IEEE P802.11
Wireless LANs

|  |
| --- |
| 11be D4.0 CR for CID 19004 and 19169 |
| Date: 2023-09-23 |
| 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:

19004, 19169

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Editorial revision based on the comment from Gaurav.
* Rev 2: Revision based on the comments during teleconference call to add texts related to add links in reconfiguration. Revise texts to avoid the case that SA Query has been done. Add status code as suggested by Yongho. Changes are marked green.
* Rev 3: Remove the texts related to SA Query in reconfiguration. Reconfiguration frame will be protected, and there is no SA Query in reconfiguration.
* Rev 4: Editorial change based on the request from Binita to remove the duplicate if description

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** |
| 19169 | Po-Kai Huang | 35.3.5.1 | 507.13 | AP MLD also needs check the MAC address of the associated non-AP MLD to see if the MAC address conflicts with existing one. Without further check, attacker can easily have another setup with conflict affiliated STA MAC address in a link to bring down the link of previous associated non-AP MLD. | Proposed texts in 11-23-1056 is a good candidate to resolve the issues. | Revised – Agree in principle with the commenter. There are 3 cases for checking the affiliated non-AP STA MAC address. We provide corresponding texts to address the 3 cases.*Case 1 (MLD-MLD non-AP STA address conflict): As raised by commenter, a non-AP MLD sending (re)association request has address of an affiliated non-AP STA conflict with the MAC address of a non-AP STA affiliated with an existing association non-AP MLD**Case 2 (MLD-non-MLD non-AP STA address conflict): a non-AP MLD sending (re)association request has MAC address of an affiliated non-AP STA conflict with the MAC address of an associated non-AP STA not affiliated with a non-AP MLD.* *Case 3 (non-MLD- MLD non-AP STA address conflict): a non-AP STA not affiliated with a non-AP MLD sending (re)association request has the same MAC address as a non-AP STA affiliated with an existing association non-AP MLD.* TGbe editor to make the changes shown in 11-23/1655r3 under all headings that include CID 19169 |
| 19004 | Chaoming Luo | 11.3.6.3 | 381.45 | There may be an attacker non-AP MLD has affiliated non-AP STAs whose MAC address(es) confilict with MAC address(es) of existing associated legacy non-AP STAs. If the AP MLD does not check with those STAs, the attacker non-AP MLD will be successfully associated and the affiliated AP will be associated with two non-AP STAs (one legacy STA and one affiliated STA) which have the same MAC address.Same issue lies in P387L12. | Change item e) as follows:e)Otherwise, if the state for the STA that has any of the MAC addresses of the affiliated STAs of the non-AP MLD or the STA that has the MLD MAC address of the non-AP MLD or the non-AP MLD is State 4 ... | Revised – Agree in principle with the commenter. There are 3 cases for checking the affiliated non-AP STA MAC address. We provide corresponding texts to address the 3 cases.*Case 1 (MLD-MLD non-AP STA address conflict): As raised by commenter, a non-AP MLD sending (re)association request has address of an affiliated non-AP STA conflict with the MAC address of a non-AP STA affiliated with an existing association non-AP MLD**Case 2 (MLD-non-MLD non-AP STA address conflict): a non-AP MLD sending (re)association request has MAC address of an affiliated non-AP STA conflict with the MAC address of an associated non-AP STA not affiliated with a non-AP MLD.* *Case 3 (non-MLD- MLD non-AP STA address conflict): a non-AP STA not affiliated with a non-AP MLD sending (re)association request has the same MAC address as a non-AP STA affiliated with an existing association non-AP MLD.* TGbe editor to make the changes shown in 11-23/1655r3 under all headings that include CID 19169 |

**Discussion:**

The commenter raises a question beyond simply checking of MAC address of affiliaterd STAs.

There are 3 cases below.

