IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 Misc CRs  |
| Date: 2025-07-28 |
| 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:

784, 589, 891, 251.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: after 07/29 meeting
* Rev 2: after 07/31 meeting.

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** |
| 784 | 3.2 | 21.28 | The definitions of EDP devices imply that CPE devices and BPE devices are subsets. Is that correct? Are there other subsets? (Does a EDP device have to be at least a CPE or BPE device?) Are the subsets distinct? (e.g., can a device be both CPE and BPE?). | Somewhere in the spec (perhaps in clause 4), it would be useful to describe the relationship between these various categories of capabilities and how they apply to APs/STAs/MLDs. | RevisedIn 11-25/1008, the definition of BPE was added, that already underlines that BPE includes CPE features. Add more text in clause 4. TGbi editor to make the changes shown in the latest version of 11-25/1383 under all headings that include CID 784 |
| 589 |   | 0.00 | It is not clear whether you can use CPE and BPE at the same time, and if so how they interact | As it says in the comment | RevisedAlso addressed with CID 784. TGbi editor to make the changes shown in the latest version of 11-25/1383 under all headings that include CID 589 |
| 891 | 10.71.4 | 85.08 | PGTK is used for two privacy purposes (EDP Epoch Start Time Computation and Establishing BPE frame anonymization parameter sets) which constitutes a bad key hygiene / key separation in terms of security. | Please define two different keys, one for the EDP Epoch Start Time Computation and one for Establishing BPE frame anonymization parameter sets. | Rejected The group could not agree on a common solution. |
| 251 | 10.71.5.5 | 91.07 | The TSF anonymization scheme can cause timestamp values overlap, i.e. TSF runs over the maximum value. This is uncommon situation that may cause issues to STAs. | Clarify how the maximum TSF value overrun is handled, or avoided. | RevisedTGbi editor to make the changes shown in the latest version of 11-25/1383 under all headings that include CID 251 |

**Discussion**

CID 784, 589

Revised

11-25/1008 adds this definition for BPE:

**BSS privacy enhancements (BPE):** BSS privacy features for AP-MLDs and non-AP MLDs, including CPE features

Clause 10.71.8 clarifies that *BSS Privacy Enhancement (BPE) operations protect privacy of BPE AP MLDs and associated BPE non-AP MLDs* and that *The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group.*

However, whilere there is a clause 4.5.4.10a clause on CPE, there is no text in the same clause for BPE, but the content is too short.

**4.5.4.10a Enhanced Data Privacy (EDP) enhancements (in 11-25/626)**

Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can modify the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a non-AP STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the non-AP STA or non-AP MLD through its messages outside of a secured connection.(#383, 384) A non-AP MLD supporting CPE frame anonymization can change the MAC address(es) and other fields used in communications by its affiliated STAs during an association.(#881, 304, 771, 297)

An AP MLD supporting BPE EDP features can reduce the availability of information about itself, such as the MAC addresses of its affiliated APs and the ESS to which it belongs, that is revealed to third party observers.(#789, 882) A BPE AP MLD can protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are configured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs can change their OTA MAC addresses and other trackable fields for both unicast and group transmissions. (#11, 382, 385, 387, 388, 389, 787, 789, 904, 297)

NOTE – EDP features might be generally described with MLO terminology, but separate descriptions are provided for individual features to explain when the behaviour of MLO and non-MLO devices will differ. (#788)

Proposed fix:

**4.5.4.10a Enhanced Data Privacy (EDP) enhancements**

Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can modify the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a non-AP STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the non-AP STA or non-AP MLD through its messages outside of a secured connection.(#383, 384) A non-AP MLD supporting CPE frame anonymization can change the MAC address(es) and other fields used in communications by its affiliated STAs during an association.(#881, 304, 771, 297)

An AP MLD supporting BPE EDP features can reduce the availability of information about itself, such as the MAC addresses of its affiliated APs and the ESS to which it belongs, that is revealed to third party observers.(#789, 882) A BPE AP MLD can protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are configured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs can change their OTA MAC addresses and other trackable fields for both unicast and group transmissions. (#11, 382, 385, 387, 388, 389, 787, 789, 904, 297)

An EDP AP MLD or non-AP MLD enables CPE features or BPE features. While a CPE AP MLD operates one or more EDP groups, a BPE AP MLD operates a single EDP group.

NOTE – EDP features might be generally described with MLO terminology, but separate descriptions are provided for individual features to explain when the behaviour of MLO and non-MLO devices will differ. (#788)

CID 251

**10.71.5.5 Timestamp anonymization**

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

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

where EDP\_Timestamp\_offset is the Timestamp offset value generated for the BPE AP MLD.

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)).

