IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Establishing frame anonymization parameter sets text for 11bi | | | | |
| Date: 2024-09-04 | | | | |
| 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 0.4 :

* 10.71.3 (Establishing frame anonymization parameter sets),
* 10.71.4 (MAC Header anonymization and transmitting functions), and
* 10.71.5 (MAC header anonymization and receiving functions)

We propose draft specification text for TGbi draft D0.6.

Accepted/Revised CID with changes in this document:

1002, 1003, 1008, 1009, 1089, 1090, 1367, 1369, 1370, 1373, 1375, 1379, 1380, 1381, 1382, 1383, 1387, 1388

Accepted CID with changes addressed by other CID in this document:

1083, 1084, 1371, 1372, 1374, 1377, 1378, 1384, 1385, 1386, 1517

Rejected CID: 1376

Open CID: 1368

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Added details for proposal using per-link EDP\_STA\_MAC\_Seed. Changed Link ID to Link ID Info.
* Rev 2: Removed details for proposal using per-link EDP\_STA\_MAC\_Seed
* Rev 3. Adjusted to a single call to KDF. Updated to using MLD sequence number spaces. Addressed all CID in sections 10.71.3, 10.71.4 and 10.71.5.

| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| 1517 | Jarkko Kneckt | 10.71.4? | 57.57? | The offset value that is used to obfuscate MAC Headers and other parameters should be calcualted per STA in a single calculation per anonymizattion, i.e. each parameter should not have a separate offset calculation. | Include to 802.11bi offset calculation function that calculates all offsets of the anonymization event in a single calculation. | **Accepted**  Check clause and P.L  Addressed as part of CID1002. |
| 1002 | Thomas Handte | 10.71.3 | 58.11 | There is a TBD | Please describe the details. | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1002 |
| 1003 | Thomas Handte | 10.71.4 | 58.16 | There are two editor comments on this page | Either delete or fill with content | **Accepted**  Proposed resolutions  59.25 Editor’s Note: <Add text to clarify when these functions are applied>  *Addressed by 10.71.2.5 (Epoch boundaries). Editor’s note deleted.*  59.35 Editor's Note: < Retransmissions are TBD>  *Addressed by 10.71.2.1 (Introduction). Editor’s note deleted.*  60.21 Editor's Note: <Add text to definition of EDP\_STA\_MAC to clarify that (a) Local/Global bit is set to value 0, local address and (b) Individual/Group bit is set to value 0, individual address>.  *Addressed as part of response to CID1002. Editor’s note deleted.*  60.28 Editor's Note: < Add text to clarify when these functions are applied>  *Added text in 10.71.5.1 Address filtering. Editor’s note deleted.*  60.50 Editor's Note: <The first sentence can be updated to include previous EDP epoch if allowing a transition period>  *Addressed by 10.71.2.5 (Epoch boundaries). Editor’s note deleted.*.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1003 |
| 1367 | Mark RISON | 10.71.4 | 58.13 | "MAC Header" should be "MAC header" | As it says in the comment | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1367 |
| 1368 | Mark RISON | 10.71.4.1 | 58.20 | "The transmitting MLD shall select the MAC header parameter set generated for the current EDP epoch of the non-AP MLD at the time when a frame is to be transmitted for the first time (i.e., with the Retry subfield in the Frame Control field set to 0). " -- hm, but in general retries under BA do not get the Retry field set. Is the i.e. really correct? | As it says in the comment | Open. Currently obtaining clarification. |
| 1090 | Julien Sevin | 10.71.4.1 | 58.21 | Please indicate and specify that the MAC header anonymization includes the Address 1 (on the downlink) and Address 2 (on the uplink) | Indicate and specify the anonymization of Address 1 (on the downlink) and Address 2 (on the uplink) | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1090 |
| 1369 | Mark RISON | 10.71.4.1 | 58.27 | "changes shown in the subsequent subclauses of this subclause" -- this subclause has no subclauses | As it says in the comment | **Revised**  Agree in principle:  Aligned with phrasing in 10.71.5.1 (Address filtering)  Instruction to the editor: apply changes referenced with tag: #1369 |
| 1089 | Julien Sevin | 10.71.4.2 | 58.31 | Althought the Sequence Number field is included in the Sequence Control field of the MAC Header, it is also addressed in the section 10.71.4.1 MAC header anonymization parameter set selection | Please clarify whether the Sequence Number anomymization is included in MAC header anonymization set selection or not. | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1389 |
| 1370 | Mark RISON | 10.71.4.2 | 58.34 | "from the value in the Sequence Number subfield " -- this is somehow trying to refer to the value in the field were we not doing anonymisation, but this is somewhat confusing | Maybe "from the sequence number SN assigned to the MPDU"? | **Accepted**  Applied the requested change  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1370 |
| 1083 | Julien Sevin | 10.71.4.2 | 58.37 | How the EDP\_SN\_offset is generated ? | Specify how the "EDP\_SN\_offset is generated | **Accepted**  Addressed as part of response to CID1002 |
| 1371 | Mark RISON | 10.71.4.2 | 58.39 | "the offset value generated for the sequence number space of the transmitting MLD (non-AP MLD or AP MLD) used in the frame " -- MLDs are not used in the frame | Reword | **Accepted**  Addressed as part of response to CID1002. |