Case 1 (MLD-MLD non-AP STA address conflict): As raised by commenter, a non-AP MLD sending (re)association request has address of an affiliated non-AP STA conflict with the MAC address of a non-AP STA affiliated with an existing association non-AP MLD

Case 2 (MLD-non-MLD non-AP STA address conflict): a non-AP MLD sending (re)association request has MAC address of an affiliated non-AP STA conflict with the MAC address of an associated non-AP STA not affiliated with a non-AP MLD.

Case 3 (non-MLD- MLD non-AP STA address conflict): a non-AP STA not affiliated with a non-AP MLD sending (re)association request has the same MAC address as a non-AP STA affiliated with an existing association non-AP MLD.

Note that non-MLD-non-MLD case is handled by SA query.

**Proposal:**

*TGbe editor: Modify Clause 9.4.1.9 as follows (track change on):*

***9.4.1.9 Status Code field***

***TGbe editor: Please update the new status code as shown below (#20007).***

**Table 9-78—Status codes *(continued)***

|  |  |  |
| --- | --- | --- |
| **Status code** | **Name** | **Meaning** |
| 141 | DENIED\_OPERATION\_PARAME- TER\_UPDATE | Operation parameter update denied because the requested operation parameters or capabilities are not acceptable. |
| <ANA> | NON\_AP\_STA\_MAC\_ADDRESS\_IN\_USE | The non-AP STA MAC address is used by an existing associated non-AP STA. |

*TGbe editor: Modify Clause 35.3.5.1 as follows (track change on):*

* + - 1. **ML (re)setup procedure**

(…existing texts…)

The AP MLD shall not accept a link that is requested for (re)setup if any of the following condition is true:

* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter of the AP affiliated with the AP MLD (if present) corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the AP affiliated with the AP MLD (if present) corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <HE-MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME- START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <EHT-MCS, NSS> tuples indicated by the Basic EHT-MCS And NSS Set field of the EHT Operation parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME- START.request primitive.
* If the non-AP STA affiliated with the non-AP MLD 1 corresponding to that link has the same MAC address as a non-AP STA 2 (that is affiliated with a non-AP MLD 2 or not affiliated with a non-AP MLD) associated with the AP affiliated with the AP MLD corresponding to the link, and the MLD MAC address of the non-AP MLD 1 is not the same as the non-AP MLD 2 when the non-AP STA 2 is affiliated with a non-AP MLD 2 or is not the same as the MAC address of the non-AP STA 2 when the non-AP STA 2 is not affiliated with a non-AP MLD 2.(#19169)

(…existing texts…)

*TGbe editor: Modify Clause 11.3.6.3 as follows (track change on):*

* + - 1. **AP, AP MLD, or PCP association receipt procedures**

***Insert the following paragraph as the first paragraph of the subclause:***

For a non-AP MLD associated with an AP MLD, if an AP affiliated with the AP MLD receives an Association Request frame without a Basic Multi-Link element from a non-AP STA affiliated with the non- AP MLD, then the AP shall reject the association request with a status code of DENIED\_STA\_AFFILIATED\_WITH\_MLD\_WITH\_EXISTING\_MLD\_ASSOCIATION.

***Change the remaining paragraphs of the subclause as follows:***

The following procedure shall be used by an AP or PCP ~~U~~upon receipt of an Association Request frame from a STA ~~the AP or PCP shall use the following procedure~~ or by an AP MLD after an AP affiliated with the AP MLD receives an Association Request frame with Basic Multi-Link element from a non-AP STA affiliated with a non-AP MLD:

(…existing texts…)

* + - * 1. The SME shall refuse an association request from a STA that does not support all of the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter in the MLME-START.request primitive.
				2. The SME shall refuse an association request from an HT STA that does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter in the MLME-START.request primitive.
				3. The SME shall refuse an association request from a VHT STA that does not support all of the

<VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter in the MLME-START.request primitive.

