IEEE P802.11
Wireless LANs

|  |
| --- |
| D1.0 CIDs in clauses 10.71.5 and 10.71.6 except SN (de)anonymization |
| Date: 2025-07-31 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

Abstract

This submission proposes resolution of comments received against the following sections of TGbi Draft 1.0:

* 10.71.5.1 (MAC header anonymization parameter set selection)
* 10.71.5.3 (Packet number anonymization)
* 10.71.5.4 (Addressing)
* 10.71.5.5 (Timestamp anonymization)
* 10.71.6.1 (Address filtering)
* 10.71.6.3 (Packet number deanonymization)
* 10.71.6.5 (Timestamp deanonymization)

We propose draft specification text for TGbi draft D1.3.

Resolved CIDs (15): 126, 127, 250, 356, 357, 567, 579, 580, 581, 587, 818, 819, 820, 874, 1072

Revisions:

* Rev 00: Initial version of the document.
* Rev 01.
	+ Resolved CIDs list was missing CID #874
	+ Included notes at the start of 10.71.5.5 and 10.71.6.5 required to address CID #579.

**Background**

Almost all changes are related to adding BPE text.

This document groups related sections so make the document easier to review.

* 10.71.5.1 (MAC header anonymization parameter set selection), 10.71.5.4 (Addressing) and 10.71.6.1 (Address filtering) are grouped because Address filtering is the receiver processing corresponding to the transmitter processing for Addressing and MAC header anonymization parameter set selection
* 10.71.5.3 (Packet number anonymization) and 10.71.6.3 (Packet number deanonymization) are grouped because they describe transmitter and receiver processing related to PN
* 10.71.5.5 (Timestamp anonymization) and 10.71.6.5 (Timestamp deanonymization) are grouped because they describe transmitter and receiver processing related to timestamp.

Changes to 10.71.5.2 (Sequence number anonymization) and 10.71.6.4 (Sequence number deanonymization) are provided in a separate document.