| 1372 | Mark RISON | 10.71.4.2 | 58.42 | ", and "mod 212" denotes reducing the result modulo 212 to a value in the range 0 to (212-1)" -- mod is basic maths, which we don't waffle on about elsewhere. Also at 59.63 | Delete the cited text | **Accepted**  Addressed as response to CID 1387 |
| 1387 | Mark RISON | - | - | Look, just remove all those locations where we spoon-feed what "mod" means | As it says in the comment | **Accepted**  These locations are in 10.71.4.2, 10.71.4.3, 10.71.5.3 and 10.71.5.4.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1387 |
| 1373 | Mark RISON | 10.71.4.2 | 58.45 | "Sequence Number subfield" -- we don't refer to things as subfields anymore -- it's fields everywhere | Fix throughout the draft | **Accepted**  Changed “subfield” to “field” throughout the document.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1373 |
| 1084 | Julien Sevin | 10.71.4.3 | 58.55 | How the EDP\_PN\_offset is generated ? | Specify how the "EDP\_PN\_offset is generated | **Accepted**  Addressed as part of the response to CID1002. |
| 1374 | Mark RISON | 10.71.4.3 | 0.00 | Same comments as for 10.71.4.2 | Fix in the same way | **Accepted**  Addressed as response to CID 1387 and part of responses to CID 1002 |
| 1375 | Mark RISON | 10.71.4.3 | 58.62 | "The transmitter shall transmit frames over the air using the OPN value encoded in fields PN0, PN1, PN2," -- it is not clear that there is any encoding here | As it says in the comment | **Accepted**.  Removed word “encoded”.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1375 |
| 1376 | Mark RISON | 10.71.4.3 | 58.51 | "For encrypted 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:" -- don't we also need to anonymise the PN in the MME etc.? | As it says in the comment | **Reject??**  CPE addressed only privacy of individual non-AP MLDs – CPE does not address not privacy of groups of non-AP MLDs nor the BSS (although BPE would).  Consequently, MAC header anonymity is applied only to individually addressed frames.  The receive sequence counters (RSCs e.g., IPN, BIPN, etc.) used in beacons and group addressed frames do not need anonymising for CPE. |
| 1377 | Mark RISON | 10.71.5.1 | 59.27 | "MAC header parameter set " -- not clear what this is | Clarify | **Accepted**  Addressed as part of the responses to CID1089 and CID 1090. |
| 1378 | Mark RISON | 10.71.5.1 | 59.27 | "the EDP\_STA\_MAC value" -- I have no idea what this is | As it says in the comment | **Accepted**  Addressed as part of the response to CID1002. |
| 1379 | Mark RISON | 10.71.5.2 | 59.46 | "the A1 field and A2 field of the (per-link) Block Ack" -- the what? Is this the Block Ack frame? Similarly next bullet | As it says in the comment | **Accepted**  Replaced “Block Ack” with “Block Ack frame” throughout document.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1379 |
| 1380 | Mark RISON | 10.71.5.2 | 59.46 | "The values in the A1 field and A2 field of the (per-link) Block Ack shall be the values in the A2 field and A1 field (respectively) of the corresponding A-MPDU. " -- not totally sure what this is all referring to, but in any case I think the fields are called Address 1 and Address 2 (I think A1 and A2 is an S1G-only thing). Similarly "SN field" in next bullet | As it says in the comment | **Accepted**  Replaced “A1” with “Address 1”. Replaced “A2” with “Address 2”.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1380 |
| 1381 | Mark RISON | 10.71.5.2 | 59.46 | "values in the A2 field and A1 field (respectively) of the corresponding A-MPDU. " -- A-MPDUs don't have address fields, only the MPDUs they contain do. Similarly in next bullet | As it says in the comment | **Accepted**  Refer to “MPDUs of the corresponding A-MPDU”.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1381 |
| 1008 | Chaoming Luo | 10.71.5.3 | 59.60 | The algorithm may result in a negative number. | Change to: PN = (2^48 + OPN - EDP\_PN\_offset) mod 2^48 | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1008 |
| 1382 | Mark RISON | 10.71.5.3 | 59.56 | "in the PN0" should be "in fields PN0" | As it says in the comment | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1382 |
| 1383 | Mark RISON | 10.71.5.3 | 59.60 | In equations should use minuses not hyphens for subtraction | As it says in the comment | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1383 |
| 1384 | Mark RISON | 10.71.5.3 | 59.60 | What if for any reason OPN is less than EDP\_PN\_offset? Is the mathematical mod behaviour well-defined and will it produce the desired outcome? | As it says in the comment | **Accepted**  Addressed as part of response to CID 1008 |
| 1009 | Chaoming Luo | 10.71.5.4 | 60.10 | The algorithm may result in a negative number. | Change to: SN = (2^12 + OSN - EDP\_SN\_offset) mod 2^12 | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1009 |
| 1385 | Mark RISON | 10.71.5.4 | 0.00 | More incorrect references to an "SN" field | As it says in the comment | **Accepted**  Replaced “SN field” with “sequence number field” throughout sections 10.71.3 and 10.71.4. In part addressed by changes in response to CID 1002.  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1385 |
| 1386 | Mark RISON | 10.71.5.4 | 60.10 | What if SN is less than EDP\_SN\_offset? This could easily happen. Is mod defined correctly for a negative first operand for this to work? | As it says in the comment | **Accepted**  Addressed as part of response to CID 1009 |
| 1388 | Mark RISON | 10.71.5.4 | 60.08 | "the OSN value in the SN field " is weird | Maybe "the value in the Sequence Number field, OSN",? | **Accepted**  Document 1394r3 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1388 |

