IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CC36 Resolution for CIDs related to Clause 12 | | | | |
| Date: 2022-04-01 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Gaurav Patwardhan | HPE |  |  | Gaurav.patwardhan@hpe.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs received for TGbe CC36: 4922, 4923, 5185, 5187, 5188, 5189, 5360, 6043, 6045, 6653, 6933, 7447.

***TGbe editor: The baseline for this document is 11be D1.5 with exceptions as listed in-line.***

**Revisions:**

* Rev 0: Initial version of the document.
* Rev 1: Changes for CID 5360 based on offline discussion
* Rev 2: Minor editorial changes

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

***Editing instructions formatted like this are intended to be copied into the TGbe 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** | **Clause** | **Pg.Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 4922 | 12.5.3.3.3 | 216.41 | Formatting of "If... otherwise" unclear for A1 | "Rephrase/reformat as is done for A4:  ""A1 is set as follows:  -- if ..., A1 is set to the MLD MAC address ...""  -- ""otherwise, A1 is set to MPDU Address 1 field.""" | **Revised**  Agree in principle with the commenter. Text is refactored to make it clear.  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 4922** |
| 4923 | 12.5.3.3.3 | 216.48 | Formatting of "If... otherwise" unclear for A2 | "Rephrase/reformat as is done for A4:  ""A2 is set as follows:  -- if ..., A2 is set to the MLD MAC address ...""  -- ""otherwise, A2 is set to MPDU Address 2 field.""" | **Revised**  Agree in principle with the commenter. Text is refactored to make it clear.  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 4923** |
| 5185 | 12.5.3.3.3 | 216.45 | The current text may make people misunderstanding that the snetence ''If ..." also applies to the second bullet. But obviously, it's not the intention | Delete bullet symbols | **Revised**  Agree in principle with the commenter. Text is refactored to make it clear.  **TGbe editor, please implement changes as shown in doc 11-21/575r2 tagged 4922** |
| 5187 | 12.5.3.3.3 | 216.46 | change "otherwise, A1 is set to MPDU Address 1 field" to "otherwise, A1 is set to the MPDU Address 1 field" | As in comment. | **Accepted**  Agree with the commenter. Text is refactored to make it clear.  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 5187** |
| 5188 | 12.5.3.3.3 | 216.53 | change "otherwise, A2 is set to MPDU Address 1 field" to "otherwise, A2 is set to the MPDU Address 2 field" | Add ''the" before "MPDU Address 2 field" | **Accepted**  Agree with the commenter. Text is refactored to make it clear.  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 5188** |
| 5189 | 12.5.3.3.3 | 216.62 | Add a subbullet to describe the case "Both To DS subfield and From DS subfield are set to 1 " | "Add a subbullet as:  else if both To DS and From DS subfields are set to 1 in the MAC header of the MPDU, set A3 to the MLD MAC address of the transmitting MLD." | **Revised**  The comment has been addressed by the resolution to CID #4294 in document 11-22/1609r0 and is already incorporated in P802.11be\_D1.5.  **TGbe Editor no further changes are needed.** |

***TGbe Editor: Modify 12.5.3.3.3 as follows (track change on):***

* + - * 1. **Construct AAD**

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

For PV0 MPDUs, the format of the AAD is shown in Figure 12-19 (AAD construction for PV0 MPDUs). The length of the AAD for PV0 varies depending on the presence or absence of the QC and A4 fields and is shown in Table 12-3 (AAD length for PV0 MPDUs).

The AAD is constructed from the MPDU header. The AAD includes neither the Duration/ID field nor the HT Control field because the contents of these fields might change during normal operation (e.g., due to a rate change preceding retransmission). The HT Control field might also be inserted or removed during normal operation (e.g., retransmission of an A-MPDU where the original A-MPDU included an MRQ that has already generated a response). For similar reasons, several subfields in the Frame Control field are masked to 0. For PV0 MPDUs, AAD construction is performed as fol- lows:

FC – MPDU Frame Control field, with

Subtype subfield (bits 4 5 6) in a Data frame masked to 0

Retry subfield (bit 11) masked to 0

Power Management subfield (bit 12) masked to 0

More Data subfield (bit 13) masked to 0

Protected Frame subfield (bit 14) always set to 1

vi) +HTC subfield (bit 15) as follows:

Masked to 0 in all Data frames containing a QoS Control field

Unmasked otherwise

vii) Other subfields are not modified

~~A1 – MPDU Address 1 field.~~(#4922)A1 is set as follows:

If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to the MLD MAC address of the intended receiver MLD of the MPDU,

otherwise, Al is set to (#5187)the MPDU Address 1 field.

~~A2 – MPDU Address 2 field.~~(#4923)A2 is set as follows:

If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to the MLD MAC address of the transmitting MLD of the MPDU,

otherwise, A2 is set to (#5188)the MPDU Address 2 field.

~~A3 – MPDU Address 3 field.~~If dot11MultiLinkActivated is true, MPDU Address 3 field is BSSID and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then:

* (#4924)A3 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD.
* (#4924)Otherwise, A3 is set to the MPDU Address 3 field.

SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked to 0. The Fragment Number subfield is not modified.

