (#6700)Basic Multi-Link element as defined in 9.4.2.312.2 (Basic Multi-Link element(#6700)).

(#2125)For each requested link in addition to the link on which the (Re)Association Response frame is
transmitted, the Link Info field (#6729)of the Basic Multi-Link element carried in the (Re)Association
Response(#5303) frame shall contain the corresponding Per-STA Profile subelement(s). If there is no other requested link in addition to the link on which the (Re)Association Response frame is transmitted, the Basic Multi-Link element carried in the (Re)Association Response frame shall not include the Link Info field.(#5303) For each Per-STA Profile subelement included in the Link Info field, the Complete Profile subfield of the STA Control field shall be set to 1 (see 35.3.2.2 (Advertisement of complete or partial per-link information(#1859))) and the Status Code field included in the STA Profile subfield of the Per-STA Profile subelement shall indicate SUCCESS if the link is accepted or the failure cause if the link is not accepted. (#6729)The Status Code field in the (Re)Association Response frame body shall indicate, as defined in 9.4.1.9 (Status Code field), whether the link on which the (Re)Association Request frame is received is accepted or not. The Status Code field included in the STA Profile subfield of the Per-STA Profile subelement shall indicate DENIED\_LINK\_ON\_WHICH\_THE\_(Re)ASSOCIATION\_FRAME\_IS\_TRANSMITTED\_NOT\_ACCEPTED if the Status Code is not set to REFUSED\_REASON\_UNSPECIFIED and the link corresponiding to the Per-STA Profile subelement is not accepted only because the link on which the (Re)Association Request frame is transmitted is not accepted. (#6642)

NOTE - DENIED\_LINK\_ON\_WHICH\_THE\_(Re)ASSOCIATION\_FRAME\_IS\_TRANSMITTED\_NOT\_ACCEPTED is not used in the Status Code field included in the (Re)Association Response frame body. (#5303)

……………(existing texts)………………………

***TGbe editor: Modify 9.4.1.9 Status Code field as follows: (track change on)***

**9.4.1.9 Status Code field**

***Insert the following news rows to*** [***Table 9-78 (Status codes)***](#bookmark70) ***while maintaining the numerical order and updating the reserved range:***

**Table 9-78—Status codes**

|  |  |  |
| --- | --- | --- |
| **Status code** | **Name** | **Meaning** |
| 130 | DENIED\_STA\_AFFILIAT- ED\_WITH\_MLD\_WITH\_EXIST- ING\_MLD\_ASSOCIATION | Association denied because the requesting STA is affili- ated with a non-AP MLD that is associated with the AP MLD. |
| 131 | NSEP\_DENIED\_UNAUTHORIZED | (#1008)NSEP priority access denied because the non-AP MLD or non-AP EHT STA is not authorized to use the service. |
| 132 | NSEP\_DENIED\_OTHER\_REASON | NSEP priority access denied due to reason outside the scope of this standard. |
| 133 | DENIED\_TID\_TO\_LINK\_MAPPING | Request denied because the requested TID-to-link map- ping is unacceptable. |
| 134 | PREFERRED\_TID\_TO\_LINK\_MAP- PING\_SUGGESTED | Preferred TID-to-link mapping suggested. |
| (#4006)135 | DENIED\_EHT\_NOT\_SUPPORTED | Association denied because the requesting STA does not support EHT features. |
| <ANA> | DENIED\_LINK\_ON\_WHICH\_THE\_(RE)ASSOCIATION\_FRAME\_IS\_TRANSMITTED\_NOT\_ACCEPTED |  Link not accepted because the link on which the (Re)Association Request frame is transmitted is not accepted.(#5303)  |

***TGbe editor: Modify 35.3.5.*1 *Multi-link (re)setup procedure as follows: (track change on)***

**35.3.5 Multi-link (re)setup**

 **35.3.5.1 Multi-link (re)setup procedure**

(…existing texts…)

(#1656)An MLD that requests or accepts multi-link (re)setup for any two links ensures that each link is located on different nonoverlapping channels.

