IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for CIDs Related to STA MAC Address of Non-AP MLD |
| Date: 2021-04-1 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Guogang Huang | Huawei |  |  | huangguogang1@huawei.com |
| Michael Montemurro |  |  |  |
| Stephen McCann |  |  |  |
| Ming Gan |  |  |  |
| Yuchen Guo |  |  |  |
| Yunbo Li |  |  |  |
| Yiqing Li |  |  |  |
| Zhenguo Du |  |  |  |
| Rob Sun |  |  |  |
| Mengyao Ma |  |  |  |

Abstract

This submission proposes resolutions for CIDs 2297 on TGbe D0.3 regarding the STA MAC address of the non-AP MLD.

Revisions:

- Rev 0: Initial version of the document.

- Rev 1: Update based on Draft P802.11\_D1.0

**Introduction**

***Editing instructions formatted like this are intended to be copied into the TGbe Draft 0.4 (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** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 2297 | Michael Montemurro | 128.46 | 35.3.3 | This should not be a requirements for a STA affiliated with a non-AP MLD since the MAC address of the AP affiliated with the non-AP MLD is different and links are based on link pairs of MAC addresses. | At cited location, delete"each non-AP STA affiliated with the non-AP MLD shall have different MAC addresses" | **Revised**Agree in principle with the commenter. The nan-AP MLD can use a single MAC address, i.e. the non-AP MLD MAC address is the same as the MAC address of any affiliated STA. So a corresponding Single MAC Address Mode Enable subfield is added. **TGbe editor to make the changes shown in 11-21/****0594r1 tagged as 2297** |

**Discussion:**

***Non-AP MLD with a single MAC Address, i.e. the non-AP MLD MAC address is the same as the MAC address of any affiliated STA***

The single MAC address for the non-AP MLD has the following benefits:

* For the AP MLD side, there is no need to do address conversion for the non-AP MLD
* No addressing issue, e.g.
	+ It simplifies the non-AP MLD’s roaming between a legacy AP and an AP MLD [1].
	+ It simplifies the TDLS addressing proposed in [2]
* Signaling overhead reduction
	+ E.g. no need to advertise the affiliated STA MAC addresses for the non-AP MLD during the association and 4-way handshake [3]

In addition, the single MAC address for the non-AP MLD is a special case of the non-AP MLD with multiple MAC addresses. Hence, no big change to the current draft text.

**References**

[1] 11-20-0669-04-00be-mld-transition

[2] 11-20-1692-01-00be-tdls-handling-in-mlo.pptx

[3] 11-20-0727-00-00be-mla-link-mac-addresses-security.pptx

**Proposed spec text:**

***TGbe editor: modify the following text in page 132***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | B0 B3 | B4 | B5 B6 | B7 B11 |  B12 | B13 B15 |
| Maximum Number Of Simultaneous Links | SRS Support | TID-To-Link Mapping Negotiation Supported | Frequency Separation For STR | Single MAC Address Mode Enable | Reserved |
| Bits: |  | 4 |  | 1 | 2 | 5 | 1 | 3 |

 **Figure 9-788em—MLD Capabilities subfield format(#1078)(#1475)(#2981) (#2297)**

(#2139)The subfields of the MLD Capabilities subfield are defined in [Table 9-322ao (Subfields of the MLD](#bookmark100) [Capabilities field(#1078)(#1475)(#2981)](#bookmark100) **[(#2297)](#bookmark100)**[)](#bookmark100).

**Table 9-322ao—Subfields of the MLD Capabilities field(#1078)(#1475)(#2981)**

|  |  |  |
| --- | --- | --- |
| **Subfield** | **Definition** | **Encoding** |
| Maximum Number Of Simultaneous Links | Indicates the maximum number of affiliated STAs in the MLD that sup- port simultaneous transmission or reception of frames. | Set to the maximum number of affiliated STAs in the MLD that support simultaneous trans- mission or reception of frames minus 1. |
| SRS Support | Indicates support for the reception of a frame that carries an SRS Control sub- field. | For an EHT AP:Set to 1 to indicate that an AP MLD with which the AP is affiliated is capable of receiving a frame with SRS Control sub- field. Set to 0 otherwise.For a non-AP EHT STA: Set to 0. |
| TID-To-Link Map- ping Negotiation Sup- ported | Indicates support for TID-to-link mapping negotiation. | Set to 0 if dot11TIDtoLinkMappingActivated is false.Set to 1 if dot11TIDtoLinkMappingActivated is true and the MLD supports mapping each TID to the same or different link set.Set to 2 if dot11TIDtoLinkMappingActivated is true and the MLD supports mapping all TIDs to the same link set.The value 3 is reserved.(See 35.3.6.1.3 (Negotiation of TID-to-link mapping)) |
| Frequency Separation For STR | Indicates the minimum frequency gap between any two links that is recom- mended by the non-AP MLD for STR operation. The frequency gap is speci- fied as the difference between the nearest frequency edges of the two links. | For a non-AP EHT STA:Set to 0 to indicate no frequency separation information is provided.Set to a nonzero value to indicate the STR frequency gap, in units of 80 MHz, minus 80 MHz.For an EHT AP: Set to 0. |
| Single MAC Address Mode Enable | Indicate the single MAC address mode is used by a non-AP MLD. The single MAC address means that the non-AP MLD MAC address is the same as the MAC address of any affiliated STAs. | For a non-AP MLD:Set to 1 to indicate the single MAC address mode is used. Set to 0 otherwise.For an AP MLD:Set to 0.  |

***TGbe editor: Please update the following paragraphs in page 133 as follows:***

Each Per-STA Profile subelement starts with STA Control field followed by a variable number of fields and elements as defined in 35.3.2 (Advertisement of multi-link information in Multi-Link element(#2294)).