~~A4 – MPDU Address field, if present.~~A4, if present, is set as follows:

* if dot11MultiLinkActivated is true, MPDU Address 4 field is a BSSID, and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A4 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD.
* otherwise A4, if present, is set to the MPDU Address 4 field.

QC – QoS Control field contains the MSDU priority, if present. The QC TID is used in the construction of the AAD. When in a non-DMG BSS and both the STA and its peer have their SPP A-MSDU Capable fields equal to 1, bit 7 (the A-MSDU Present field) is used in the construction of the AAD. The remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDU Type bit 8 are used in the construction of the AAD, and the remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 9 to 15).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Pg.Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 6043 | 12.5.3.3.4 | 217.35 | the condition that the recipient is ffliated with MLD should be added (part of if sentence) | AS in comment | **Accept**  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 6043** |
| 6045 | 12.5.3.3.4 | 219.58 | the condition that the recipient is ffliated with MLD should be added (part of if sentence) | AS in comment | **Accept**  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 6045** |

***TGbe Editor: Modify 12.5.3.3.4 as follows (track change on):***

**12.5.3.3.4 Construct CCM nonce**

Octets: 1 6 6

|  |  |  |
| --- | --- | --- |
| Nonce Flags | STA Or MLD MAC Address Identified By A2 | PN |

**Figure 12-21—CCM nonce**

If dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed Data frame (#6043) to a STA affiliated with an MLD, then the STA Or MLD MAC Address Identified By A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ STA Or MLD MAC Address Identified By A2 subfield shall contain the Address 2 field from the MAC header for PV0 MPDUs and the MAC address identified by the A2 field in the MAC header for PV1 MPDUs (see 9.8.3.2 (Address fields)).

***TGbe Editor: Modify 12.5.5.3.4 as follows (track change on):***

**12.5.5.3.4 Construct GCM nonce**

## *Change the second paragraph as follows:*

If dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed Data frame (#6045) to a STA affiliated with an MLD, then the A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ A2 subfield shall contain the Address 2 field from the MAC header.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Pg.Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 5360 | 12.5.3.3.1 | 215.31 | Retransmitted MPDUs are not modified on retransmission, it's not correct for the MLD device as the TA/RA changed in the MAC header if we say it retransmission on other link. | separate MLD device from legacy device when illustrate the retransmitted MPDUs. | **Revised**  Agree in principle with the commenter. Text added to handle the case of retransmitted MPDUs in multi-link operation.  **TGbe editor, please implement changes as shown in doc 11-22/575r2 tagged 5360.** |

***TGbe Editor: Modify 12.5.3.3.1 as follows (track change on):***

* + - * 1. **General**

***(…. exisiting text and Fig 12-18…)***

For secure PV0 MPDUs, CCMP encrypts the Frame Body field of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key.

NOTE—Retransmitted MPDUs are not modified on retransmission. (#2577)(#2578)For MLO, MPDUs are not encapsulated with a new PN when retransmitted on another link.

NOTE -(#5360) For MLO, a retransmitted individually addressed MPDU on another link has different addresses in the address fields of the MAC header when compared to the original transmission. (See 35.3.3 Multi-link device addressing)

NOTE – (#5360) For MLO, when an individually addressed management frame is retransmitted on another link, the encrypted data is modified on retransmission.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Pg.Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 6653 | 12.5.3.3.1 | 215.41 | "In case of a secure PV0 MPDU that is an individually addressed Data frame to be encrypted by an MLD, construct the CCM nonce block as defined in 12.5.3.3.4 (Construct CCM nonce) from the PN, transmitting MLD MAC address, and the priority value of the MPDU." Is CCMP allowed to be used for encryption of individually addressed frames by EHT devices? The spec also requires that EHT devices to support GCM -256. Please clarify. | As in comment. | **Reject**  CCMP is allowed for encryption of individually addressed frames by EHT devices. In addition to this, an EHT device mandatorily supports GCM-256. The comment fails to identify a technical issue and lacks context and details necessary to come up with changes to draft text to satisfy it. |
| 6933 | 12.5.3.3.3 | 216.55 | In case of 4 addresses (To DS=1, From DS=1, Basic A-MSDU) the addresses of the frame transmitted over the air is A3=TA, A4=TA however the addresses for AAD Construction is A3=Receiving MLD, A4 = Transmitting MLD. This replacement is not consistent. A3 should be the same as A4. | Change as in comment | **Revised**  The comment has been addressed by the resolution to CID #4294 in document 11-22/1609r0 and is already incorporated in P802.11be\_D1.5.  **TGbe Editor no further changes are needed.** |
| 7447 | 12.5.3.3.3 | 0.00 | This subclause defines the fields (and masks) used for AAD calculation, however the changes here appear to specify how the field values themselves are defined (e.g. "A1 is set to ... field"). If the idea is that a different value should overwrite the value in the A1 field purely for the purpose of AAD calculation, that should be more clearly specified | Clarify | **Reject**  Overwriting a value in A1 with a second value before being used for AAD constuction has the same end result as setting A1 directly to the second value before AAD construction. Additionally, there is precedence from baseline specification (REVme\_D1.0) to use the verb ‘set’ in AAD construction as indicated by the following normative text from subclause 12.5.3.3.3 Bullet a) Sub-bullet 1) sub-bullet v) - *“Protected Frame subfield (bit 14) always set to 1”* |