IEEE P802.11
Wireless LANs

|  |
| --- |
| D1.0 SN (de)anonymization |
| Date: 2025-07-08 |
| 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:

* 10.71.5.2 (Sequence number anonymization)
* 10.71.6.4 (Sequence number deanonymization)

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

Resolved CIDs (10): 248, 249, 252, 582, 584, 585, 586, 592, 817, 821

*Note: This document includes changes for CID resolutions in 25/1118: 126, 127, 579*

Revisions:

* Rev 0: Initial version of the document.

**Background**

Overview of noteworthy changes

* Updated terminology aligned with 25/1100
* Merged description of using EDP\_SN\_offset to reduce redundant text.

| **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 | **The resolution to this CID is addressed in 25/1118** **Discussion**: See 25/1118**Changes** (copied from 25/1118)For clauses outside of 10.71.5.1 and 10.71.6.1, only refer to “applicable CPE/BPE MHA parameter set” and add per-clause notes indicating that the applicable CPE/BPE MHA parameter set.is defined in 10.71.5.1 and 10.71.6.1. |
| 582 | Mark RISON | 10.71.5.2 | 87.09 | There are 4 instances of "SNS1 (Baseline)" | Delete "(Baseline)" in each | **ACCEPTED** |
| 817 | John Wullert | 10.71.5.2 | 87.13 | Listing the same equation in identical form five times when one of the parameters is different in each instance seems confusing | Show the equation one time and describe the manner in which EDP\_SN\_offset is calcuated for each of the instances (SNS1, SNS3, SNS9, SNS10 and DLSNS1/SNS11) | **Revised**:**Discussion**: Agreed in principle.**Changes**:Grouped description of SNS1 when Tx by non-AP MLD, SNS3, SNS9 and SNS10.since they are the 12-bit sequence number spaces processed by CPE MHADescription for SNS12 can stay as is since it is the only 10-bit sequence number space.Grouped description of SNS1 when Tx by AP MLD, and SNS11.since they are 12-bit sequence number spaces processed by BPE MHA. |
| 248 | Jarkko Kneckt | 10.71.5.2 | 87.19 | The SNS1 is not anonymized for the AP. AP needs to apply static SNS1 for the DL (group) frames, because legacy STAs use SNS1. | Modify the text:" transmitting MLD (non-AP MLD or AP MLD)" to:" transmitted non-AP MLD". | **Revised**:**Discussion**: Agreed in principle. Applicable in multiple places.**Changes**: See inline. |
| 249 | Jarkko Kneckt | 10.71.5.2 | 87.23 | The SNS3 has only a single SN offset, but SNS3 has TID specific time priority frames. The TID specific anonymization would need one anonymization field per TID | Please add a note to say that the same offset is used for all TIDs of the SNS3 frames. | **Rejected**Independent offsets are generated for all TIDs of SNS3 frames. See Table 10-40d. |
| 584 | Mark RISON | 10.71.5.2 | 88.15 | "Access Class Index" missing "field" | As it says in the comment | **Revised**:**Discussion**: Agreed in principle. Applicable in 2 places.**Changes**: See inline. |
| 585 | Mark RISON | 10.71.5.2 | 88.18 | "The transmitter shall transmit frames over the air using the OSN value in the Sequence Number field of the Sequence Control field (see 9.2.4.4 (Sequence Control field))." -- why is this in the middle of the subclause? Doesn't it apply to all the OSN values? | As it says in the comment | **Revised****Discussion**: Agreed. Move to end of clause). **Changes**:Move identified sentence to the end of clause 10.71.5.2 |
| 586 | Mark RISON | 10.71.5.2 | 88.22 | "DL sequence number space SNS1 (Baseline)" -- it is not clear what a DL SN space is, or how it differs from the SN space for SNS1 described at the start of the subclause | As it says in the comment | **Revised****Discussion**: Agreed in principle. Clarified as shown below.**Changes**:10.71.5.2: “transmitted by a BPE AP MLD”10.71.6.4: received by an BPE non-AP MLD” |
| 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". | **The resolution to this CID is addressed in 25/1118** Also, to indicate BPE is not enabled, used “If dot11FrameAnonymizationMechansmActivated is cpe(1)” (noting that CPE is assumed to be enabled throughout 10.71) |
| 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 | **The resolution to this CID is addressed in 25/1118** Globally replace “group frame” with “group addressed frame” |
| 821 | John Wullert | 10.71.6.4 | 91.13 | Listing the same equation four times when one of the parameters is different in each instance seems confusing | Show the equation one time and describe the manner in which EDP\_SN\_offset is calcuated for each of the instances. (SNS1, SNS3, SNS9, SNS10 and DLSNS1/SNS11) | **Revised**:**Discussion**: Agreed in principle.**Changes**:Grouped description of SNS1 when Rx by AP MLD, SNS3, SNS9 and SNS10.since they are the 12-bit sequence number spaces processed by CPE MHADescription for SNS12 can stay as is since it is the only 10-bit sequence number space.Grouped description of SNS1 when Rx by BPE non-AP MLD, and SNS11.since they are the 12-bit sequence number spaces processed by BPE MHA. |
| 592 | Mark RISON | 10.71.6.4 | 91.27 | Are we sure the mod operator is well-defined and will do what we want with a negative first operand? | As it says in the comment | **Rejected**.**Rationale**: This text is already aligned with use of mod operator used elsewhere in 802.11. |
| 252 | Jarkko Kneckt | 10.71.6.4 | 91.29 | SNS1 frame transmitted by CPE AP is not anonymized. This special case should be considered in the deanonymization description. | Please clarify that only SNS1 frame transmitted by CPE non-AP MLD or BPE MLD are deanonymizes. |  |

