IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 CRs for 10.71.4 |
| Date: 2025-07-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco Systems |  |  | jerhenry@cisco.com |
| Domenico Ficara | Cisco Systems |  |  | dficara@cisco.com |
| Ugo Campiglio | Cisco Systems |  |  | ucampigl@cisco.com |
| Javier Contreras | Cisco Systems |  |  | jacontre@cisco.com |

Abstract

This submission proposes resolutions for the following CIDs:

569, 154, 575, 572, 576, 577, 578.

Revisions:

* Rev 0: Initial version of the document.

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 TGbi D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D1.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 569 | 10.71.4 | 0.00 | This subclause is missing all the stuff at the start of 10.71.3 that introduces FA blocks etc. | Align the two subclauses (even better, put the common stuff in a common subclause, and only have CPE- and BPE-specific stuff in their subclauses) | Revised Add intro text to align 10.71.4 to 10.71.3. TGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 569 |
| 154 | 10.71.4 | 84.54 | If you expand "EDP BPE" you have "Enhanced Data Privacy BSS Privacy Enhancements". I think some of this terminology can be optimised. | Replace "EDP BPE" with "BPE" and also at P84L55, P84L56, P84L62 (x2), P85L16, P85L17 and P88L65. | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 154 |
| 575 | 10.71.4 | 85.02 | Length is undefined | Define it (as for CPE) | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 575 |
| 572 | 10.71.4 | 85.14 | "The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp" -- are these field names? | As "fields" | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 572 |
| 576 | 10.71.4 | 85.16 | "Tables" should be "tables" | As it says in the comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 576 |
| 577 | 10.71.4 | 86.01 | "The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymizes" bad grammar | "The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymize" | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 577 |
| 578 | 10.71.4 | 86.02 | "except the Group/Individual bit shall" should be "except that the Group/Individual bit shall" | As it says in the comment | AcceptedTGbi editor to make the changes shown in the latest version of 11-25/1107 under all headings that include CID 578 |

**Discussion**

Clause 10.71.4 (draft 1.2) before the CIDs:

**10.71.4 Establishing BPE frame anonymization parameter sets**

All associated BPE non-AP MLDs and the BPE AP MLD shall generate EDP BPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom EDP BPE FA block which is partitioned into a set of EDP BP frame anonymization parameters according to the following tables.

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

EDP\_BPE\_FA\_block = KDF-*Hash*-*Length* (PGTK, "EDP BPE frame anonymization", n),

where

 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))

 PGTK is the Privacy Group Transient Key

 n is the current number of the EDP epoch in the EDP epoch sequence as

 defined in 10.71.2.4 (EDP Epoch Start Time Computation)

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp together with the anonymized BPE AP link addresses are created from the EDP\_BPE\_FA\_block. The offsets and the AP link addresses have static assignments within the EDP\_BPE\_FA\_block as shown in the Tables below.

**Extracting EDP\_PN\_offset values from EDP FA Block**

|  |  |
| --- | --- |
| **48-bit sub-block of EDP FA block** | **Value** |
| 0:47 | EDP\_Group\_PN\_offset |

**Extracting EDP\_AP\_address values from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:45]** | **Sub-block** **Bits [46:47]** |
| 48:95 | EDP\_AP\_address [0:45] for Link ID 0  | Reserved |
| 96:143 | EDP\_AP\_address [0:45] for Link ID 1 | Reserved |
| 144:191 | EDP\_AP\_address [0:45] for Link ID 2 | Reserved |
| 192:239 | EDP\_AP\_address [0:45] for Link ID 3 | Reserved |
| 240:287 | EDP\_AP\_address [0:45] for Link ID 4 | Reserved |
| 288:335 | EDP\_AP\_address [0:45] for Link ID 5 | Reserved |
| 336:383 | EDP\_AP\_address [0:45] for Link ID 6 | Reserved |
| 384:431 | EDP\_AP\_address [0:45] for Link ID 7 | Reserved |
| 432:479 | EDP\_AP\_address [0:45] for Link ID 8 | Reserved |
| 480:527 | EDP\_AP\_address [0:45] for Link ID 9 | Reserved |
| 528:575 | EDP\_AP\_address [0:45] for Link ID 10 | Reserved |
| 576:623 | EDP\_AP\_address [0:45] for Link ID 11 | Reserved |
| 624:671 | EDP\_AP\_address [0:45] for Link ID 12 | Reserved |
| 672:719 | EDP\_AP\_address [0:45] for Link ID 13 | Reserved |
| 720:767 | EDP\_AP\_address [0:45] for Link ID 14 | Reserved |

The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymizes the group addresses as described in 10.71.5.4 (Addressing). All bits of the group address are anonymized, except the Group/Individual bit shall be set to 1 and the Local/Global bit value shall not be modified.