**Background**

SN anonymization and SN deanonymization are applied to sequence number spaces SNS9, SNS10 and SNS12.

NOTE- The sequence number spaces SNS1, SNS8 and SNS11 have a single counter per AP MLD, so SN anonymization is not applied to these sequence number spaces for CPE. Sequence number space SNS5 does not have a counter, and sequence number spaces SNS2, SNS3, SNS4, SNS6 and SNS7 are not used by MLD, so SN anonymization is not applied to these sequence number spaces.

Each of SNS9 and SNS10 use set of independent 12-bit counters; one for each combination of the transmitter (non-AP MLD or AP MLD – two possibilities) and TID (16 possibilities).

SNS12 use set of independent 10-bit counters, where the SN comprises a 10-bit counter in SN[0:9] and an Access Class Index ACI in SN[10:11]. There is a 10-bit counter for each combination of the transmitter (non-AP MLD or AP MLD– two (2) possibilities) and ACI (four (4) possibilities).

Each of the counters for SNS9, SNS10 and SNS12 has an independent EDP\_SN\_offset.

If parameters for AID anonymization are generated in the same KDF call as the MAC header anonymization parameters, then the text can be easily updated.

**Proposed spec text:**

***TGbi editor: Apply the following changes to 10.71.3 (Establishing frame anonymization parameter sets). The baseline for this text is Draft P802.11bi\_D0.5.***

* Establishing frame anonymization parameter sets

This subclause describes how an AP MLD and associated non-AP MLD establish the FA parameter set for each EDP epoch for the non-AP MLD.

The non-AP MLD and AP MLD establish(#Ed) the EDP epochs used for frame anonymization as described in 10.71.2 (EDP epoch operation)(#Ed).