| **CID** | **Commenter** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| 579 | Mark RISON | 10.71.5.1 | 86.53 | "A MAC header parameter set for given EDP epoch comprises a set of values for EDP\_SN\_offset, EDP\_PN\_offset and EDP\_STA\_address (defined in 10.71.3 (Establishing frame anonymization parameter sets))" is ignoring the BPE variants in 10.71.4 | Refer to 10.71.4 too | **Revised****Changes**:*Instructions to the editor:*Please make the changes as shown under CID #579 in doc 11-25/1118 |
| 580 | Mark RISON | 10.71.5.1 | 86.56 | "the sequence number field, packet number field and either Address 1 (in frames transmitted by the AP MLD) or Address 2 (in frames transmitted by the non-AP MLD) respectively." -- field names are uppercase and should be followed by "field" | As it says in the comment | **Revised****Changes**:*Instructions to the editor:*Please make the changes as shown under CID #580 in doc 11-25/1118 |
| 1072 | Philip Hawkes | 10.71.5.1 | 86.62 | "the current EDP epoch" is not quite correct. If an OTA MAC collision is detected then there is an epoch offset added as per 10.71.2.5. | Correct | **Rejected****Rationale**: This text is appropriate here. The epoch offset resulting from an OTA MAC Collision warning is addressed in 10.71.3. |
| 581 | Mark RISON | 10.71.5.1 | 86.64 | "Retransmissions are addressed in 10.71.2.1 (General). " -- no, they're not | Give the correct xref or add a description of retransmissions (are they the same as retries?) | **Revised****Changes**:*Instructions to the editor:*Please make the changes as shown under CID #581 in doc 11-25/1118 |
| 250 | Jarkko Kneckt | 10.71.5.3 | 88.40 | The OPN anonymization scheme can cause OPN values overlap, i.e. OPN runs over the maximum value. This is uncommon situation that may cause issues to STAs. | Clarify how the maximum OPN value overrun is handled, or avoided. | **Rejected**.**Rationale**: The transmitter reduces the value of OPN (after addition with EDP\_PN\_offset) to be within the range 0 to 2^48-1, so there is no problem. This text is already aligned with use of mod operator used elsewhere in 802.11. |
| 126 | Chaoming Luo | 10.71.5.4 | 88.64 | Use consistent term. "BPE MLD", "BPE AP MLD", and "BPE EDP AP MLD" shows out in different places. | Change "BPE MLD" to "BPE AP MLD" or "BPE non-AP MLD" appropriatly.Change "BPE EDP AP MLD" to "BPE AP MLD". | **Revised**.**Discussion**: Agreed in principle **Changes**:*Instructions to the editor:*Please make the changes as shown under CID #126 in doc 11-25/1118 |
| 127 | Chaoming Luo | 10.71.5.4 | 89.01 | "group frame" is undefined, assume it should be "group addressed frame". "the group address of the frame" is vague, should be specific to the fields. The term "group frame" occurs 4 times, "group frames" occurs 2 times. | Change to: If a group addressed frame is transmitted by an affiliated STA of a BPE AP MLD, the Address 1 field value of the frame is anonymized as follows | **Revised****Discussion**: Agreed in principle. **Changes**: *Instructions to the editor:*Please make the changes as shown under CID #127 in doc 11-25/1118 |
| 587 | Mark RISON | 10.71.5.4 | 89.04 | It is not clear what the O in OGroupAddress means. If it's OTA then it should be OTAGroupAddress | As it says in the comment | **Accept** |
| 356 | Carol Ansley | 10.71.6.1 | 89.61 | Missing word, "During" | Change Sentence to start: "During the dot11EDPEpochStartTimeMargin before and during..." | **Accept***Note: Identical to CID #818* |
| 818 | John Wullert | 10.71.6.1 | 89.61 | The first phrase is worded in a manner that results in an incomplete sentence. | Rephrase as "During the dot11EDPEpochStartTimeMargin period and the transition period (see 10.71.2.1 (General) and10.71.2.2 (EDP group operations)) from an old EDP epoch to a new EDP epoch of the BPE non-AP MLD, ..." | **Accept***Note: Identical to CID #356* |
| 874 | Patrice Nezou | 10.71.6.1 | 89.61 | Why some BPE references appears in this subclause ? I think that address filtering concerns indifferently BPE and CPE STAs. | Please clarify | **Reject****Discussion:** The details when BPE is disabled are slightly different when BPE is enabled, so it made sense to deal with the two cases separately |
| 357 | Carol Ansley | 10.71.6.1 | 90.14 | Change "the" to "a" | Change to: After this transition period, until a dot11EDPEpochStartTimeMargin before the start..." | **Accepted** |
| 819 | John Wullert | 10.71.6.1 | 90.27 | Use "affiliated with" to describe STA-to-MLD relationship | Rephrase as "If a group frame is received by a STA affiliated with a BPE MLD, ..." | **Accepted**Note: This text has moved to earlier within 10.71.6.1 – see new subclause 10.71.6.1.1 (General). |
| 820 | John Wullert | 10.71.6.1 | 90.31 | Typo - Missing open parenthesis in equation | Change to "(OGroup address = GroupAddress - ..." | **Revised****Discussion**: Agreed in principle.**Changes**: *Instructions to the editor:*Please make the changes as shown under CID #820 in doc 11-25/1118 |
| 567 | Mark RISON | 10.71.3  | 83.16 | "-- The remaining 46 bits are extracted from EDP FA block according to Table 10-40b (ExtractingEDP\_STA\_address values from EDP FA Block)." -- I can imagine no end of interop issues due to endianness etc. interpretations | Be much clearer on the endianness and bit order, and give an example | **Rejected****Rationale**: The existing description is sufficiently clear. |

**Proposed spec text:**

***TGbi editor: First, we address the clauses on MAC header anonymization parameter set selection and addressing/ address filtering together together***

***TGbi editor: Apply the following changes to the text in clause 10.71.6.1 (Addressing)***

* MAC header anonymization parameter set selection

 (#579, #580)

If the AP MLD does not have BPE FA mechanisms enabled, then:

* The transmitting MLD shall generate the applicable CPE MHA parameter set according to 10.71.3 (Establishing CPE MAC header anonymization parameter sets), for the current EDP epoch in the EDP epoch sequence of the non-AP MLD at the time when a frame is to be transmitted for the first time. Retransmissions are addressed in 10.71.2.3 (EDP epoch transitions operations). (#579, #581)
* The transmitting MLD shall perform sequence number anonymization (10.71.5.2 (Sequence number anonymization), packet number anonymization (10.71.5.3 (Packet number anonymization)) and address anonymization for affiliated STA of the non-AP MLD (10.71.5.4 (Addressing)) on individually addressed frames using the selected CPE MHA parameter set. (#579)

If the AP MLD has BPE FA mechanisms enabled, then: (#126, #579)

* The transmitting BPE MLD shall generate the applicable CPE MHA parameter set according to 10.71.3 (Establishing CPE MAC header anonymization parameter sets), for the current EDP epoch in the EDP epoch sequence of the BPE AP MLD at the time when a frame is to be transmitted for the first time. Retransmissions are addressed in 10.71.2.3 (EDP epoch transitions operations). (#579, #581)
* The transmitting BPE MLD shall perform sequence number anonymization (10.71.5.2 (Sequence number anonymization), packet number anonymization (10.71.5.3 (Packet number anonymization)) and address anonymization for the affiliated STAs of the BPE non-AP MLD (10.71.5.4 (Addressing)) on individually addressed frames using the selected CPE MHA parameter set. (#579)
* The transmitting BPE MLD shall generate the applicable BPE MHA parameter set according to 10.71.4 (Establishing BPE MAC header anonymization parameter sets), using the current non-AP MLD Specific Epoch Number for the EDP epoch of the AP MLD at the time when a frame is to be transmitted for the first time. Retransmissions are addressed in 10.71.3.3 (EDP epoch transitions operations) (#579, #581).
* A transmitting BPE MLD shall perform address anonymization for the affiliated APs of the BPE AP MLD (10.71.5.4 (Addressing)) using the selected BPE MHA parameter set in all frames. (#579)
* A transmitting BPE AP MLD shall perform the following using the applicable BPE MHA parameter set: (#127, #579)
* sequence number anonymization (10.71.5.2 (Sequence number anonymization), packet number anonymization (10.71.5.3 (Packet number anonymization)), anonymization (10.71.5.4 (Addressing)) on group addressed frames
* timestamp anonymization (10.71.5.5 (Timestamp anonymization)) for Privacy Beacon frames using the selected BPE MHA parameter set.

NOTE—If the AP MLD has BPE FA mechanisms enabled, then the EDP epoch of the non-AP MLD is also the EDP epoch of the AP MLD. (#126)

***TGbi editor: Apply the following changes to the text in clause 10.71.5.4 (Addressing)***

* Addressing

MLD addressing shall be applied per 35.3.2 (MLD addressing) with the following addressing clarification. (#579)

Within the scope of this clause: (#579)

* A link-specific EDP\_STA\_address assigned to an affiliated STA on a given link is the MAC address defined as follows:
* The Local/Global bit shall be set to value 1, local address.
* The Individual/Group bit shall be set to value 0, individual address.
* EDP\_STA\_address[0:45] shall be extracted from EDP FA block as described in Table 10-40b (Extracting EDP\_STA\_address values from EDP FA Block) , according to the link ID of the link, where the EDP FA block is generated for the current EDP epoch. (#579)
* If the AP MLD has the BPE FA mechanisms enabled, then a link-specific EDP\_AP\_address assigned to an affiliated STA on a given link is the MAC address defined as follows:
* The Local/Global bit shall be set to value 1, local address.
* The Individual/Group bit shall be set to value 0, individual address.
* EDP\_AP\_address[0:45] shall be extracted from EDP FA block as described in Table 10-40h (Extracting EDP\_AP\_address values from EDP FA Block), according to the link ID of the link, where the EDP FA block is generated for the current EDP epoch. (#579)

For individually addressed frames transmitted to or from a non-AP MLD: (#579)

* If the frame is transmitted by an AP MLD to the non-AP MLD, then AP MLD shall set the Address 1 field to the link-specific EDP\_STA\_address value. (#579)
* If the frame is transmitted by the non-AP MLD to an AP MLD, then non-AP MLD shall set the Address 2 field to the link-specific EDP\_STA\_address value. (#579).