(#3220)If the link on which the (Re)Association Request frame was received cannot be accepted by the AP
MLD, the AP MLD shall treat the multi-link (re)setup as a failure and shall not accept any requested links. Otherwise, the multi-link (re)setup is successful.(#6629)

(…existing texts…)

***TGbe editor: Modify 35.3.5.4 Usage and rules of Basic Multi-Link element in the context of multi-link (re)setup(#6700) as follows: (track change on)***

**35.3.5.4 Usage and rules of Basic Multi-Link element in the context of multi-link (re)setup(#6700)**

(…existing texts…)

(#5303)

(…existing texts…)

***TGbe editor: Modify 12.7.2 EAPOL-Key frames as follows: (track change on)***

**12.7.2 EAPOL-Key frames**

***Change item g) of the fifth paragraph as follows:***

g) **Key RSC**. This field (#4696)contains the current receive sequence counter (RSC) for the GTK being installed. It is used in message 3 of the 4-way handshake and message 1 of the group key handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. If the RSC is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the Key RSC field. The RSC for TKIP is the TKIP sequence number (TSC); for CCMP and GCMP it is the packet number (PN); see Table 12-8 (Key RSC field).

(#2290)For MLO, the Key RSC field is set to 0 in all messages.

***Change the fifth item of the 20th paragraph as follows (not all items are shown):***

The following EAPOL-Key frames are used to implement the three different exchanges:

— **…**

— **Group key handshake message 1** is an EAPOL-Key frame with the Key Type subfield equal to 0. (#1028)(#2505)(#2594)For non-MLO, the~~The~~ Key Data field shall contain a GTK KDE and shall be encrypted. For MLO, the Key Data field may include one MLO GTK KDE, one MLO IGTK KDE, and one MLO BIGTK KDE for each of the setup links and shall be encrypted.

***Insert the following news rows to*** [***Table 12-10 (KDE selectors)***](#bookmark15) ***while maintaining the numerical order and updating the reserved range:***

**Table 12-10—KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data type** | **Meaning** |
| 00-0F-AC | 16 | MLO GTK KDE |
| 00-0F-AC | 17 | MLO IGTK KDE |
| 00-0F-AC | 18 | MLO BIGTK KDE |
| 00-0F-AC | 19 | MLO Link KDE(#2290) |
| 00-0F-AC | ~~15~~20–255 | Reserved |

***Insert the following figure and paragraphs after the description on Figure 12-36 (GTK KDE format) in the fifth paragraph:***

The format of the MLO GTK KDE is shown in [Figure 12-36a (MLO GTK KDE format(#2290))](#bookmark16).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Key ID | Tx | Reserved | LinkID | PN | GTK |

Bits: 2 1 1 4 48 (Length – 11) **×** 8

**Figure 12-36a—MLO GTK KDE format(#2290)**

(#2290)The definitions of Key ID, Tx, and GTK fields are the same as in the GTK KDE described above. The LinkID field contains the link identifier that corresponds to the link this GTK applies.

(#2290)The PN field contains the packet number and is formatted as described in Table 12-8 (Key RSC field).

***Insert the following figure and paragraph after the description on Figure 12-42 (IGTK KDE format) in the sixth paragraph:***

The format of the MLO IGTK KDE is shown in [Figure 12-42a (MLO IGTK KDE format(#2290))](#bookmark17).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key ID | IPN | Reserved | LinkID | IGTK |

Bits: 16 48 4 4 (Length – 13) **×** 8

**Figure 12-42a—MLO IGTK KDE format(#2290)**

(#2290)The definitions of Key ID, IPN, and IGTK fields are the same as in the IGTK KDE described above. The LinkID field contains the link identifier that corresponds to the link this IGTK applies.