The EDP CPE frame anonymization parameters for a given EDP epoch shall be generated (by the CPE non-AP MLD and CPE AP MLD) by computing a single pseudorandom EDP FA block which is partitioned into the set of EDP CPE frame anonymization parameters according to Table 10-a (EDP FA block bit positions used for EDP\_PN\_offset values), Table 10-b (EDP FA block bit positions used for EDP\_STA\_MAC values), Table 10-c (EDP FA block bit positions used for SNS9 EDP\_SN\_offset), Table 10-d (EDP FA block bit positions used for SNS10 EDP\_SN\_offset) and Table 10-e EDP FA block bit positions used for SNS12 EDP\_SN\_offset).

For a given EDP epoch, the EDP FA block shall be generated as:

EDP CPE FA block =KDF-*Hash-Length*( KDK, “EDP CPE frame anonymization”, GTn)

where:

EDP FA block is the block of bits which is partitioned into the sets of all possible values for each EDP frame anonymization parameter

KDF-*Hash-Length* is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors))

KDK is the Key Derivation Key

GTn is the reference start time of the EDP Epoch (see 9.4.2.337 (Enhanced Data Privacy (EDP) element) )

*Length* is the total number of bits to derive. A total of 1634-bits are derived for a EDP FA block.(#1002)

Table 10-a of EDP FA block bit positions used for EDP\_PN\_offset values (#1002)

|  |  |
| --- | --- |
| Transmitter | Bits positions |
| non-AP MLD | 0:47 |
| AP MLD | 48:95 |

Within a given EDP epoch, the EDP\_STA\_MAC for a give Link ID shall be the MAC address defined as follows:

* The Local/Global bit shall be set to value 0, local address,
* The Individual/Group bit is set to value 0, individual address,
* The remaining bits are extracted from EDP FA block according to Table 10-b (EDP FA block bit positions used for EDP\_STA\_MAC values).

Table 10-b EDP FA block bit positions used for EDP\_STA\_MAC values (#1002)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Link ID (hex) | Bits positions | Link ID (hex) | Bits positions | Link ID (hex) | Bits positions |
| 0 | 96:141 | 5 | 326:371 | A | 556:601 |
| 1 | 142:187 | 6 | 372:417 | B | 602:647 |
| 2 | 188:233 | 7 | 418:463 | C | 648:693 |
| 3 | 234:279 | 8 | 464:509 | D | 694:739 |
| 4 | 280:325 | 9 | 510:555 | E | 740:785 |

Table 10-c EDP FA block bit positions used for SNS9 EDP\_SN\_offset (#1002)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Transmitter is a non-AP MLD | | | | Transmitter is an AP MLD | | | |
| TID (hex) | Bits positions | TID (hex) | Bits positions | TID (hex) | Bits positions | TID (hex) | Bits positions |
| 0 | 786:797 | 8 | 882:893 | 0 | 978:989 | 8 | 1074:1085 |
| 1 | 798:809 | 9 | 894:905 | 1 | 990:1001 | 9 | 1086:1097 |
| 2 | 810:821 | A | 906:917 | 2 | 1002:1013 | A | 1098:1109 |
| 3 | 822:833 | B | 918:929 | 3 | 1014:1025 | B | 1110:1121 |
| 4 | 834:845 | C | 930:941 | 4 | 1026:1037 | C | 1122:1133 |
| 5 | 846:857 | D | 942:953 | 5 | 1038:1049 | D | 1134:1145 |
| 6 | 858:869 | E | 954:965 | 6 | 1050:1061 | E | 1146:1157 |
| 7 | 870:881 | F | 966:977 | 7 | 1062:1073 | F | 1158:1169 |

Table 10-d EDP FA block bit positions used for SNS10 EDP\_SN\_offset (#1002)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Transmitter is a non-AP MLD | | | | Transmitter is an AP MLD | | | |
| TID (hex) | Bits positions | TID (hex) | Bits positions | TID (hex) | Bits positions | TID (hex) | Bits positions |
| 0 | 1170:1181 | 8 | 1266:1277 | 0 | 1362:1373 | 8 | 1458:1469 |
| 1 | 1182:1193 | 9 | 1278:1289 | 1 | 1374:1385 | 9 | 1470:1481 |
| 2 | 1194:1205 | A | 1290:1301 | 2 | 1386:1397 | A | 1482:1493 |
| 3 | 1206:1217 | B | 1302:1313 | 3 | 1398:1409 | B | 1494:1505 |
| 4 | 1218:1229 | C | 1314:1325 | 4 | 1410:1421 | C | 1506:1517 |
| 5 | 1230:1241 | D | 1326:1337 | 5 | 1422:1433 | D | 1518:1529 |
| 6 | 1242:1253 | E | 1338:1349 | 6 | 1434:1445 | E | 1530:1541 |
| 7 | 1254:1265 | F | 1350:1361 | 7 | 1446:1457 | F | 1542:1553 |