If the AP MLD has BPE FA mechanisms enabled, then: (#579)

* The AP MLD shall set the Address 2 field to the link-specific EDP\_AP\_address value in all frames transmitted by the AP MLD. (#579)
* A non-AP MLD shall set the Address 1 field to the link-specific EDP\_AP\_address value in all frames transmitted by the non-AP MLD to the AP MLD. (#579)
* The AP MLD shall set the Address 1 field value of a group addressed frame to: (#127, #819)

 OTAGroupAddress = (group address + EDP\_Group\_Anonymization\_Offset) mod 246, (#587)

where group address is 46 bits of the group address excluding the local/global and individual/group bits, and where EDP\_Group\_Anonymization\_Offset is the single EDP\_Group\_Anonymization\_Offset value obtained from the BPE MHA parameter set, selected for the frame as per 10.71.5.1. (#579)

***TGbi editor: Apply the following changes to the text in clause 10.71.6.1 (Address filtering)***

* Address filtering
	+ - * 1. General

Address filtering shall be applied per 10.2.8 (MAC data service) with the addressing clarifications in 10.71.5.4 (Addressing).

Within the scope of 10.7.6.1:

* a link-specific EDP\_STA\_address assigned to an affiliated STA on a given link for an identified EDP epoch is the MAC address defined as follows:
* The Local/Global bit shall be set to value 1, local address.
* The Individual/Group bit shall be set to value 0, individual address.
* EDP\_STA\_address[0:45] shall be extracted from the EDP FA block according to the link ID of the link as described in Table 10-40b (Extracting EDP\_STA\_address values from EDP FA Block), where the EDP FA block is generated for the identified EDP epoch. (#579)
* a link-specific EDP\_AP\_address assigned to an affiliated AP on a given link for an identified EDP epoch is the MAC address defined as follows
* The Local/Global bit shall be set to value 1, local address.
* The Individual/Group bit shall be set to value 0, individual address.
* EDP\_AP\_address[0:45] shall be extracted from EDP FA block as described in Table 10-40h (Extracting EDP\_AP\_address values from EDP FA Block), according to the link ID of the link, where the EDP is generated for the identified EDP epoch. (#579)
* an STA affiliated with a BPE non-AP MLD shall obtain the deanonymized group address for an identified EDP epoch from a received group address as: (#579, #819)

 Group address = (OTAGroupAddress - EDP\_Group\_Anonymization\_Offset) mod 246, (#579, #587, #819)

where OTAGroupAddress is 46 bits of the received group address excluding the local/global and individual/group bits, and the single EDP\_Group\_Anonymization\_Offset value in the BPE MHA parameter set of the identified EDP epoch as specified in 10.71.4 (Establishing BPE frame anonymization parameter sets). (#579, #587)

NOTE: If the AP MLD has BPE FA mechanisms enabled, then the EDP epoch of the non-AP MLD is also the EDP epoch of the AP MLD. (#126)

* + - * 1. Address filtering for CPE MHA only

This clause applies when the AP MLD does not have BPE FA mechanisms enabled. (#126)

For a frame received on a given setup link of the non-AP MLD: (#126)

During the margin period and the transition period of the EDP epoch of the non-AP MLD (see 10.71.2.3 (EDP epoch transition operations)), the affiliated STA of the non-AP MLD and the affiliated AP of the AP MLD of the setup link shall perform address filtering using:

* the link-specific EDP\_STA\_address of the affiliated STA for the old EDP epoch (if any), and the (fixed) address of the affiliated AP, (#579)
* the link-specific EDP\_STA\_address of the affiliated STA for the new EDP epoch, and the (fixed) address of the affiliated AP, and (#579)
* for each group to which the affiliated STA is assigned, the (fixed) group address and the (fixed) address of the affiliated AP.

