IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for EDP Epoch Start Time | | | | |
| Date: 2025-07-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Stéphane Baron | Canon Research centre France |  |  | Stephane.baron@crf.canon.fr |
| Julien Sevin |  |  | Julien.sevin@crf.canon.fr |
| Patrice Nezou |  |  | Patrice.nezou@crf.canon.fr |
|  |  |  |  |
|  |  |  |  |  |

Abstract

Abstract

This submission proposes resolutions and discussions for 23 CIDs number:

77, 79, 82, 83, 84, 85, 86, 89,108,109,

120,150,197, 345, 437,554,854,870,954, 1051,

1053, 1054, 1058

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: CID 996 transferred to document 1112, CIDs 77, 79, 82, 83 transferred from Doc 1113.
  + Resolution of CID 77, 79, 83, 1054, and 554 changed.
  + Resolution of CIDs 345, and 994 changed.

1. Introduction

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 Draft. The introduction and the explanation of the proposed changes are not part of the adopted material.

The baseline for this text is 802.11 REVme D7.0, and 802.11 TGbi draft D1.2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Clause | Pg, Ln | Comment | Proposed Change | Resolution |
| 78 | Graham Smith | 10.71.2.4 | 79, 57 | "Upon reception on a link of an EDP Epoch Request frame.." Any other way of receiving the fame? Delete "on a link" | At cited location delete "on a link" | Revised  The sentence has been reworded, and reception of the frame is not mentioned any more, see also resolution of CID 554  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 554 |
| 79 | Graham Smith | 10.71.2.4 | 79, 59 | "...the AP may send in response to the requesting non-AP STA," Long winded. Also is it really a "may". If the STA sends the request, is not the AP obliged to respond? | Change cited text to "an AP may respond with" ALSO consider alternative "an AP responds with" | Revised  The sentence has been reworded, and reception of the frame is not mentioned any more, see also resolution of CID 554  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 554 |
| 82 | Graham Smith | 10.71.2.4 | 79, 60 | "...time based on the TSF of the link," Superfluous, the field description already says this. | At cited location delete "based on the TSF of the link" | Accept: |
| 83 | Graham Smith | 10.71.2.4 | 79, 65 | "...EDP element on a link," How else? Delete "on a link" | At cited location delete "on a link," | Revised  The sentence has been reworded, and reception of the frame is not mentioned any more, see also resolution of CID 554  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 554 |
| 84 | Graham Smith | 10.71.2.4. | 80, 01 | "Store the First planned epoch start time, the epoch interval,.." Needs tidying iup also omits TSF from the field name. | Replace cited text with "Store the values of the First Planned Epoch TSF Start Time and Epoch Interval fields, | Revised - Agree in principle.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 84 |
| 85 | Graham Smith | 10.71.2.4 | 80, 02 | "to the value of the received Epoch number offset for that link" Value of the field! | Replace cited text with "to the value of the received Epoch Number Offset field." | Accepted  Modification already incorporated to the D1.2. No action required for the TGbi editor. |
| 86 | Graham Smith | 10.71.2.4 | 80, 04 | "Constructs the corresponding First planned epoch start time of its other links according to the formula:" Value of.. | Replace cited text with "Constructs the value of the corresponding First Planned Epoch TSF Start Time of its other links according to the formula: | Revised - Agree in principle.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 86 |
| 89 | Graham Smith | 10.71.2.4 | 80, 21 | "with" should be "where" | At cited location replace "with" with "where" | Accepted  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 89 |
| 108 | Chaoming Luo | 10.71.2.3 | 79, 28 | The "Epoch Interval Duration field" is not defined, assume it should be "Epoch Interval field" | Define it or use the correct field name. | Accepted  Modification already incorporated to the D1.2. No action required for the TGbi editor. |
| 109 | Chaoming Luo | 10.71.2.4 | 80, 40 | The "Epoch Interval Duration field" is not defined, assume it should be "Epoch Interval field" | Define it or use the correct field name. | Accepted  Modification already incorporated to the D1.2. No action required for the TGbi editor. |
| 120 | Chaoming Luo | 10.71.2.4 | 80, 64 | When to apply the FA parameters is described in P79, so it's better to move this sentence to P79. | Move this sentence to P79L40. | Accepted  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 120 |
| 150 | Stephen McCann | 10.71.2.3 | 78, 10 | Outside of the definitions in clause 3.2, this is the only use of "EDP parameters". What are "the EDP parameters" referring to, as they have not been mentioned before? | Replace "the EDP parameters" with "the privacy parameters" and also at P21L43, P22L6 and P22L12. | Revised - Agree in principle.  “EDP parameters” is replaced by “FA parameters”  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 150 |
