### IEEE P802.11Wireless LANs

|  |
| --- |
| 11be D0.3 CR for 11.3.4 |
| Date: 2021-03-10 |
| 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:

1165, 1664, 1666, 2082, 2083, 2084, 2279, 2280, 2825, 2881, 2882, 2883, 3364

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 D0.3 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D0.3 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** | **P.L** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 1165 | Arik Klein | 92.01 | 11.3.4.3 | Define MLD Authenticate frame, in a similar way that is defined for the MLD Probe Request (section 35.3.4.2).This way the terminlogy will be much easier to distinct between Authenticate frame which does not include the MLE (and/or any other TBD elements, if needed in future) and the Authenticate frame which shall include the MLE (and/or any other TBD elements, if needed in future) | 1. Add section with the definition for MLD authenticate frame, as proposed.2. Change the "Authenticate frame" throughout this section to "MLD Authenticate frame" accordingly, as well as in the following setions: 12.3.3.2, 12.4.1, 12.4.8.3.1, 35.3.2.1Still, the frame that will be used will be the Authentication frame, but in case of Multi-link (re)setup it shall include the MLE (and/or any other TBD elements, if needed in future). | Rejected – The frame itself is Authentication frame, and we are not changing the format, so we do not need a different name, which implies that we are creating a new frame. The text in 9.3.3.11 Authentication frame format is also clear that between two MLD, the authentication frame will always include multi-link element. *The Basic variant Multi-Link element is optionally present if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. Otherwise it is not present.*The text in 35.3.5.4 (Usage and rules of Basic variant Multi-link element in the context of multi-linksetup) further clarifies that the multi-link is basic variant and MLD MAC address is present. *An STA affiliated with an MLD shall include a Basic variant Multi-Link element containing the MLD MACaddress of the MLD with which the STA is affiliated in the Authentication frame that it transmits.*  |
| 1664 | GEORGE CHERIAN | 90.51 | 11.3.4 | If authentication/de-auth frames are allowed to be sent on more than one link, it can lead to race-conditions. So, specfy that the authentication/deauth signaling for a particular sessions is conducted on one link, which can be any link that the MLD chooses. | As in the comment | Revised – It is certainly clear that the authentication frame exchange should be in one link to finish the authentication procedure, but it is not clear that disauthentication needs to be in the same link. If the authentication sequence is not finished, then the disauthentication frame from the peer technically does not have any impact. If the authentication procedure is done, since each MLD will only send one management frame at a time. As a result, the MLD that will send response to an authentication frame will send disauthentcaiton after the response to an authentication frame is sent.We only add sentence to mandate that authentication frame exchange needs to be in the same link. TGbe editor to make the changes shown in 11-21/0434r0 under all headings that include CID 1664. |
| 1666 | GEORGE CHERIAN | 91.58 | 11.3.4.3 | Add a text to clarify that a common PTK is generated for the MLD, where as separate GTKs are assigned for each link (35.3.5.2 talks defines it -pp132/LL1) | As in the comment | Rejected – One PTK is already covered by the description of one PTKSA per MLD setup. *12.6.1.1.6 PTKSA**there shall be only one PTKSA per band (see 12.6.19 (Protection of robust Managementframes))* ***or per MLD setup (****see 35.3.5 (Multi-link (re)setup)) with the same Supplicant and AuthenticatorMAC addresses.*Separate GTKs is there for GTKSA. |
| 2082 | Joseph Levy | 91.02 | 11.3.4.1 | What is a peer MLD. This legacy text was written so that all types of STA to STA authentications are supported. Will MLO allow for all types of MLD to MLD authentication? I thought MLO was being considered for infrastructure configuration only. Why use this legacy style if only infrastructure association and authentications are allowed. | Clearly state when MLD reauthentication is allowed or define what a peer MLD is. | Rejected – Authentication is between two entities. When the authentication is between two STAs, the peer STA is just another STA. When the authenticaton is between two MLDs, the peer MLD is just another MLD. Note that the baseline does not define peer STA, and there is no need to define peer MLD. It is true that currently, we only enable MLD for infrastructure case, and that is already clear in 35.3.1 General.  |
| 2083 | Joseph Levy | 91.08 | 11.3.4.1 | Authentication is not between two STAs or an AP MLD and a non-AP MLD it is a between a STA and the BSS, ESS, or optionally the IBSS. The statement that authentication is required between an AP MLD and a non-AP MLD makes not sense. | please clarify what is meant by authentication between MLDs or remove the concept. | Rejected – Authentication is between two entities. In the baseline, the two entities are two STAs, and in 11be the concept has been extended to be between two MLDs. We note that authenticaton is not between a STA and the entire BSS based on the baseline. |