After this transition period and until the margin period of the next EDP epoch of the non-AP MLD, the affiliated STA of the non-AP MLD and the affiliated AP of the AP MLD of the setup link shall perform address filtering using:

* the link-specific EDP\_STA\_address of the affiliated STA for the new EDP epoch (if any), and the (fixed) address of the affiliated AP, and (#579)
* for each group to which the affiliated STA is assigned, the (fixed) group address and the (fixed) address of the affiliated AP.
	+ - * 1. Address filtering for BPE MHA

This clause applies when the AP MLD has BPE FA mechanisms enabled. (#126)

During the dot11EDPEpochStartTimeMargin before and during the transition period (see 10.71.2.1 (General) and 10.71.2.2 (EDP group operations)) from an old EDP epoch to a new EDP epoch of the BPE non-AP MLD, the affiliated STA of the BPE non-AP MLD and the affiliated AP of the BPE AP MLD (on a setup link of the BPE non-AP MLD) shall perform address filtering using: (#356, #818)

* the link-specific EDP\_STA\_address of the affiliated STA and link-specific EDP\_AP\_ address of the affiliated AP for the old EDP epoch of the AP MLD, (#579)
* the link-specific EDP\_AP\_address and deanonymized group address (obtained from the received group address) for the old EDP epoch of the AP MLD, (#127, #579)
* the link-specific EDP\_STA\_MAC and link-specific EDP\_AP\_address for the new EDP epoch of the AP MLD, and (#579)
* and the link-specific EDP\_AP\_address and deanonymized group address (obtained from the received group address) for the new EDP epoch of the AP MLD. (#127, #579)

After this transition period, and until a dot11EDPEpochStartTimeMargin before the start of the transition period of the next EDP epoch of the BPE group, the affiliated STA of the BPE non-AP MLD and the affiliated AP of the BPE AP MLD (on a setup link of the BPE non-AP MLD) shall perform address filtering using: (#357)

* the link-specific EDP\_STA\_address and link-specific EDP\_AP\_address for the new EDP epoch of the AP MLD, and (#579-with deleted text moved to 10.71.6.1.1)
* and the link-specific EDP\_AP\_address and deanonymized group address for the new EDP epoch of the AP MLD. (#127, #579)

(#579)

* + - * 1. MAC header anonymization parameter set selection

If an individually addressed frame is received by a non-AP MLD, then the non-AP MLD shall perform packet number deanonymization (10.71.6.3 (Packet number deanonymization)) and sequence number deanonymization (10.71.6.4 (Sequence number deanonymization)) using the CPE MHA parameter set containing the link-specific EDP\_STA\_address value matching the Address 1 field in the MAC header. (#579)

An AP MLD shall perform packet number deanonymization (10.71.6.3 (Packet number deanonymization)) and sequence number deanonymization (10.71.6.4 (Sequence number deanonymization)) using the applicable CPE MHA parameter set containing the link-specific EDP\_STA\_address value matching the Address 2 field in the MAC header.

The CPE MHA parameter set so identified is the applicable CPE MHA parameter set for the received frame. (#579)

If dot11FrameAnonymizationMechanismActivated is bpe(2), then: (#126)

* If a group addressed frame is received by a BPE non-AP MLD, then the BPE non-AP MLD shall perform packet number deanonymization (10.71.6.3 (Packet number deanonymization)) and sequence number deanonymization (10.71.6.4 (Sequence number deanonymization)) using the applicable BPE MHA parameter set containing the link-specific EDP\_AP\_address value matching the Address 2 field in the MAC header of the group addressed frame.(#127, #579)
* The BPE MHA parameter set so identified is the applicable BPE MHA parameter set for the received frame. (#579)
* If a Privacy Beacon is received by a BPE non-AP MLD, then the BPE non-AP MLD shall perform timestamp deanonymization (10.71.6.5 (Timestamp deanonymization)) using the BPE MHA parameter set containing the link-specific EDP\_AP\_address value matching the Address 2 field in the MAC header of the Privacy Beacon. (#579)

***TGbi editor: Next, we address the clauses on packet number anonymization/deanonymization***

***TGbi editor: Apply the following changes to the text in clause 10.71.5.3 (Packet number anonymization)***

* Packet number anonymization

NOTE—The applicable CPE MHA parameter set is determined in 10.71.5.1 (MAC header anonymization parameter set selection). If dot11FrameAnonymizationMechanismsActivated is equal to bpe(2), then the applicable BPE MHA parameter set is determined in 10.71.5.1 (MAC header anonymization parameter set selection). (#579)