Note 1 – The sum Timestamp + EDP\_Timestamp\_offset may occasionally exceed 264 and wrap. This event does not affect the BPE non-AP MLD, as it does not use OTSF, but the interval Timestamp for its operations.

*TGbi editor: Modify clause 4.5.4.10a as follows (track change on – changes from version after 11-25/626):*

Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can modify the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a non-AP STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the non-AP STA or non-AP MLD through its messages outside of a secured connection.(#383, 384) A non-AP MLD supporting CPE frame anonymization can change the MAC address(es) and other fields used in communications by its affiliated STAs during an association.(#881, 304, 771, 297)

An AP MLD supporting BPE EDP features can reduce the availability of information about itself, such as the MAC addresses of its affiliated APs and the ESS to which it belongs, that is revealed to third party observers.(#789, 882) A BPE AP MLD can protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are configured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs can change their OTA MAC addresses and other trackable fields for both unicast and group transmissions. (#11, 382, 385, 387, 388, 389, 787, 789, 904, 297)

An AP MLD or non-AP MLD implementing EDP features can support CPE features, BPE features or both. While a CPE AP MLD implements one or more EDP groups, a BPE AP MLD implements a single EDP group. As such, an AP MLD or non-AP MLD operating solely with BPE implements CPE features, but without multi-group management. (#784, 589)

NOTE – EDP features might be generally described with MLO terminology, but separate descriptions are provided for individual features to explain when the behaviour of MLO and non-MLO devices will differ. (#788)

*TGbi editor: Modify clause 10.71.6.1 as follows (track change on):*

**10.71.6.1 Address filtering**

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

If CPE is enabled for the non-AP MLD and BPE is not enabled for the BSS, then for each setup link of the non-AP MLD:

During the dot11EDPEpochStartTimeMargin period and the transition period of the EDP epoch of the non-AP MLD (see 10.71.2.1 (General) and 10.71.2.2 (EDP group 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 EDP\_STA\_address of the affiliated STA from the MAC header anonymization parameters (defined in 10.71.5.1 (MAC header anonymization parameter set selection)) of the old EDP epoch (if any), and the (fixed) address of the affiliated AP,

the EDP\_STA\_address of the affiliated STA from the MAC header anonymization parameters (if any) of the new EDP epoch, and the (fixed) address of the affiliated AP, and

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 dot11EDPEpochStartTimeMargin 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 EDP\_STA\_address of the affiliated STA from the MAC header anonymization parameters (if any) of the new EDP epoch, and the (fixed) address of the affiliated AP, and

for each group to which the affiliated STA is assigned, the (fixed) group address and the (fixed) address of the affiliated AP.

 (#590) 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, starting dot11EDPEpochStartTimeMargin before the transition period (#590), 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:

the EDP\_STA\_MAC and anonymized AP address from the MAC header anonymization parameters (if any) of the old EDP epoch,

the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the old EDP epoch,

the EDP\_STA\_MAC and anonymized AP address from the MAC header anonymization parameters (if any) of the new EDP epoch, and

and the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the new EDP epoch.

After this transition period, until the 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:

the EDP\_STA\_MAC and AP anonymized address from the MAC header anonymization parameters of the new EDP epoch, and

and the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the new EDP epoch.