| 2084 | Joseph Levy | 91.38 | 11.3.4.2 | What is meant by SAE authentication between and AP MLD and a non-AP MLD. This concept does not make sense to me and does not seem to be defined anywhere in the current .11 spec. Authentication is a concept suitable for a BSS, ESS, IBSS, or MBSS - how does it make sense to discuss authentication on a peer to peer link? | please clarify what is meant by authentication between MLDs or remove the concept. | Rejected – Authentication is between two entities. In the baseline, the two entities are two STAs, and in 11be the concept has been extended to be between two MLDs. It is not correct to state that authentication is for the entire BSS or ESS.  |
| 2279 | Michael Montemurro | 91.91 | 11.3.4.1 | Why is this statement even required? Up until this point, it looks as though state between an AP MLD and non-AP MLD operate in a BSS. That better be the case. | Delete "Between an AP MLD and a non-AP MLD, authentication is required." | Rejected – The definition of BSS is a set of STAs that have synchronized with each other. For AP MLD, different APs may have different TSFs, and it is not correct to call the whole AP MLD one BSS. As a result, the statement is required. *basic service set (BSS): A set of stations (STAs) that have successfully synchronized using the JOINservice primitives19 and one STA that has used the START primitive.* |
| 2280 | Michael Montemurro | 92.15 | 11.3.4.3 | Why is this statement even required? Up until this point, it looks as though state between an AP MLD and non-AP MLD operate in a BSS. That better be the case. | Delete "between an AP MLD and a non-AP MLD or" | Rejected – The definition of BSS is a set of STAs that have synchronized with each other. For AP MLD, different APs may have different TSFs, and it is not correct to call the whole AP MLD one BSS. As a result, the statement is required. *basic service set (BSS): A set of stations (STAs) that have successfully synchronized using the JOINservice primitives19 and one STA that has used the START primitive.* |
| 2825 | Srinivas Kandala | 93.25 | 11.3.4.4 | The abbreviation "MLDME" is not defined anywhere. Presumably it is meant to be "MLD MAC sublayer management entity". | Define MLDME and update the management model in subclause 6.1 and figure 6-1 (and possibly elsewhere as well) | Revised – Agree that we already have the following statement in the spec, so we simpley change MLDME to SME.*In 11.3 (STA/MLD authentication and association), when referring to MLD authentication, MLDdeauthentication, MLD (re)association, MLD disassociation, or MLD 4-way handshake, the reference of“SME” means the entity that manages the MLD*TGbe editor to make the changes shown in 11-21/0434r0 under all headings that include CID 2825. |
| 3364 | Zhiqiang Han | 93.25 | 11.3.4.4 | MLDME is multi-link device management entity, but what is the relationship between MLDME and MLME? and the architecute don't have this entity. Please clarify it. | It's better to define the MLD architecure in 4.9 Reference model and clarify the relationship between MLDME and SME and other entity. | Revised – Since we already have the following statement in the spec, we do not need MLDME anymore and we simpley change MLDME to SME.*In 11.3 (STA/MLD authentication and association), when referring to MLD authentication, MLDdeauthentication, MLD (re)association, MLD disassociation, or MLD 4-way handshake, the reference of“SME” means the entity that manages the MLD*TGbe editor to make the changes shown in 11-21/0434r0 under all headings that include CID 2825. |
| 2881 | Stephen McCann | 91.37 | 11.3.4.2 | In the cited sentence authentication between a non-AP MLD and an AP MLD is the same as authentication within an infrastructure BSS, IBSS, or MBSS. Therefore the extra terms are not required. | Remove the changes to bullet item 3), as they are not required. | Rejected –We note that authentication is between two entities. In the baseline, the two entities are two STAs, and in 11be the concept has been extended to be between two MLDs. As a result, the description is still required here.  |
| 2882 | Stephen McCann | 92.45 | 11.3.4.3 | What is an "originating MLD"? | The term "originating MLD" needs ot be defined. | Rejected – We note that in the baseline, there is no definition of originaiting STA, and it simply means the STA that initiates the auhtenticaiotn. Originating MLD means the MLD that initiates the authentication.  |
| 2883 | Stephen McCann | 93.61 | 11.3.4.5 | In the cited sentence, there is no "indicated non-AP MLD". | Change the sentence to "If the MLD is an AP MLD, release the AID assigned for the indicated MLD." | Revised – Agree in principle that in the baseline, the sentence also just says the “indicated STA”. Ok to revise with similar description. Note that the indication is in MLME-DEAUTHENTICATE.indication primitive.TGbe editor to make the changes shown in 11-21/0434r0 under all headings that include CID 2883. |

**Discussion:** *None.*

**Propose:**

*TGbe editor: Change 11.3.4* *as follows (track change on):*

* Authentication and deauthentication
* General

***Change the second and third paragraphs as follows:***

Successful authentication sets the state for a STA or an MLD to State 2, if it was in State 1. Unsuccessful authentication leaves the state for the STA or the MLD unchanged.