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

The following EAPOL-Key frames are used to implement the three different exchanges:

* **4-way handshake message 1** is an EAPOL-Key frame with the Key Type subfield equal to 1. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached

PMKSA is not being used, inclusion of the PMKID (if derived) is optional. (#2290)For MLO, the Key Data field shall include the MAC Address KDE set to the MLD MAC address of the Authenticator. The Key Data field need not be encrypted.

* **4-way handshake message 2** is an EAPOL-Key frame with the Key Type subfield equal to 1. The Key Data field shall contain an RSNE, may contain an RSNXE, and need not be encrypted. (#2290)For MLO, the Key Data field shall include the MAC Address KDE set to the MLD MAC address of the Supplicant.

An ESS Supplicant’s SME shall insert the RSNE it sent in its (Re)Association Request frame, and shall insert the RSNXE it sent in its (Re)Association Request frame if the RSNXE is present in the (Re)Association Request frame it sent. The RSNE and the RSNXE are included as transmitted in the Management frame. (#2290)For MLO, if the non-AP MLD includes requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame, the non-AP MLD shall include a MLO Link KDE containing the LinkID field and affiliated STA MAC address for each link included by the non-AP MLD in the Multi-Link element in the (Re)Association Request frame. (#5303) On receipt of message 2, the Authenticator’s SME shall validate the selected security config- uration against the RSNE received in the (Re)Association Request frame, and shall validate the RSNXE included in message 2 against the RSNXE received in the (Re)Association Request frame from the Supplicant(#6050).

An IBSS Supplicant’s SME shall insert an RSNE containing a selected pairwise cipher suite. The Authenticator’s SME shall validate that the pairwise cipher suite selected is one of its configured cipher suites and that the group cipher suite and AKM are consistent.

* **4-way handshake message 3** is an EAPOL-Key frame with the Key Type subfield equal to 1. The Key Data field shall contain one or two RSNEs, and may contain an RSNXE. If a group cipher has been negotiated, this field shall also include a GTK. This field shall be encrypted if a GTK is included. (#2290)For MLO, the Key Data field shall include the MAC Address KDE set to the MLD MAC address of the Authenticator. When the Authenticator is an AP MLD and the Supplicant is a non-AP MLD, this field shall include one MLO GTK for each setup link (see 35.3.5 (Multi-link (re)setup)).

An Authenticator’s SME shall insert the RSNE it sent in its Beacon or Probe Response frame, and shall insert the RSNXE it sent in its Beacon or Probe Response frame if the RSNXE is present in the Beacon or Probe Response frame it sent. When this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name is added in the PMKID List field of the RSNE. (#2290)For MLO, an Authenticator’s SME shall insert a MLO Link KDE that includes the LinkID field, affiliated AP MAC address, RSNE, and RSNXE, if it was present, for each affiliated AP link that was advertised in the Multi-Link element included in Beacons, Probe Response, and ML Probe Response frames. The Supplicant’s SME shall validate the selected security configuration against the RSNE received in message 3, and shall validate the RSNXE included in message 3 against the RSNXE received in the Beacon or Probe Response frame from the Authenticator. (#2290)For MLO, the Supplicant’s SME shall validate the security configu- ration for each LinkID field, affiliated AP MAC address, RSNE, and RSNXE for each affiliated AP link included in message 3 against the affiliated AP MAC address, RSNE, and RSNXE received (#6053)for each link in Beacon, Probe Response that is not an ML probe response, or Probe Response frame that is an ML probe response frame. (#6050)If the second optional RSNE is present, the STA shall either use that cipher suite with its pairwise key or deauthenticate. In any of these cases, if the values do not match, then the receiver shall consider the RSNE or the RSNXE modified and shall use the MLME-DEAUTHENTICATE.request primitive to break the association. A secu- rity error should be logged at this time.