| 197 | Jarkko Kneckt | 9.4.1.83 | 49, 05 | Capital letters and unclear sentence | Change to :"The Epoch Number Offset field indicates the offset between the AP MLD and the non-AP MLD epoch numbers." | Accepted  Modification already incorporated to the D1.2. No action required for the TGbi editor. |
| 345 | Carol Ansley | 10.71.2.4 | 79, 52 | Clarify sentence, it's overly wordy :To avoid an easy determination of the epoch start time by an eavesdropper in a link, the start time of each EDP epoch in a link is determined by introducing a pseudo random variation around a planned start time occurring at a regular interval. " | Change sentence to: To avoid an easy determination of the epoch start time on a specific link by an eavesdropper, a pseudo random variation is introduced to vary the regularly scheduled start time of each EDP epoch. | Revised - Agree in principle.  New sentence is proposed.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 345 |
| 437 | Mark RISON | 9.4.1.83 | 48, 53 | "Epoch number offset field value" should be uppercase field name and not have value | Change to "Epoch Number Offset field" | Accepted  Modification already incorporated to the D1.2 .No action required for the TGbi editor. |
| 554 | Mark RISON | 10.71.2.3 | 79, 57 | " the AP may send in response to the requesting non-AP STA, an EDP element" -- it should be mandatory to respond, and also it should be clear in which frame the element is sent | As it says in the comment | Revised - Agree in principle.  It is proposed to replace “may” with “shall”.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 554 |
| 1054 | Philip Hawkes | 10.71.2.4 | 79, 59 | "the AP may send in response to the requesting non-AP STA, an EDP element" is awkward to read | Replace identified text with "an EDP element in the corresponding response," | Revised  Agree in principle, the sentence has been revised. see resolution of CID 554  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 554 |
| 854 | Patrice Nezou | 9.4.1.83 | 47, 50 | The "Time Range" field is always required for an EDP Epoch. I think the "present" bit is useless. | Please clarify or remove this bit | Reject  Time Range field is not always present, this field is for instance absent from EDP request “join” frame. |
| 870 | Patrice Nezou | 10.71.2.3 | 79, 26 | What is a "Group Enhanced Privacy" element ? It seems that it does not exist. | Please clarify | Revised - Agree in principle.  Replace “Group Enhanced Privacy element” by “EDP element”.  Modification already applied in the draft D1.2. No action required for the TGbi editor. |
| 954 | Robert Stacey | 10.71.2.4 | 79, 52 | Clumsy wording. The fact that the adjustment is pseudo random as opposed to random is not important in describing the principle. | Change "To avoid an easy determination of the epoch start time by an eavesdropper in a link, the start time of each EDP epoch in a link is determined by introducing a pseudo random variation around a planned start time occurring at a regular interval." to "To prevent an eavesdropper from easily predicting the epoch start times, each epoch start time is adjusted by a random amount." | Revised - Agree in principle.  New sentence is proposed. (see also resolution of CID345)  Regarding “random” V.S “pseudo random”. This point is especially important because the same offset is computed by AP and STAs, and this is possible because this is a pseudo random computation, not a really random one.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 954 |
| 1051 | Philip Hawkes | 10.71.2.3 | 79, 24 | This sentece is complex for an overview. Only the first phrase is needed. | Compress sentence to "The next epoch boundary is derived as described in 10.71.2.4 (EDP Epoch Start Time Computation)." | Revised - Agree in principle.  The last sentence of the paragraph is removed for clarification.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 1051 |
| 1053 | Philip Hawkes | 10.71.2.4 | 79, 57 | This sentence is not quite correct | Replace "At the start of the new group EDP epoch, the new anonymization parameters are ...", with "From the start of one EDP epoch until the start of the next EDP epoch for that EDP group, the frame anonymization parameters for that EDP epoch are ... | Revised  Agree in principle with the commenter. Sentence is modified accordingly.  Instruct TGbi editor to make the changes shown in the latest version of 11-25/1113r1 under all headings that include CID 1053 |
| 1058 | Philip Hawkes | 10.71.2.4 | 80, 26 | the function "int ()" is not defined. | Define the function "int ()" | Rejected  Function int() is defined in clause 1.5 (Terminology for mathematical, logical, and bit operations) |

**TGbi Editor: *Instruction: Modify 10.71.2.3 as follows***

* EDP epoch transition(#552) operations

Each EDP epoch(#535) starts with a transition period.

During the transition period of an EDP epoch(#535), the FA[#150] parameters assigned to a non-AP MLD during the preceding EDP epoch(#536) shall remain valid only for the following operations:

* Retransmission of a frame.
* Reception of a retransmitted frame.
* Frame acknowledgement.