Deauthentication notification sets the state for a STA or an MLD to State 1. Deauthentication notification when in State 3 or 4 implies disassociation as well. A STA or an MLD may deauthenticate a peer STA or a peer MLD, respectively, at any time, for any reason.

***Change the fifth paragraph as follows:***

Authentication is optional in an IBSS. Between an AP MLD and a non-AP MLD, authentication is required. In a non-DMG infrastructure BSS, authentication is required. In a DMG infrastructure BSS and PBSS, the Open System authentication algorithm is not used (see 12.3.3.1 (Overview)). APs, AP MLDs, and PCPs do not initiate authentication.

***Change the title of the subclause 11.3.4.2 as follows:***

* Authentication—originating STA or MLD

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

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA or MLD shall authenticate with the indicated STA or MLD, respectively, using the following procedure:

* If the STA is in an IBSS, the SME shall delete any PTKSA, GTKSA, IGTKSA and temporal keys held for communication with the indicated STA by using the MLME-DELETEKEYS.request primitive (see 12.6.18 (RSNA security association termination)).
* The STA or the MLD shall execute one of the following:
* For the Open System or Shared Key authentication algorithm, the authentication mechanism described in 12.3.3.2 (Open System authentication) or 12.3.3.3 (Shared Key authentication), respectively.
* For the fast BSS/ML transition (FT) authentication algorithm in an ESS, the authentication mechanism described in 13.5 (FT protocol), or, if resource requests are included, 13.6 (FT resource request protocol).
* For SAE authentication between an AP MLD and a non-AP MLD or in an infrastructure BSS, IBSS, or MBSS, the authentication mechanism described in 12.4 (Authentication using a password).
* For FILS authentication, the authentication mechanism described in 12.11 (Authentication for FILS). An AP or PCP may provide estimated association response latency to a non-AP and non-PCP STA using the Association Delay Info field in the Association Delay Info element (9.4.2.174 (Future Channel Guidance element)). The value of the Association Delay Info field shall be larger than dot11HLPWaitTime.
* If the authentication was successful within the AuthenticateFailureTimeout, the state for the indicated STA or MLD shall be set to State 2 if it was State 1; the state shall remain unchanged if it was other than State 1.
* The MLME shall issue an MLME-AUTHENTICATE.confirm primitive to inform the SME of the result of the authentication.

***Change the title of the subclause 11.3.4.3 as follows:***

* Authentication—destination STA or MLD

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

Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA or MLD shall authenticate with the originating STA or MLD, respectively, using the following procedure:

* If Open System or Shared Key authentication algorithm is being used, the STA or the MLD shall execute the procedure described in 12.3.3.2 (Open System authentication) or 12.3.3.3 (Shared Key authentication) respectively. These result in the generation of an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request.
* If FT authentication is being used, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, including the FT Authentication Elements, and the SME shall execute the procedure as described in 13.5 (FT protocol) or 13.6 (FT resource request protocol).
* If SAE authentication is being used between an AP MLD and a non-AP MLD or in an infrastructure BSS, IBSS, or MBSS, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, including the SAE authentication elements, and the SME shall execute the procedure as described in 12.4 (Authentication using a password).
* If FILS authentication is being used, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, and the SME shall execute the procedure described in 12.11 (Authentication for FILS).
* If the STA is in an IBSS and management frame protection was not negotiated when the PTKSA(s) were created, the SME shall delete any PTKSA, GTKSA, IGTKSA and temporal keys held for communication with the originating STA by using the MLME-DELETEKEYS.request primitive (see 12.6.18 (RSNA security association termination)).
* Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is not SUCCESS, the MLME shall transmit an Authentication frame with the corresponding status code, as defined in 9.4.1.9 (Status Code field), and the state for the originating STA or MLD shall be left unchanged. The Authentication frame is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5 (FT protocol) or 13.6 (FT resource request protocol).
* Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is SUCCESS, the MLME shall transmit an Authentication frame that is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5 (FT protocol) or 13.6 (FT resource request protocol), with a status code of SUCCESS, and the state for the originating STA or MLD shall be set to State 2 if it was in State 1; the state shall remain unchanged if it was other than State 1.