It may happen, for example, that a Supplicant selects a pairwise cipher suite which is advertised by an AP, but which policy disallows for this particular STA. An Authenticator may, therefore, insert a second RSNE to overrule the STA’s selection. An Authenticator’s SME shall insert the second RSNE, after the first RSNE, only for this purpose. The pairwise cipher suite in the second RSNE included shall be one of the ciphers advertised by the Authenticator. All other fields in the second RSNE shall be identical to the first RSNE.

A GTK shall be included and the unencrypted length of the GTK is six less than the length of the GTK KDE in octets. The entire Key Data field shall be encrypted as specified by the Key Descriptor Version.

* **4-way handshake message 4** is an EAPOL-Key frame with the Key Type subfield equal to 1. The Key Data field can be empty. (#2290)For MLO, the Key Data field shall include the MAC Address KDE set to the MLD MAC address of the Supplicant.
* **Group key handshake message 1** is an EAPOL-Key frame with the Key Type subfield equal to 0.

The Key Data field shall contain a GTK KDE and shall be encrypted.

* **Group key handshake message 2** is an EAPOL-Key frame with the Key Type subfield equal to 0.

The Key Data field can be empty.

***Insert the following figure and paragraphs at the end of the subclause:***

The format of the MLO BIGTK KDE is shown in [Figure 12-48a (MLO BIGTK KDE(#2290))](#bookmark18).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key ID | BIPN | Reserved | LinkID | BIGTK |

Bits: 16 48 4 4 (Length – 13) **×** 8

**Figure 12-48a—MLO BIGTK KDE(#2290)**

(#2290)The BIPN corresponds to the BIPN value that was carried in the MME of the last protected Beacon frame corresponding to the LinkID field and it is used by the receiver as the initial value for the BIP replay counter for the BIGTK.

The LinkID field contains the link identifier that corresponds to the link this BIGTK applies. The format of the MLO Link KDE is shown in [Figure 12-48b (MLO Link KDE(#2290))](#bookmark19).

|  |  |  |  |
| --- | --- | --- | --- |
| Link Information | MAC Address | RSNE | RSNXE |

Octets: 1 6 variable variable

**Figure 12-48b—MLO Link KDE(#2290)**

The Link Information field, which contains information identifying the presence of fields in the MLO Link KDE, is shown in [Figure 12-48c (Link Information field(#2290)(#6594))](#bookmark20).

|  |  |  |  |
| --- | --- | --- | --- |
| LinkID | RSNEInfo | RSNXEInfo | Reserved |

Bits 4 1 1 2

**Figure 12-48c—Link Information field(#2290)(#6594)**

The LinkID field contains the link identifier for the affiliated STA link.

(#6594)The RSNEInfo field indicates that the RSNE is present in the MLO Link KDE when its value is equal to 1, otherwise the RSNE is not present.

The RSNXEInfo field indicates that the RSNXE is present in the MLO Link KDE when its value is set to 1.

The MAC Address field contains the MAC address of the affiliated STA for the link specified in the Link Information field.

The RSNE field contains the RSNE of the affiliated STA for the link specified in the Link Information field. The RSNE is described in 9.4.2.24 (RSNE).

The RSNXE field contains the RSNE of the affiliated STA for the link specified in the Link Information field. The RSNXE is described in 9.4.2.241 (RSNXE).

***TGbe editor: Modify 12.7.6 4-way handshake as follows: (track change on)***

**12.7.6 4-way handshake**

**12.7.6.1 General**

***Change the first paragraph as follows:***

RSNA defines a protocol using EAPOL-Key frames called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID} or

{MAC Address}(#2290))

Message 2: Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or

{RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE} or {RSNE,

MAC Address} or {RSNE, RSNXE, MAC Address}or

{RSNE, OCI KDE, RSNXE, MAC Address}(#5303) or {RSNE,

MAC Address, MLO Linkn} or {RSNE, RSNXE, MAC Address, MLO Linkn}or

{RSNE, OCI KDE, RSNXE, MAC Address (#5303), MLO Linkn}(#2290))

Message 3: AuthenticatorSupplicant: EAPOL-

Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or {RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or {RSNE, GTK[N], OCI KDE, RSNXE} or

{MAC Address, MLO Linkn, MLO GTKn, MLO IGTKn, MLO BIGTKn} or {OCI KDE, MAC Address, MLO Linkn, MLO GTKn, MLO IGTKn, MLO BIGTKn}(#2290))

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{} or {MAC Address}(#2290)).