**Extracting EDP\_Group\_Anonymization\_Offset from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:45]** | **Sub-block Bits [46:47]** |
| 768:815 | EDP\_Group\_Anonymization\_Offset | Reserved |

**Extracting EDP\_SN\_offset values for SN1 and SNS 11 from EDP FA Block**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:11]** | **Sub-block Bits [12:23]** | **Sub-block Bits [24:35]** | **Sub-block Bits [36:47]** |
|  | EDP\_SN\_offset values for SNS1 | EDP\_SN\_offset values for SNS11 |  |  |
| 816:863 | Reserved  | Value for frames transmitted by AP MLD | Reserved  | Value for frames transmitted by AP MLD |

**Extracting Timestamp Offset from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:63]** | **Sub-block Bits [64:95]** |
| 864:959 | Timestamp offset  | Reserved |

**Discussion**

CID 569:

Revised

This subclause describes how an AP MLD and associated non-AP MLD establish the BPE FA parameter set for each EDP epoch for the BPE AP MLD and the non-AP MLD. The creation of the CPE FA parameter sets is described in 10.71.3 (Establishing frame anonymization parameter sets).

The non-AP MLD and AP MLD establish the EDP epochs used for frame anonymization as described in 10.71.8 (BSS Privacy Operations).

All associated BPE non-AP MLDs and the BPE AP MLD shall generate EDP BPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom EDP BPE FA block which is partitioned into a set of EDP BP frame anonymization parameters according to the following tables.

CID 154:

Accepted

11-25/1008 established that BPE was an EDP feature, therefore the repeat is not needed

Editor, please aslore place draft-wise EDP BPE and BPE EDP with BPE

**Establishing BPE frame anonymization parameter sets**

This subclause describes how an AP MLD and associated non-AP MLD establish the BPE FA parameter set for each EDP epoch for the BPE AP MLD and the non-AP MLD. The creation of the CPE FA parameter sets is described in 10.71.3 (Establishing frame anonymization parameter sets).

The non-AP MLD and AP MLD establish the EDP epochs used for frame anonymization as described in 10.71.8 (BSS Privacy Operations).

All associated BPE non-AP MLDs and the BPE AP MLD shall generate ~~EDP~~ BPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom ~~EDP~~ BPE FA block which is partitioned into a set of ~~EDP~~ BPE frame anonymization parameters according to the following tables.

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

~~EDP\_~~BPE\_FA\_block = KDF-*Hash*-*Length* (PGTK, "~~EDP~~ BPE frame anonymization", n),

where

 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))

 PGTK is the Privacy Group Transient Key

 n is the current number of the EDP epoch in the EDP epoch sequence as

 defined in 10.71.2.4 (EDP Epoch Start Time Computation)

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp together with the anonymized BPE AP link addresses are created from the ~~EDP\_~~BPE\_FA\_block. The offsets and the AP link addresses have static assignments within the ~~EDP\_~~BPE\_FA\_block as shown in the Tables below.

CID 575

Revised

 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))

 PGTK is the Privacy Group Transient Key

 n is the current number of the EDP epoch in the EDP epoch sequence as

 defined in 10.71.2.4 (EDP Epoch Start Time Computation)

 *Length* is the total number of bits to derive. A total of 1728 bits are derived for a

 BPE FA block.

CID 572

Revised

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp fields together with the anonymized BPE AP link addresses are created from the BPE\_FA\_block. The offsets and the AP link addresses have static assignments within the BPE\_FA\_block as shown in the Tables below.

CID 576

Accepted

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp fields together with the anonymized BPE AP link addresses are created from the BPE\_FA\_block. The offsets and the AP link addresses have static assignments within the BPE\_FA\_block as shown in the ~~T~~tables below.

CID 577

Accepted

The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymize~~s~~ the group addresses as described in 10.71.5.4 (Addressing). All bits of the group address are anonymized, except the Group/Individual bit shall be set to 1 and the Local/Global bit value shall not be modified.

CID 578

The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymize the group addresses as described in 10.71.5.4 (Addressing). All bits of the group address are anonymized, except that the Group/Individual bit shall be set to 1 and the Local/Global bit value shall not be modified.