Table 10-e EDP FA block bit positions used for SNS12 EDP\_SN\_offset (#1002)

|  |  |  |  |
| --- | --- | --- | --- |
| Transmitter is a non-AP MLD | | Transmitter is an AP MLD | |
| ACI | Bits positions | ACI | Bits positions |
| 0 | 1554:1563 | 0 | 1594:1603 |
| 1 | 1564:1573 | 1 | 1604:1613 |
| 2 | 1574:1583 | 2 | 1614:1623 |
| 3 | 1584:1593 | 3 | 1624:1633 |

***TGbi editor: Apply the following changes to 10.71.4 (MAC Header anonymization and transmitting functions). The baseline for this text is Draft P802.11bi\_D0.5.***

* MAC header(#1367) anonymization and transmitting functions

(#1003)

* MAC header anonymization parameter set selection

A MAC header parameter set for given ED epoch comprises a set of values for EDP\_SN\_offset, EDP\_PN\_offset and EDP\_STA\_MAC (defined in 10.71.3 (Establishing frame anonymization parameter sets) which are used to anonymize 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.(#1090,#1089)

The transmitting MLD shall select the MAC header parameter set generated for the current EDP epoch of the non-AP MLD at the time when a frame is to be transmitted for the first time (i.e., with the Retry field(#1373) in the Frame Control field set to 0). Retransmissions are addressed in 10.71.2.1 (Introduction).(#1003)

(#1003)The transmitting MLD shall perform sequence number deanonymization (10.71.4.2 (Sequence number anonymization), packet number anonymization (10.71.4.3 (Packet number deanonymization)) and address anonymization (10.71.4.4 (Addressing))(#1369) using this MAC header anonymization parameter set.

* Sequence number anonymization

If the MAC header of the frame includes a Sequence Control field using sequence number space SNS9 (MLD Individually addressed QoS Data frame) or sequence number space SNS10 (MLD Individually addressed Management frame) (see Table 10-5 (Transmitter sequence number spaces)), then the transmitter shall compute an over-the-air SN (OSN) value from the sequence number SN assigned to the MPDU (#1370) as follows:

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

where EDP\_SN\_offset is the offset value in the MAC header anonymization parameter set selected for the frame as specified in 10.71.3 (Establishing frame anonymization parameter sets), (#1002)generated according to the combination of the(#1002) sequence number space (SNS9 or SNS10)(#1002) the transmitting MLD (non-AP MLD or AP MLD) and the TID(#1002,#1387).

If the MAC header of the frame includes a Sequence Control field using sequence number space SNS12 (IQMF) (see Table 10-5 (Transmitter sequence number spaces)), 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 the offset value in the MAC header anonymization parameter set selected for the frame as specified in 10.71.3 (Establishing frame anonymization parameter sets), generated according to the combination of the sequence number space (SNS12), the transmitting MLD (non-AP MLD or AP MLD) and the Access Class Index (SN[10:11]).(#1002)

The transmitter shall transmit frames over the air using the OSN value in the Sequence Number field(#1373) of the Sequence Control field (see 9.2.4.4 (Sequence Control field)).

* Packet number anonymization

For encrypted 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:

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

where EDP\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the MAC header anonymization parameter set selected for the frame (#1387).

The transmitter shall transmit frames over the air using the OPN value (#1375) 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)).

* Addressing

MLD addressing shall be applied per 35.3.2 (MLD addressing) with the following addressing clarification:

* The MAC address of a STA affiliated with a non-AP MLD corresponding to a link is the EDP\_STA\_MAC value assigned to that link in the selected MAC header anonymization parameter set.