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

The following apply:

* EAPOL-Key() denotes an EAPOL-Key frame conveying the specified argument list, using the notation introduced in [12.7.4 (EAPOL-Key frame notation)](#bookmark18).
* ANonce is a nonce that the Authenticator contributes for PTK generation. ANonce has the same value in message 1 and message 3.
* SNonce is a nonce from the Supplicant for PTK generation.
* P means the pairwise bit is set.
* The MIC is computed over the body of the EAPOL-Key frame (with the Key MIC field first zeroed before the computation) using the KCK defined in [12.7.1.3 (Pairwise key hierarchy)](#bookmark11) for PTK generation.
* RSNE represents the appropriate RSNEs. (#2290)For MLO, the RSNE is present in the MLO Link KDE.
* GTK[N] represents the GTK with its key identifier.
* OCI KDE contains the current operating channel information for the operating channel in which the EAPOL-Key frame is sent. OCI KDE is present when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant in Message 2 and Authenticator in Message 3. Otherwise it is absent.
* RSNXE, when included in message 2, contains the RSNXE that the Supplicant sent in its (Re)Association Request frame, and when included in message 3, contains the RSNXE that the Authenticator sent in its Beacon or Probe Response frame. RSNXE is present in message 2 if this element is present in the (Re)Association Request frame that the Supplicant sent, and is present in message 3 if this element is present in the Beacon or Probe Response frame that the Authenticator sent. (#2290)For MLO, the RSNXE is present in the MLO Link KDE.
* (#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.
* For MLO, an MLO Link KDE is included for an affiliated STA link of an MLD as follows. When more than one link is requested and(#5303) 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 on the same link used by the latest exchange of successful (Re)Association Request/Response
frame.

**12.7.6.2 4-way handshake message 1**

***Change the first paragraph as follows:***

Message 1 uses the following values for each of the EAPOL-Key frame fields: Descriptor Type **=** N – see [12.7.2 (EAPOL-Key frames)](#bookmark12)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0

Key Type = 1 (Pairwise) Reserved = 0

Install = 0 Key Ack = 1 Key MIC = 0

Secure = 0

Error = 0

Request = 0

Encrypted Key Data = 0

Reserved = 0 – unused by this protocol version

Key Length = Cipher-suite dependent; see Table 12-7 (Cipher suite key lengths)

Key Replay Counter = *n* – to allow Authenticator or initiator STA to match the right message 2 from Supplicant or peer STA

Key Nonce = ANonce EAPOL-Key IV = 0 Key RSC = 0

Key MIC = 0

Key Data Length = length of Key Data field in octets (#2290)Key Data =

* PMKID for the PMK being used during PTK generation
* For MLO, a MAC Address KDE containing the MLD MAC address of the Authenticator.

**12.7.6.3 4-way handshake message 2**

***Change the first paragraph as follows:***

Message 2 uses the following values for each of the EAPOL-Key frame fields: Descriptor Type **=** N – see [12.7.2 (EAPOL-Key frames)](#bookmark12)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1 Reserved = 0

Install = 0 Key Ack = 0

Key MIC = 0 when using an AEAD cipher or 1 otherwise Secure = 0 – same as message 1

Error = 0 – same as message 1 Request = 0 – same as message 1

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n* – to let the Authenticator or initiator STA know to which message 1 this corresponds

Key Nonce = SNonce EAPOL-Key IV = 0

Key RSC = 0

Key MIC = Not present when using an AEAD cipher; otherwise, MIC(KCK, EAPOL) – MIC com- puted over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets Key Data =