**Proposed spec text:**

***TGbi editor: Apply the following changes to the text in clause 10.71.5.2 (Sequence number anonymization)***

* Sequence number anonymization

NOTE 1—The sequence number spaces are defined in Table 10-5 (Transmitter sequence number spaces).

NOTE 2—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).If the MAC header of the frame includes a Sequence Control field using:

* sequence number space SNS1 when the frame is transmitted by a non-AP MLD, or (#248, #582, #817)
* sequence number space SNS3 (Time Priority Management), or (#817)
* sequence number space SNS9 (MLD Individually addressed QoS Data frame), or (#817)
* sequence number space SNS10 (MLD Individually addressed Management frame), (#817)

then the transmitter shall compute an over-the-air SN (OSN) value from the sequence number SN assigned to the MPDU as follows:

 OSN = (SN + EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is selected from the applicable CPE MAC header anonymization parameter set for the frame, according to mechanisms specific to the sequence number space. (#579)

* In the case of SNS1 when the frame is transmitted by a non-AP MLD, the transmitter shall select the single defined EDP\_SN\_offset value for SNS1. (#248, #582, #817).
* In the case of SNS3, the transmitter shall select an EDP\_SN\_offset value for SNS3 according to the combination of the transmitting MLD (non-AP MLD or AP MLD) and the TID. (#817)
* In the case of SNS9, the transmitter shall select an EDP\_SN\_offset value for SNS9 according to the combination of the transmitting MLD (non-AP MLD or AP MLD) and the TID. (#817)
* In the case of SNS10, the transmitter shall select an EDP\_SN\_offset value for SNS10 according to the transmitting MLD (non-AP MLD or AP MLD). (#817)

If the MAC header of the frame includes a Sequence Control field using sequence number space SNS12 (IQMF), then the transmitter shall compute an OSN value from the sequence number SN assigned to the MPDU (defined in Figure-9-9 (Sequence Number field format in QMFs)) as follows:

 OSN[10:11] = SN[10:11], and

 OSN[0:9] = (SN[0:9] + EDP\_SN\_offset) mod 210,

where EDP\_SN\_offset is an EDP\_SN\_offset value for SNS12 selected from the applicable CPE MAC header anonymization parameter set for the frame according to the combination of the transmitting MLD (non-AP MLD or AP MLD) and the Access Class Index field (SN[10:11]). (#584, ##ed)

 (#585)

If dot11FrameAnonymizationMechanismsActivated is equal to bpe(2), and if the MAC header of a frame transmitted by the BPE AP MLD includes a Sequence Control field using: (#126, #586)

* sequence number space SNS1 or (#582, #817)
* sequence number space SNS11 (Group addressed data), (#817)

then the transmitter shall compute an over-the-air SN (OSN) value from the sequence number SN assigned to the MPDU as follows:

 OSN = (SN + EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is selected, from the applicable BPE MAC header anonymization parameter set for the frame, according to mechanisms specific to the sequence number space. (#579)

* In the case of SNS1, the transmitter shall select the single EDP\_SN\_offset value for SNS1. (#582, #817)
* In the case of SNS11, the transmitter shall select an EDP\_SN\_offset value for SNS11 according to the transmitting MLD (non-AP MLD or AP MLD). (#817)

 (#817)

 (#585)

***TGbi editor: Apply the following changes to the text in clause 10.71.6.4 (Sequence number deanonymization)***

* Sequence number deanonymization

NOTE 1—The sequence number spaces are defined in Table 10-5 (Transmitter sequence number spaces).NOTE 2—The applicable CPE MHA parameter set is determined in 10.71.6.1.4 (MAC header anonymization parameter set selection). If dot11FrameAnonymizationMechanismsActivated is equal to bpe(2), then the applicable BPE MHA parameter set is determined in 10.71.6.1.4 (MAC header anonymization parameter set selection). (#579)

If the MAC header of the frame includes a Sequence Control field using:

* sequence number space SNS1 when the frame is received by an AP MLD, or (#248, #582, #821)
* sequence number space SNS3 (Time Priority Management), or (#821)
* sequence number space SNS9 (MLD Individually addressed QoS Data frame), or (#821)
* sequence number space SNS10 (MLD Individually addressed Management frame), (#821)

then the receiver shall compute a recovered original SN value (assigned to the MPDU by the transmitter) from the over-the-air value in the sequence number field, OSN, as follows:

 SN = (OSN - EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is selected from the applicable CPE MAC header anonymization parameter set for the frame, according to mechanisms specific to the sequence number space. (#579)

* In the case of SNS1 when the frame is received by an AP MLD, the receiver shall select the single defined EDP\_SN\_offset value for SNS1. (#248, #582, #821)
* In the case of SNS3 and SNS9, the receiver shall select an EDP\_SN\_offset value according to the combination of the transmitting MLD (non-AP MLD or AP MLD) and the TID. (#821)
* In the case of SNS10, the receiver shall select an EDP\_SN\_offset value for in Table 10-40c (Extracting EDP\_SN\_offset values for SNS1 and SNS 10 from the CPE Block) according to the transmitting MLD (non-AP MLD or AP MLD). (#817, #821)

If the MAC header of the frames includes a Sequence Control field using sequence number space SNS12 (IQMF)), then the receiver shall compute the original SN value (assigned to the MPDU by the transmitter) from the over-the-air value in the sequence number field, OSN, (defined in Figure 9-9 (Sequence Number field format in QMFs)) as follows: (#ed)

 SN[10:11] = OSN[10:11], and

 SN[0:9] = (OSN[0:9] - EDP\_SN\_offset) mod 210,

where EDP\_SN\_offset is an EDP\_SN\_offset value for SNS12 selected from the applicable CPE MAC header anonymization parameter set for the frame, according to the combination of the transmitting MLD (non-AP MLD or AP MLD) and the Access Class Index field (SN[10:11]). (#584, #ed)

If dot11FrameAnonymizationMechanismsActivated is equal to bpe(2), and if the MAC header of a frame received by a BPE non-AP MLD (#586) includes a Sequence Control field using: (#126)

* sequence number space SNS1 (#582) or
* sequence number space SNS11 (Group addressed data),

then the receiver shall compute a recovered original SN value (assigned to the MPDU by the transmitter) from the over-the-air value in the sequence number field, OSN, as follows:

 OSN = (SN + EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is selected from the applicable CPE MAC header anonymization parameter set for the frame, according to mechanisms specific to the sequence number space.

* In the case of SNS1, the receiver shall select the single EDP\_SN\_offset value for SNS1. (#248)
* In the case of SNS11, the receiver shall select an EDP\_SN\_offset value for SNS11according to the transmitting MLD (non-AP MLD or AP MLD). (#821)

 (#821)

(#585)

NOTE 2 —If dot11FrameAnonymizationMechanismsActivated is equal to bpe(2), and a frame received by a non-AP MLD includes a Sequence Control field using sequence number space SNS1, then the sequence number is not deanonymized in that frame. (#126, #252)