For encrypted individually addressed frames, the transmitter shall compute an over-the-air PN (OPN) value from the PN value in the CCMP header or GCMP header of the frame as follows: (#579)

 OPN = (PN + EDP\_PN\_offset) mod 248,

where EDP\_PN\_offset is the selected from the applicable CPE MHA parameter set for the frame, according to the transmitting MLD (non-AP MLD or AP MLD). (#579)

If the AP MLD has BPE FA mechanisms enabled, then for encrypted group addressed frames, the transmitter shall compute an over-the-air PN (OPN) value from the PN value in the CCMP header or GCMP header of the frame as follows: (#126, #127, #579)

 OPN = (PN + EDP\_Group\_PN\_offset) mod 248, (#579)

using the EDP\_Group\_PN\_offset value is the single EDP\_Group\_PN\_offset value in the applicable BPE MHA parameter set for the frame. (#579)

The transmitter shall transmit frames over the air using the OPN value in fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header (see 12.5.2.2 (CCMP MPDU format)) or GCMP header (see 12.5.4.2 (GCMP MPDU format)).

***TGbi editor: Apply the following changes to the text in clause 10.71.6.3 (Packet number anonymization)***

* Packet number deanonymization

NOTE—The applicable CPE MHA parameter set and applicable BPE MHA parameter set (when the AP MLD enables BPE FA mechanisms) are determined in 10.71.6.1.4 (MAC header anonymization parameter set selection). (#579)

For encrypted individually addressed frames, the receiver shall obtain the PN value from the OPN value encoded in the fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header as follows: (#579)

 PN = (OPN – EDP\_PN\_offset) mod 248,

where EDP\_PN\_offset is selected from the applicable CPE MHA parameter set for the frame according to the transmitting MLD (non-AP MLD or AP MLD). (#579)

If the AP MLD has BPE FA mechanisms enabled, then for encrypted group addressed frames, the receiver shall obtain the PN value from the OPN value encoded in the fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header as follows: (#126, #127, #579)

 PN = (OPN - EDP\_Group\_PN\_offset) mod 248, (#579)

where EDP\_Group\_PN\_offset is the single EDP\_Group\_PN\_offset in the BPE MHA parameter set selected for the frame. (#579)

The PN value (nominally the PN value assigned by the transmitter) shall replace the OPN value in subsequent processing of the frame in the receiving MLD.

***TGbi editor: Next, we address the clauses on timestamp anonymization/deanonymization***

***TGbi editor: Apply the following changes to the text in clause 10.71.5.5 (Timestamp anonymization)***

* Timestamp anonymization

NOTE—If the AP MLD has BPE FA mechanisms enabled, then the applicable BPE MHA parameter set is determined in 10.71.5.1 (MAC header anonymization parameter set selection). (#579)

For Privacy Beacon frames, the transmitter shall compute an over-the-air Timestamp (OTSF) value from the Timestamp value of the frame as follows: (#126)

 OTSF = (Timestamp + EDP\_Timestamp\_offset) mod 264,

where EDP\_Timestamp\_offset is the single EDP\_Timestamp \_ffset value in the BPE MHA parameter set selected for the frame. (#579)

The BPE AP shall transmit Privacy Beacon frames over the air using the OTSF value in the Timestamp field (see 9.3.4.4 (Privacy Beacon frame format)).

***TGbi editor: Apply the following changes to the text in clause 10.71.6.5 (Timestamp deanonymization)***

* Timestamp deanonymization

NOTE— If the AP MLD has BPE FA mechanisms enabled, then the applicable BPE MHA parameter set is determined in 10.71.6.1.4 (MAC header anonymization parameter set selection). (#579)

For Privacy Beacon frames, the receiver shall recover the Timestamp value (assigned by the transmitter) from the OTSF value encoded in the Timestamp fields as follows: (#126)

 Timestamp = (OTSF - EDP\_Timestamp\_offset) mod 264,

where EDP\_Timestamp\_offset is the single EDP\_Timestamp\_offset value in the BPE MHA parameter set selected for the frame. (#579)

The Timestamp value (nominally the Timestamp value assigned by the transmitter) shall replace the OTSF value in subsequent processing of the Privacy Beacon frame in the receiving MLD.