* included RSNE – the sending STA’s RSNE for PTK generation or peer RSNE for the current operating band, and when this message 2 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK- R1) is included in the PMKID List field of the RSNE and the FTE and MDE are also included, or;
* The sending STA’s Multi-band element for PTK generation for a supported band other than the current operating band if dot11MultibandImplemented is true, or;
* The sending STA’s RSNE and Multi-band element(s) for generating a single PTK for all involved bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s); or;
* The sending STA’s RSNE and Multi-band element(s) for generating a different PTK for each involved band, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield of the RSN capabilities field is 1 for both the Authenticator and the Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.
* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant.
* The RSNXE that the Supplicant sent in its (Re)Association Request frame, if this element is present in the (Re)Association Request frame that the Supplicant sent.
* (#2290)For MLO, a MAC Address KDE containing the MLD MAC address of the Supplicant.
* (#2290)For MLO, when more than one link is requested, an MLO Link KDE for each affiliated STA link containing the affiliated STA MAC address included by the non-AP MLD in the Multi-Link element in (Re)Association Request frame. (#5303)

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

Otherwise, the Authenticator:

* + - * 1. Derives PTK.
				2. Verifies the message 2 MIC or AEAD decryption operation result.

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.

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,

if the non-AP MLD includes requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame, validates that the affiliated STA MAC addresses are the same for each link (#5303) included in the Multi-Link element in the (Re)Association Request frame.

If these are not exactly the same, the Authenticator uses MLME-DEAUTHENTI- CATE.request primitive to terminate the association.

If they do match bitwise, the Authenticator constructs message 3.

* + - * 1. If management frame protection is being negotiated, the AP initializes the SA Query Transaction Identifier to an implementation-specific non-negative integer value, valid for the current pairwise security association.

**12.7.6.4 4-way handshake message 3**

***Change the first paragraph as follows:***

Message 3 uses the following values for each of the EAPOL-Key frame fields: Descriptor Type **=** N – see [12.7.2 (EAPOL-Key frames)](#bookmark12)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1 Reserved = 0

Install = 0/1 – For PTK generation, 0 only if the AP does not support key mapping keys, or if the STA has the No Pairwise bit (in the RSN Capabilities field) equal to 1and only the group key is used.

Key Ack = 1

Key MIC = 0 when using an AEAD cipher or 1 otherwise Secure = 1 (keys installed)

Error = 0 – same as message 1 Request = 0 – same as message 1 Encrypted Key Data = 1

Reserved = 0 – unused by this protocol version

Key Length = Cipher-suite dependent; see Table 12-7 (Cipher suite key lengths) Key Replay Counter = *n+1*

Key Nonce = ANonce – same as message 1

EAPOL-Key IV = 0 (Version 2) or random (Version 1)

Key RSC = (#1028)(#2505)(#2594)For PTK generation for non-MLO, starting TSC or PN that the Authenticator’s STA uses in MPDUs protected by GTK. 0 for MLO.

Key MIC = Not present when using an AEAD cipher; or otherwise, MIC(KCK, EAPOL) or MIC(SKCK, EAPOL) – MIC computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets Key Data =

* For PTK generation for the current operating band, the AP’s Beacon/Probe Response frame’s RSNE for the current operating band, and, optionally, a second RSNE that is the Authenticator’s pairwise cipher suite assignment for the current operating band, and, if a group cipher has been negotiated, the GTK and the GTK’s key identifier (see [12.7.2](#bookmark12) [(EAPOL-Key frames)](#bookmark12)) for the current operating band, and if management frame

protection is negotiated, the IGTK KDE, and if beacon protection is enabled, the BIGTK KDE, and when this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.6.4 (PMK-R1) in the PMKID List field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime]; or

