IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe CC-36 Miscellaneous Comment Resolutions |
| Date: 2021-11-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | montemurro.michael@gmail.com  |

Background

This contribution proposes comment resolutions to comments received in CC36 on Clause 12 of P802.11be D1.0. The resolutions will be shown relative to D1.0 and when indicated D1.1

CIDs 6050, 6052, 6934, 6184, 5191

Straw\_poll: Adopt the resolutions in document 11-21/1657r3 for CIDs 6050, 6052, 6934, and incorporate the changes into the TGbe draft.

Straw\_poll: Adopt the resolutions in document 11-21/1657r3 for CIDs 6184 and 5191, and incorporate the changes into the TGbe draft.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6050 | 12.7.2 | 225.13 | the link Id + related address in Association Request that is not accepted need not be in EAPOL-Key 2. | As in comment |
| 6052 | 12.7.2 | 225.13 | the link Id + related address in Association Request that is not accepted need not be verified. | As in comment |

### Discussion:

In the 4-way handshake for legacy devices, the Supplicant includes the RSNE and RSNXE in message 2 so that Authenticator can verify that information (RSNE and RSNXE) supplied by the Supplicant in the Reassociation Request. In the case of MLO, the Authenticator also needs to verify that the link information provided by the non-AP MLD Supplicant in the Reassociation Request (Affiliated STA MAC Address, RSNE and RSNXE). This helps prevent against man-in-the-middle attacks (see 12.7.6.8) in the base standard.

At the time that the non-AP MLD Supplicant provides the link ID, related MAC address, RSNE, and RSNXE in the Reassociation Request, there is no indication that a link is not accepted by the AP MLD. The information supplied in message 2 must be the same as supplied in the Reassociation Request to be verified. Note that the Reassociation request is not protected.

After further offline discussion, the following

* For message 2, no changes in the spec needed because the AP MLD authenticator needs to verify the general integrity of the (re)association message despite the fact that the AP MLD may have accepted only a subset of the requested links.
* For message 3, the AP MLD authenticator includes MAC link mac address, RSNE, and RSNXE of all the affiliated APs. The non-AP MLD supplicant verifies that the information for all the requested links match the information advertised in beacons/probe resp/ML probe resp received for those links. In addition, the non-AP MLD shall also verify the beacon/probe response/ML probe response for all the other links, \*if\* such info is available in the non-AP MLD
* Since the 4-way handshake takes place between the AP MLD Authenticator, and the non-AP MLD Supplicant, there is no reason to check that the A2 field in the MAC header matches the MAC address of the link the exchange is occurring on. That text should be removed.

### Proposed Resolution: (6050, 6052)

Revised. The non-AP MLD supplicant needs to provide the link ID and related address in Message 2 of the 4-way handshake so that the Authenticator can validate the information and to guard against man-in-the-middle attacks. The AP MLD needs to provide the link ID, address, and RSNE/RSNXE information in message 3 so that the Supplicant can validate the information and guard against man-in-the middle attacks. Also, remove the text that validates the A2 field since the 4-way handshake takes place between the AP MLD Authenticator and non-AP MLD Supplicant.

No changes are required for message 2.

For message 3, at 282.47 relative to draft 1.2, change

"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."

to:

"For MLO, verifies the following:

* The affiliated AP MAC address and all fields in the RSNE, and the RSNXE if present, for each requested link are identical to those as advertised by the corresponding affiliated APs of the AP MLD in Beacon, Probe Response, and ML Probe Response frame
* The affiliated AP MAC address and all fields in the the RSNE, and the RSNXE if present, of other discovered links, if information is available are identical to those advertised by the affiliated APs of the AP MLD in Beacon, Probe Response, and ML Probe Response frames

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 deauthenticates."

For message 2 at 273.52 relative to draft 1.2, remove:

“For MLO, the Authenticator’s SME shall validate that the MAC address used as the Address 2 field of the MAC header of the MPDU containing message 2 matches an affiliated STA MAC address included in one of the MLO Link KDEs and that the LinkID field and affiliated STA MAC address for each link matches the LinkID field and affiliated STA MAC address included in the Multi-Link element received in the (Re)Association Request frame.’

For message 3 at 274.24 relative to draft 1.2, remove:

“For MLO, the Supplicant’s SME validates that the Address 2 field of the MAC header of the MPDU containing message 3 matches an affiliated AP MAC address included in one of the MLO Link KDEs.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6934 | 9.6.34 | 159.11 | EHT Action frames are delivered at MLD level (i.e. SN/PN at MLD level and PPDU can be transmitted over any affiliated link). What other non-EHT management frames are considered as MLD Level (Association Req/Res, ADDBA etc.). | Need to indicate which management frames should be handled at MLD level and which are link related (Measurement etc.) ? |

### Discussion:

From the comment, this is less a question about EHT Action frames and more a question about ML operation and which management frames are transmitted at the MLD level. As such, this is more of an architecture question. Clause 4.9.5 was added to a subsequent draft after the comment collection on D1.0. This clause describes the distribution of MAC functions between the MLD level and the affiliated STA level.

### Proposed Resolution: (6934)

Revised. The comment asks a multi-link architecture question on which management frames are transmitted at the MLD level. Clause 4.9.5 was added with the acceptance of document <https://mentor.ieee.org/802.11/dcn/21/11-21-0577-05-00be-cr-mld-architecture.docx> and is already published. In clause 4.9.5, see page 57 line 38 of D1.2 for a description in the distribution of MAC functions.

Note to Editor: This contribution has been approved in Motion 215 so no further changes required for the draft.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 6184 | 35.3.3 | 250.57 | The note seems to indicate that the affliated AP MAC can be the same as the MLD MAC. However the requirement above states that "An MLD has an MLD MAC address that singly identifies the MLD." Not only does this contradict, but it causes problems with protocols such as FT, which require each MAC in the ESS to to be different. If the objective behind the requirement is to reduce the number of global MACs required, one of the affiliated AP MACs could set the "locally addressed bit" in the MAC address. | Remove the cited sentence "NOTE--The MLD MAC address of an MLD might be the same as the MAC address of one affiliated STA or different from the MAC address of any affiliated STA." |
| 5191 | 35.3.3 | 250.57 | If we allow that the MLD MAC address can be the same as an affiliated STA's MAC address, then for the link that the link MAC address is different from the MLD MAC address, the MSDU to the non-AP MLD will be separated from the MSDU to the legacy STA through going different MAC SAP; for the link that the link MAC address is the same as the MLD MAC address, the MSDU to the non-AP MLD will be mixed with the MSDU to the legacy STA through going the same MAC SAP. I'm wondering that this asymettric may complicate the MAC processing design. Furthermore, it will not bring any benefits except of saving a global MAC address | Remove this note "(#2759)NOTE--The MLD MAC address of an MLD might be the same as the MAC address of one affiliated STA or different from the MAC address of any affiliated STA." |

### Discussion:

The MLD MAC address uniquely identifies the MAC entity. Furthermore for security purposes, the MLD MAC Address provides the identity for the Authenticator or the Supplicant. On the AP side, an affiliated AP can provide services to legacy STAs. In that case, the MAC address needs to be distinct from the AP MLD since they have different Authenticators.

Note that if there is a concern about assigning a globally unique MAC address to an affiliated AP or the AP MLD, the AP MLD could be assigned a globally unique MAC address while the affiliated AP could use the same MAC address, but with the locally addressed bit set.

There is no really need for a note like this. It suggests an implementation decision that has the potential to open a new security attack surface. Given that it the note isn’t even a requirement, it should be removed.

### Proposed Resolution: (6184, 5191)

Accepted.