(#1002,#1003)

***TGbi editor: Apply the following changes to 10.71.5 (MAC Header deanonymization and transmitting functions). The baseline for this text is Draft P802.11bi\_D0.5***

* MAC header anonymization and receiving functions

(#1003)

* Address filtering

Address filtering shall be applied per 10.2.8 (MAC data service) with the addressing clarifications in 10.71.4.4 (Addressing). During the transition period (see 10.71.2.1 (Introduction) and 10.71.2.5 (Epoch boundaries)) from an old EDP epoch to a new EDP epoch of the CPE non-AP MLD, the affiliated STA of the CPE non-AP MLD and the affiliated AP of the CPE AP MLD (on a setup link of the CPE non-AP MLD) shall perform address filtering using the EDP\_STA\_MAC address from the MAC header anonymization parameters (if any) of the old EDP epoch and the EDP\_STA\_MAC address from the MAC header anonymization parameters (if any) of the new EDP epoch. After this transition period, and until the start of the transition period of the next EDP epoch of the CPE non-AP MLD, the affiliated STA of the CPE non-AP MLD and the affiliated AP of the CPE AP MLD (on a setup link of the CPE non-AP MLD) shall perform address filtering using the EDP\_STA\_MAC address from the MAC header anonymization parameters of the new EDP epoch. (#1003)

A receiving STA affiliated with a non-AP MLD shall perform packet number deanonymization (10.71.5.3 (Packet number deanonymization)) and sequence number deanonymization (10.71.5.4 (Sequence number deanonymization)) using the MAC header parameter set (see 10.71.4.1 (MAC header anonymization parameter set selection))(#1090,#1089) containing the EDP\_STA\_MAC value matching the Address 1 field in the MAC header.

A receiving AP affiliated with a AP MLD shall perform packet number deanonymization (10.71.5.3 (Packet number deanonymization)) and sequence number deanonymization (10.71.5.4 (Sequence number deanonymization)) using the MAC header anonymization parameter set containing the EDP\_STA\_MAC value matching the Address 2 field in the MAC header.

* (#1003)Block ack scoreboarding

Block ack scoreboarding shall be applied per 35.3.8 (Block ack procedures in MLO), with the following clarifications:

* The values in the Address 1(#1380) field and Address 2(#1380) field of the (per-link) Block Ack frame (#1379) shall be the values in the Address 2(#1380) field and Address 1(#1380) field (respectively) of the MPDUs of the (#1381)corresponding A-MPDU.
* The (per-link) Block Ack frame (#1379) shall report the OSN values received in the sequence number(#1385) field of the MPDU header within the MPDUs of the corresponding (#1381) A-MPDU (rather than reporting the SN values recovered after SN deanonymization).
* Packet number deanonymization

For encrypted frames, the receiver shall recover the original PN value (assigned by the transmitter) from the OPN value encoded in the fields (#1382) PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header as follows:

PN = (248 + (#1008)OPN −(#1383) EDP\_PN\_offset) mod 248,

where EDP\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the MAC header anonymization parameter set selected for the frame(#1387).

The recovered original PN value shall replace the OPN value in subsequent processing of the frame in the receiving MLD.

* Sequence number deanonymization

For frames using sequence number space SNS9 (MLD Individually addressed QoS Data frame) or sequence number space SNS10 (MLD Individually addressed Management frame) (see Table 10-5 (Transmitter sequence number spaces))(#1002), the receiver shall compute the original SN value from the value in the sequence number field, OSN, (#1388)as follows:

SN = (212 + (#1009)OSN −(#1383) EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is the offset value in the MAC header anonymization parameter set selected for the frame as specified in 10.71.3 (Establishing frame anonymization parameter sets), (#1002)generated according to the combination of the(#1002) sequence number space (SNS9 or SNS10),(#1002) of the transmitting MLD (non-AP MLD or AP MLD) and the TID(#1002)(#1387).

For frames using sequence number space SNS12 (IQMF) (see Table 10-5 (Transmitter sequence number spaces)), then the transmitter shall compute the original SN value from the value in the sequence number field, OSN, (defined in Figure 9-9 (Sequence Number field format in QMFs)) as follows:

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

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

where EDP\_SN\_offset is the offset value in the MAC header anonymization parameter set selected for the frame as specified in 10.71.3 (Establishing frame anonymization parameter sets), generated according to the combination of the sequence number space (SNS12), the transmitting MLD (non-AP MLD or AP MLD) and the Access Class Index (OSN[10:11]).(#1002)

The recovered original SN value shall replace the OSN value in subsequent processing of the frame in the receiving MLD.