*TGbi editor: Modify Table 3-373 as follows (track change on):*

**Table 9-373 Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| … |  |  |
| 23 | EDP Robust Individually Addressed Management Frame Support | An EDP STA sets the EDP Robust Individually Addressed Management Frame Support field to 1 if dot11EDPRobustIndividuallyAddressedManagementFrameActivated is true. Otherwise, this field is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frames and Robust Individually Addressed Beamforming/CSI/CQI Frames(#647)).(#40) |
| 24 | EDP Robust Individually Addressed Beamforming/CSI/CQI Frame TB(#209) Tx Support | An EDP STA sets the EDP Robust Individually Addressed Beamforming/CSI/CQI Frame TB(#209) Tx Support field to 1 if dot11EDPRobustIndividuallyAddressedBeamformingCSICQIFrameTBTxActivated(#209) is true. Otherwise, this field is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frames and Robust Individually Addressed Beamforming/CSI/CQI Frames(#647)).(#40) |
| 25 | EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Rx Support | An EDP STA sets the EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Rx Support field to 1 if dot11EDPRobustIndividuallyAddressedBeamformingCSICQIFrameRxActivated is true. Otherwise, this field is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frames and Robust Individually Addressed Beamforming/CSI/CQI Frames(#647)).(#40) |
| 26 | EDP Capabilities And Operation Parameters Request/Response Support | An EDP STA sets the EDP Capabilities And Operation Parameters Request/Response field to 1 if dot11EDPCapabilitiesAndOperationParametersRequestResponseActivated is true. Otherwise, this field is set to 0. See 12.16.4 (Capabilities and operation parameters request and response procedure(#159)).(#40) |
| 27 | (Re)Association Frame Encryption Support | An EDP STA sets the (Re)Association Frame Encryption Support field to 1 if dot11EDPReAssociation FrameEncryptionSupportActivated is true. Otherwise, this field is set to 0. See 12.16.6 ((Re)Association Request/Response Frame Encryption).(#40) |
| 28 | IEEE 802.1X Authentication Utilizing Authentication Frame Support | An EDP STA sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field to 1 if dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true. Otherwise, this field is set to 0.(#40) |
| 29 | PMKSA Caching Privacy Support | An EDP STA sets the PMKSA Caching Privacy Support field to 1 if dot11EDPPMKSACachingPrivacySupportActivated is true. Otherwise, this field is set to 0. See 12.16.7 (PMKSA caching privacy).(#40) |
| 30 | Group EDP Epoch Supported | An EDP STA (#466)sets the Group EDP Epoch Supported field to 1 when dot11EDPGroupEpochActivated is true and sets it to 0 otherwise. |
| 31 | DS MAC Address Support | The DS MAC Address Support field is set to 1 when dot11DSMACAddressActivated is true and is set to 0 otherwise. |
| 32 | EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Non-TB(#209) Tx Support | An EDP STA sets the EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Non-TB Tx Support field to 1 if dot11EDPRobustIndividuallyAddressedBeamformingCSICQIFrameNonTBTxActivated is true. Otherwise, this field is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frames and Robust Individually Addressed Beamforming/CSI/CQI Frames(#647)).(#209) |

*TGbi editor: Modify Annex C-3 as follows (track change on):*

dot11EDPGroupEpochActivated OBJECT-TYPE

 SYNTAX TruthValue

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

 "This is a control variable.

 It is written by an external management entity.

 This attribute, when true, indicates that the station capability of group epochs is enabled. False indicates that the capability is present but is disabled. This attribute is not present if the capability is not present. (#738)"

 DEFVAL { false }

 ::= { dot11EDPStationConfigEntry 2 }

dot11EDPEpochStartTimeMargin OBJECT-TYPE

 SYNTAX Unsigned32 (1..100)

 UNITS "0.1 milliseconds"

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

 "This is a control variable.

 It is written by an external management entity or the SME.

 Changes take effect as soon as practical in the implementation.

 This attribute indicates the duration, before an epoch boundary, during which a STA receiving individually addressed frames accepts (#739)frames that use the current nor the next epoch parameters."

 DEFVAL { 100 }

 ::= { dot11EDPStationConfigEntry 3 }

dot11EDPEpochTransitionTime OBJECT-TYPE

 SYNTAX Unsigned32 (1..1000)

 UNITS "TUs"

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

 "This is a control variable.

 It is written by an external management entity or the SME.

 Changes take effect as soon as practical in the implementation.

 This attribute indicates the duration, after an epoch boundary, during which a STA receiving individually addressed frames accepts (#739)frames that use the previous nor the current epoch parameters."

 DEFVAL { 300 }

 ::= { dot11EDPStationConfigEntry 4 }

*TGbi editor: Modify clause 10.71.2.4 as follows (track change on):*

**10.71.2.4 EDP Epoch Start Time Computation**

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.

Upon reception on a link of an EDP Epoch Request frame or a(#553) (Re)Association Request frame, the AP may send in response to the requesting non-AP STA, an EDP element including the first epoch TSF start time(#81) based on the TSF of the link, 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 first epoch TSF start time(#81), the epoch interval, and set its epoch number for this epoch(#80) to the value of the received epoch(#80) number offset for that link.

Construct(#330) the corresponding first epoch TSF(#81) 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

with

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

ΔIT = int (KDF-*Hash*-*Length*(PGTK1 (#891), "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)

 PGTK1(#891) 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)

If the start time of an EDP epoch occurs during an ongoing TXOP, the FA parameters corresponding to the new EDP epoch(#535) apply(#90) at the end of that(#1065) TXOP.

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

**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* (PGTK2 (#891), "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))

 PGTK2 (#891) 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.

*TGbi editor: Modify Clause 10.71.5.5 as follows (track change on):*

**10.71.5.5 Timestamp anonymization**

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

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

where EDP\_Timestamp\_offset is the Timestamp offset value generated for the BPE AP MLD.

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)).

Note 1 – the sum Timestamp + EDP\_Timestamp\_offset may occasionally exceed 264 and wrap. This event does not affect the BPE non AP MLD, as it does not use OTSF, but the interbal Timestamp for its operations. (#251)