A transition period terminates at the end of a transition timeout interval or before the end of the transition timeout interval, after the completion of the successful transmissions or retransmissions initiated during the preceding EDP epoch, whichever comes first.



* Example of EDP epoch(#535) timeline

Figure 10-166a (Example of EDP epoch(#535) timeline) shows an example EDP epoch sequence of consecutive EDP epochs with their associated EDP epoch start times tn and transition period tpn.

An overview of the group EDP epoch is shown in Figure 10-166b (Overview of group EDP epoch).



* Overview of group EDP epoch

The next epoch boundary is derived (as described in 10.71.2.4 (EDP Epoch Start Time Computation)) from the value of the first epoch TSF start time defined in the EDP Epoch Settings field of the EDP(#117) element of the (Re)Association Response frame or the EDP Response(#118) frame. [#1051]

A CPE non-AP MLD belonging to an EDP group and the CPE AP MLD may calculate the new OTA values to be used for the non-AP MLD in the next group EDP epoch.

From the start of an EDP epoch until the start of the next EDP epoch for that EDP group,, the new frame anonymization parameters are used to anonymize the selected OTA fields of all new individual frames transmitted during the epoch.[#1053]

[#120]

To account for clock drifts, the CPE non-AP MLD and CPE AP MLD shall begin to accept individually addressed frames that use the new anonymization parameters for a dot11EDPEpochStartTimeMargin before the start of the new epoch. The CPE non-AP MLD and CPE AP MLD shall accept individually addressed frames with the old anonymization parameters for dot11EDPEpochTransitionTime after the start of the new epoch. The rules of 10.71.2.1 (General) apply for frame retransmissions and acknowledgments.

**TGbi Editor: *Instruction: Modify 10.71.2.4 as follows***

* EDP Epoch Start Time Computation

To prevent an eavesdropper from easily predicting the EDP Epoch start time, a pseudo random offset is computed and used by both the AP and each non-AP STAs of the EDP group..[#345, 954]

An AP sending to an non-AP STA, an EDP Epoch Response frame or an Association Response frame, shall include[#554] an EDP element including the first epoch TSF start time(#81)(#82), the epoch interval, and the Epoch Number Offset field(#80) set to the next epoch number of the EDP epoch sequence of the EDP group assigned to the non-AP STA.

Upon reception of an EDP Epoch Response frame, or of a (Re)Association Response frame containing an EDP element on a link, the non-AP STA of a non-AP MLD shall:

* Store the value of the first epoch TSF start time[#84], the epoch interval, and set its epoch number for this epoch(#80) to the value of the received epoch number offset[#85].
* Construct(#330) the value of the corresponding first epoch TSF[#86] start time of its other links according to the formula:

First(#81) epoch TSF start time of another link= First epoch TSF start time of the receiving link + TSF Offset value between the other link and the receiving link

NOTE 1—the TSF Offset value is the value received in the latest Basic Multi-Link element exchange.

At any point of time, for a given link, for any EDP epoch number *n* (*n* > 0) in an EDP epoch sequence, the link TSF timer value corresponding to the start time of the EDP epoch number *n* is called EpochTSFStartTime(*n*) and is computed according to the formula:

EpochTSFStartTime(*n*) = PlannedTSFStartTime(*n*) for the link + ΔIT

where [#89]

PlannedTSFStartTime(*n*) = FirstPlannedEpochTSFStartTime + (*n* – EpochNumberOffset) × EpochInterval

ΔIT = int (KDF-*Hash*-*Length*(PGTK, "ERCM", *n*)) mod TimeRange

and where

*n* is a 2 bytes value in little endian order of the current number of

the EDP epoch in the EDP epoch sequence.

PlannedTSFStartTime(*n*) is the TSF timer value of the link corresponding to the start

time of the EDP epoch number n in the EDP epoch sequence.

EpochNumberOffset is the value indicated in the Epoch Number Offset field of the

EDP Epoch Settings field.(#80, #764)

EpochInterval is the value in TU corresponding to the Epoch Interval

field(#871) of the EDP Epoch Settings field .

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 9-190 (AKM suite selectors)).

*Length* is the number of bits to derive. 16 bits are derived for ΔIT.

FirstPlannedEpochTSFStartTime is the value of the first epoch TSF start time,

computed upon reception of an EDP element by the STA based

on the First Epoch TSF Start Time value of the EDP element of

the received EDP Epoch Settings field.(#764)

TimeRange is the value in TU corresponding to the Time Range field of

the EDP Epoch Settings field.(#549, #764)

PGTK(#550) is the cryptographic key assigned by an EDP AP MLD that is

used to manage the group EDP epoch, distributed to the EDP

non-AP MLDs associated with the EDP AP MLD.(#764)

[#120]