NOTE—If management frame protection was negotiated, the SME does not change the state for the originating STA or originating MLD and does not delete any of the previously created SAs or temporal keys as a part of this authentication procedure.

***Add the following paragraph to the end of 11.3.4.3:***

For a destination MLD, an Authentication frame that is constructed using the appropriate procedure to complete the authentication procedure shall be sent to the STA affiliated with the originating MLD that sends the Authentication frame with authentication transaction sequence number equal to 1.(#1664)

***Change the title of the subclause 11.3.4.4 as follows:***

* Deauthentication—originating STA or MLD

***Change as follows:***

The originating STA or MLD shall deauthenticate with the indicated STA or MLD, respectively, using the following procedure:

* The SME shall generate an MLME-DEAUTHENTICATE.request primitive containing the appropriate reason code for the STA or MLD deauthentication, as defined in Table 9-49 (Reason codes) of 9.4.1.7 (Reason Code field).
* On receipt of the MLME-DEAUTHENTICATE.request primitive, if the state for the indicated STA or MLD is State 2, State 3, or State 4, the MLME shall generate a Deauthentication frame to be transmitted to the indicated STA or MLD, respectively.

NOTE—As the Deauthentication frame is a bufferable MMPDU, the transmission of this frame might be delayed by the operation of a power saving protocol. The AID and the PTKSA are maintained (when applicable) until the frame is acknowledged or attempts to transmit the frame are abandoned.

* The state for the indicated STA or MLD shall be set to State 1.
* Once the Deauthentication frame is acknowledged or attempts to transmit the frame are abandoned, the MLME shall issue an MLME-DEAUTHENTICATE.confirm primitive to inform the SME of the deauthentication.
* The SME, upon receipt of an MLME-DEAUTHENTICATE.confirm primitive, shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA and temporal keys held for communication with the indicated STA or MLD by using the MLME-DELETEKEYS.request primitive (see 12.6.18 (RSNA security association termination)) and by generating an MLME-SETPROTECTION.request(None) primitive.
* If the STA is contained within an AP or PCP, its SME, upon receipt of an MLME-DEAUTHENTICATE.confirm primitive, shall release the AID assigned for the indicated STA, if the state for the indicated STA was State 3 or State 4.
* If the MLD is an AP MLD, its SME(#2825), upon receipt of an MLME-DEAUTHENTICATE.confirm primitive, shall release the AID assigned for the indicated non-AP MLD, if the state for the indicated MLD was State 3 or State 4.
* If the STA is contained within an AP, its SME shall inform the DS of the disassociation, if the state for the indicated STA was State 3 or State 4.
* If the MLD is an AP MLD, its SME(#2825) shall inform the DS of the disassociation, if the state for the indicated non-AP MLD was State3 or State4.
* If the STA is a mesh STA, its SME shall inform the mesh peering instance controller (see 14.3.4 (Mesh peering instance controller)) of the deauthentication.
* Deauthentication—destination STA or MLD

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

Otherwise, upon receipt of a Deauthentication frame from a STA or an MLD for which the state is State 2, State 3, or State 4, the destination STA or MLD, respectively, shall deauthenticate with the originating STA or MLD, respectively, using the following procedure:

* If management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection is in use and the frame is not discarded per management frame protection processing, the MLME shall issue an MLME‑DEAUTHENTICATE.indication primitive to inform the SME of the deauthentication, and set the state for the originating STA or the originating MLD to State 1.
* Upon receiving an MLME-DEAUTHENTICATE.indication primitive, the SME shall
* Delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA and temporal keys held for communication with the originating STA or the originating MLD by using the MLME-DELETEKEYS.request primitive (see 12.6.18 (RSNA security association termination)) and by generating an MLME-SETPROTECTION.request(None) primitive.
* If the STA is contained within an AP or PCP, release the AID assigned for the indicated STA.
* If the MLD is an AP MLD, release the AID assigned for the indicated MLD(#2883).
* If the STA is contained within an AP, inform the DS of the disassociation, if the state for the originating STA was State 3 or State 4.
* If the MLD is an AP MLD, inform the DS of the disassociation, if the state for the originating non-AP MLD was State 3 or State 4.
* If the STA is a mesh STA, inform the mesh peering instance controller (see 14.3.4 (Mesh peering instance controller)) of the deauthentication.