*TGbi editor: Modify clause 10.71.4 as follows (track change on):*

**10.71.4 Establishing BPE frame anonymization parameter sets**

This subclause describes how an AP MLD and associated non-AP MLD establish the BPE FA parameter set for each EDP epoch for the BPE AP MLD and the non-AP MLD. The creation of the CPE FA parameter sets is described in 10.71.3 (Establishing frame anonymization parameter sets).

The non-AP MLD and AP MLD establish the EDP epochs used for frame anonymization as described in 10.71.8 (BSS Privacy Operations). (#569)

All associated BPE non-AP MLDs and the BPE AP MLD shall generate (#154) BPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom (#154) BPE FA block which is partitioned into a set of EDP BP frame anonymization parameters according to the following tables.

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

(#154)BPE\_FA\_block = KDF-*Hash*-*Length* (PGTK, "(#154)BPE frame anonymization", n),

where

 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))

 PGTK is the Privacy Group Transient Key

 n is the current number of the EDP epoch in the EDP epoch sequence as

 defined in 10.71.2.4 (EDP Epoch Start Time Computation)

 *Length* is the total number of bits to derive. A total of 1728 bits are derived for a

 BPE FA block. (#575)

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp fields (#572) together with the anonymized BPE AP link addresses are created from the (#154)BPE\_FA\_block. The offsets and the AP link addresses have static assignments within the (#154)BPE\_FA\_block as shown in the (#576)tables below.

**Extracting EDP\_PN\_offset values from EDP FA Block**

|  |  |
| --- | --- |
| **48-bit sub-block of EDP FA block** | **Value** |
| 0:47 | EDP\_Group\_PN\_offset |

**Extracting EDP\_AP\_address values from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:45]** | **Sub-block** **Bits [46:47]** |
| 48:95 | EDP\_AP\_address [0:45] for Link ID 0  | Reserved |
| 96:143 | EDP\_AP\_address [0:45] for Link ID 1 | Reserved |
| 144:191 | EDP\_AP\_address [0:45] for Link ID 2 | Reserved |
| 192:239 | EDP\_AP\_address [0:45] for Link ID 3 | Reserved |
| 240:287 | EDP\_AP\_address [0:45] for Link ID 4 | Reserved |
| 288:335 | EDP\_AP\_address [0:45] for Link ID 5 | Reserved |
| 336:383 | EDP\_AP\_address [0:45] for Link ID 6 | Reserved |
| 384:431 | EDP\_AP\_address [0:45] for Link ID 7 | Reserved |
| 432:479 | EDP\_AP\_address [0:45] for Link ID 8 | Reserved |
| 480:527 | EDP\_AP\_address [0:45] for Link ID 9 | Reserved |
| 528:575 | EDP\_AP\_address [0:45] for Link ID 10 | Reserved |
| 576:623 | EDP\_AP\_address [0:45] for Link ID 11 | Reserved |
| 624:671 | EDP\_AP\_address [0:45] for Link ID 12 | Reserved |
| 672:719 | EDP\_AP\_address [0:45] for Link ID 13 | Reserved |
| 720:767 | EDP\_AP\_address [0:45] for Link ID 14 | Reserved |

The 46 bits of the EDP\_Group\_Anonymization\_Offset anonymize(#577) the group addresses as described in 10.71.5.4 (Addressing). All bits of the group address are anonymized, except that (#578) the Group/Individual bit shall be set to 1 and the Local/Global bit value shall not be modified.

**Extracting EDP\_Group\_Anonymization\_Offset from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:45]** | **Sub-block Bits [46:47]** |
| 768:815 | EDP\_Group\_Anonymization\_Offset | Reserved |

**Extracting EDP\_SN\_offset values for SN1 and SNS 11 from EDP FA Block**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:11]** | **Sub-block Bits [12:23]** | **Sub-block Bits [24:35]** | **Sub-block Bits [36:47]** |
|  | EDP\_SN\_offset values for SNS1 | EDP\_SN\_offset values for SNS11 |  |  |
| 816:863 | Reserved  | Value for frames transmitted by AP MLD | Reserved  | Value for frames transmitted by AP MLD |

**Extracting Timestamp Offset from EDP FA Block**

|  |  |  |
| --- | --- | --- |
| **48-bit sub-block of EDP FA block** | **Sub-block Bits [0:63]** | **Sub-block Bits [64:95]** |
| 864:959 | Timestamp offset  | Reserved |

*TGbi editor: please also replace draft-wised EDP BPE with BPE, and BPE EDP with BPE.*