* + - * 1. The SME shall refuse an association request from a HE STA that does not support all of the <HE- MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter in the MLME-START.request primitive.

i1) The AP affiliated with an AP MLD shall refuse an association request from a non-AP STA 1 that is not affiliated with a non-AP MLD if the MAC address of the non-AP STA 1 is the same as a non-AP STA associated with the AP and affiliated with a non-AP MLD 1, and the MAC address of the non-AP STA 1 is not the same as the MLD MAC address of the non-AP MLD 1. (#19169)

(…existing texts…)

*TGbe editor: Modify Clause 11.3.6.5 as follows (track change on):*

* + - 1. **AP, AP MLD, or PCP reassociation receipt procedures**

(…existing texts…)

The following procedure shall be used by an AP or PCP u~~U~~pon receipt of a Reassociation Request frame from a STA ~~the AP or PCP shall use the following procedure~~ or by an AP affiliated with an AP MLD upon receipt of a Reassociation Request frame with Basic Multi-Link element from a non-AP STA affiliated with a non-AP MLD:

(…existing texts…)

* + - * 1. The SME shall refuse a reassociation request from a STA that does not support all the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter in the MLME-START.request primitive.
				2. The SME shall refuse a reassociation request from an HT STA that does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter in the MLME-START.request primitive.
				3. The SME shall refuse a reassociation request from a VHT STA that does not support all of the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter in the MLME-START.request primitive.
				4. The SME shall refuse a reassociation request from a HE STA that does not support all of the <HE- MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter in the MLME-START.request primitive.

i1) The AP affiliated with an AP MLD shall refuse a reassociation request from a non-AP STA 1 that is not affiliated with a non-AP MLD if the MAC address of the non-AP STA 1 is the same as a non-AP STA associated with the AP and affiliated with a non-AP MLD 1, and the MAC address of the non-AP STA 1 is not the same as the MLD MAC address of the non-AP MLD 1. (#19169)

(…existing texts…)

*TGbe editor: Modify Clause 35.3.6.4 as follows (track change on):*

* + - 1. **ML reconfiguration to the ML setup**

(…existing texts….)

The AP MLD shall accept a delete link request for a link ID and shall set the corresponding Status subfield to SUCCESS in the Reconfiguration Status Duple subfield, except if it is an NSTR mobile AP MLD and the delete link request is for deleting the primary link of the NSTR mobile AP MLD in which case the AP MLD shall reject the delete link request and shall set the corresponding Status subfield to REQUEST\_DECLINED.

The AP MLD shall reject an add link request if any of the following condition is true:

* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the rates in the BSSBasicRateSet parameter and all of the membership selectors in the BSSMembershipSelectorSet parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the MCSs in the Basic HT-MCS Set field of the HT Operation parameter of the AP affiliated with the AP MLD (if present) corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the AP affiliated with the AP MLD (if present) corresponding to the link in the MLME-START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <HE-MCS, NSS> tuples indicated by the Basic HE-MCS And NSS Set field of the HE Operation parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME- START.request primitive.
* The non-AP STA affiliated with the non-AP MLD corresponding to the link does not support all of the <EHT-MCS, NSS> tuples indicated by the Basic EHT-MCS And NSS Set field of the EHT Operation parameter of the AP affiliated with the AP MLD corresponding to the link in the MLME- START.request primitive.
* If the non-AP STA affiliated with the non-AP MLD corresponding to that link has the same MAC address as a non-AP STA (that is affiliated with a non-AP MLD or not affiliated with a non-AP MLD) associated with the AP affiliated with the AP MLD corresponding to the link.(#19169)

If the AP MLD accepts link addition for one or more links, the AP MLD shall include Group Key Data subfield in the Link Reconfiguration Response frame when using RSN. For each added link, the AP MLD shall include an MLO GTK KDE, an MLO IGTK KDE, and an MLO BIGTK KDE in the Group Key Data subfield providing group keys for the added link identified by the Link ID subfield.

(…existing texts….)