(#1035)(#2183)(#2451)(#1799)(#1050)(#1778)(#2165)The format of a Per-STA Profile subelement is defined in [Figure 9-788en (Per-STA Profile subelement format)](#bookmark102).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subelement ID | Length | STA Control | STA Info | STA Profile |

Octets: 1 1 2 variable variable

**Figure 9-788en—Per-STA Profile subelement format**

The format of the STA Control field is defined in [Figure 9-788eo (STA Control field for-](#bookmark103) [mat(#1906)(#1907)(#1078)(#1475)(#2981))](#bookmark103).

B0 B3 B4 B5 B6 B7 B8 B9 B10 B15

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Link ID | Complete Profile | MACAddress Present | Beacon Interval Present | DTIM Info Present | NSTRLink Pair Present | NSTRBitmap Size | Reserved |

Bits: 4 1 1 1 1 1 1 6

**Figure 9-788eo—STA Control field format(#1906)(#1907)(#1078)(#1475)(#2981)**

The Link ID subfield specifies a value that uniquely identifies the link where the reported STA is operating on. The usage of link ID is defined in 35.3.2.1 (General)(#1776).

(#2436)The Complete Profile subfield is set to 1 when the Per-STA Profile subelement of the Multi-Link element carries the complete profile as defined in 35.3.2.2 (Advertisement of complete or partial per-link information (#1859)). Otherwise the subfield is set to 0.

(#1035)(#2183)(#2451)(#1799)(#1050)(#1778)(#2165)The MAC Address Present subfield indicates the presence of the STA MAC Address subfield in the STA Info field and is set to 1 if the STA MAC Address subfield is present in the STA Info field; otherwise set to 0. (#2297)For a non-AP MLD, this field is set to 1 if both the Complete Profile subfield and the Single MAC Address Mode Enable subfield are set to 1; otherwise, this subfield is set to 0. For an AP MLD, this field is set to 1 if the Complete Profile subfield is set to 1; otherwise, this field is set to 0.

***TGbe editor: Please update the following paragraphs in page 226 as follows:***

The format of the MLO BIGTK KDE is shown in [Figure 12-47b (MLO BIGTK KDE(#2290))](#bookmark15).

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

Bits: 16 48 4 4 (Length – 13) **×** 8

**Figure 12-47b—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 12-47c (MLO Link KDE(#2290))](#bookmark16).

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

Octets: 1 0 or 6 variable variable

**Figure 12-47c—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 12-47d (Link Information field(#2290))](#bookmark17).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | LinkID | RSNXEInfo | MAC Address Present | Reserved |
| Bits: | 4 | 1 | 1 | 2 |

**Figure 12-47d—Link Information field(#2290)(#2297)**

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

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

(#2297)The MAC Address Present subfield indicates whether the MAC Address field is present. For a non-AP MLD, then the MAC Address Present subfield is set to 0 if the single MAC address mode is used by a non-AP MLD; otherwise, the MAC Address Present subfield is set to 1. For an AP MLD, the MAC Address Present subfield 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.

***TGbe editor: Please update the following paragraphs in page 224 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
* **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) (#2297)For MLO, the non-AP MLD shall include a MLO Link KDE containing the LinkID field and affiliated STA MAC address for each link included in the Association Request frame if the single MAC address mode is not used by the non-AP MLD. 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. (#2290) (#2297)For MLO, if the single MAC address mode is not used by the non-AP MLD, 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.

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 for each link in Beacons, Probe Response, and ML Probe Response frames. For MLO, the Authentica- tor’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. If the second optional RSNE is present, the STA shall either use that cipher suite with its pairwise key or deau- thenticate. 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 security 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.

***TGbe editor: Please update the following paragraphs in Subclause 35.3.3:***

* + 1. **Multi-link device addressing**

An MLD has an MLD MAC address that singly identifies the MLD.

(#1156)The MAC address of each AP affiliated with an AP MLD shall be different from each other.

(#2297)The non-AP MLD MAC address is different from the MAC address of any affiliated STA and the MAC address of each affiliated STA is different from each other. If the single MAC address mode is used, the non-AP MLD MAC address is the same as the MAC address of any affiliated STA;

**SP 1: Do you support the single MAC address mode for a non-AP MLD in R2?**

**SP 2: Do you support the single MAC address mode for a non-AP MLD in R1?**