* (#2290)For MLO, the MLO GTK KDE for each setup link (see 35.3.5.1 (Multi-link (re)setup procedure)). If management frame protection is negotiated, the MLO IGTK KDE for each setup link. If beacon protection is enabled, the MLO BIGTK KDE for each setup link. When this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.6.4 (PMK-R1) in the PMKID List field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime]; or
* For PTK generation for a supported band other than the current operating band, the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s Multi-band element associated with the supported band, and optionally a second Multi-band element that indicates the Authenticator’s pairwise cipher suite assignment for the supported band, and, if group cipher for the supported band is negotiated, the Multi- band GTK KDE for the supported band if dot11MultibandImplemented is true, or;
* For generating a single PTK for all involved bands, the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band element(s) that indicate the Authenticator’s assignment of one pairwise cipher suite for all involved bands; if a group cipher for all involved bands is negotiated, the GTK and the GTK’s key identifier for all involved bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s), or;
* For generating different PTKs for the current operating band and other supported band(s), the Authenticator’s Beacon/DMG Beacon/Announce/Probe Response/Information Response frame’s RSNE and Multi-band element(s), and optionally, additional RSNE and Multi-band elements that are the Authenticator’s pairwise cipher suite assignments for one or more involved bands; if group ciphers for the involved bands are negotiated, the Multi- band GTK KDEs for the involved bands, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield is 1 for both the Authenticator and Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.
* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
* The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.
* (#2290)For MLO, a MAC Address KDE containing the MLD MAC address of the Authenticator.
* (#2290)For MLO, a MLO Link KDE containing the LinkID field, the 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.

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

The Supplicant also:

* + - * 1. Verifies the RSNE and, if present, the RSNXE. If this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Supplicant verifies that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and verifies that all other fields of the RSNE are identical to the fields in the RSNE present in the Beacon or Probe Response frames and verifies that the FTE and MDE are the same as in the (Re)Association Response frame. Otherwise, the Supplicant verifies that the RSNE is identical to that the STA received in the Beacon or Probe Response frame. If the RSNXE is present, the Supplicant verifies that the RSNXE is identical to that the STA received in the Beacon or Probe Response frame. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant uses the pairwise cipher suite specified in the second RSNE or deauthenticates.
				2. (#2290)For MLO, verifies that the affiliated AP MAC address, the RSNE, and the RSNXE, if present, are the same as advertised by the affiliated APs of the AP MLD in Beacon, Probe Response, and ML Probe Response frames.
				3. Verifies the message 3 MIC or AEAD decryption operation result. If the calculated MIC does not match the MIC that the Authenticator included in the EAPOL-Key frame or AEAD decryption operation returns failure, the Supplicant silently discards message 3.
				4. Updates the last-seen value of the Key Replay Counter field.
				5. If the Extended Key ID for Individually Addressed Frames subfield of the RSN Capabilities field is 1 for both the Authenticator and Supplicant: Uses the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to receive individually addressed MPDUs protected by the PTK with the assigned Key ID.
				6. Constructs message 4.
				7. Sends message 4 to the Authenticator.
				8. Uses the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to send and, if the receive key has not yet been installed, to receive individually addressed MPDUs protected by the PTK. The GTK is also configured by MLME-SETKEYS primitive.

**12.7.6.5 4-way handshake message 4**

***Change the first paragraph as follows:***

Message 4 uses the following values for each of the EAPOL-Key frame fields: Descriptor Type **=** N – see [12.7.2 (EAPOL-Key frames)](#bookmark12)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1 Reserved = 0

Install = 0

Key Ack = 0 – this is the last message

Key MIC = 0 when using an AEAD cipher or 1 otherwise Secure = 1

Error = 0

Request = 0

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n+1*

Key Nonce = 0 EAPOL-Key IV = 0 Key RSC = 0

Key MIC = Not present when using an AEAD cipher; or otherwise, MIC(KCK, EAPOL) – MIC computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets

Key Data = (#2290)~~none required~~For MLO, a MAC Address KDE containing the MLD MAC address of the Supplicant, otherwise there is no Key Data.