IEEE P802.11
Wireless LANs

|  |
| --- |
| Frame Anonymization  |
| Date: 2024-05-07 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Domenico Ficara | Cisco |  |  | dficara@cisco.com |
| Jerome Henry | Cisco |  |  | jerhenry@cisco.com |
| Ugo Campiglio | Cisco |  |  | ucampigl@cisco.com |
| Javier Contreras | Cisco |  |  | jacontre@cisco.com |
| Jarkko Kneckt | Apple |  |  | jkneckt@apple.com |
| Stéphane Baron | Canon Research centre France |  |  | Stephane.baron@crf.canon.fr |
| Julien Sevin | Canon Research centre France |  |  | Julien.sevin@crf.canon.fr |
| Patrice Nezou | Canon Research centre France |  |  | Patrice.nezou@crf.canon.fr |

Abstract

This submission is normative text for the individual and group EDP epochs.

The automatic EDP epochs is presented in submission 11-24-579r0.

The group EDP epochs is presented in submission 11-23-1984r3.

Version history:

V0 was presented and discussed on 802.11bi meeting sloton Wed 3/13 PM2.

V1 incorporates the feedback from the 802.11bi. The submission follows more closely 802.11bi D0.2 structure.

V2 incorporates the feedback from the TG after presentation.

V3 integrates more feedback.

V4 integrates 11-24-0645 and comments from 11-24-731.

V5: Changes in this version:

* This doc only captures the epoch framework. The actual anonymization of fields such as STA MAC address, AID, PN, SN, subset of MAC header frames, etc. will be discussed separately in another document.
* Left the minimum EPOCH duration TBD but no shorter than 1s.
* Removed AID obfuscation.
* Replaced the Individual epoch by EDP epoch request.
* A CPE STA can request starting a group EDP epoch (with preferred epoch parameters specified) or request to join a specify Group epoch (with Group ID specified).
* CPE AP accepts or rejects the request. The CPE AP can create a new group EDP epoch to match the requested parameters or ask the STA to join an existing group EDP epoch with same parameters.
* Group EDP epoch can have one or more CPE STAs as members.

V6: APs and STAs are MLDs. There is a transition period between epochs.

## 10.71.2.1 Introduction

*Instructions to the 802.11bi Editor: Please add the following changes as shown with track changes.*

## A CPE AP provides anonymization of selected OTA fields of individually addressed frames of associated CPE STAs within a structure of EDP epochs.

## An EDP epoch(#Ed) is a time period in which a set of EDP parameters remain constant. EDP epoch(#Ed) operation is an EDP feature that is valid when MLO is supported.

## A group(#Ed) EDP epoch(#Ed) sequence is created by an AP MLD advertising the EDP epoch(#Ed) support in beacons and probe responses. A group EDP epoch has zero or more STAs as its members. A CPE AP advertises at least a default group EDP epoch, and possibly other group epochs. All CPE STAs joining the BSS are placed in the default group EDP epoch by default upon association. If a CPE STA chooses not to join any of the existing group EDP epochs, it may send an EDP epoch sequence request to the CPE AP to create a new group EDP epoch. A CPE STA can request to leave any group and/or join a different group at any time.

## The AP MLD advertises the EDP epoch (#Ed) parameters as defined in 10.71.2.3 (EDP Epoch Settings (#Ed))(#Ed). Each non-AP MLD of the set of non-AP MLD members of the group applies the advertised EDP epoch(#Ed) parameters of the group(#Ed) EDP epoch(#Ed) to determine the EDP epoch(#Ed) sequence of one or more EDP epoch(#Ed) start times.

EDP epoch operation allows the AP to define a BSS-specific schedule of anonymization events to anonymize selected OTA fields (e.g., STA MAC address, AID, PN, SN, etc.) of individually addressed frames.

All EDP epochs have a similar anonymization mechanism for the MAC Header fields of the individually addressed frames as defined in 10.71.3 (Establishing frame anonymization parameter sets), 10.71.4 (Frame anonymization and transmitting functions) and 10.71.5 (Frame anonymization receiving functions).

Each EDP Epoch starts with a transition period.

During the transition period of an EDP Epoch, the EDP parameters assigned to a STA during the preceding EDP Epoch, shall remain valid only for the following operations:

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

**10.71.2.2 EDP epoch(#Ed) setup**

*Instructions to the 802.11bi Editor: Please delete this clause and its subclauses.*

**10.71.2.2 EDP epoch request**

*Instructions to the 802.11bi Editor: Please add this clause and renumber the following clauses.*

A CPE non-AP MLD shall be assigned to the default group EDP epoch, with a Epoch ID of 0, when the non-AP MLD associates to the CPE BSS and both the AP MLD and non-AP MLD support group EDP epoch. The group EDP epoch setup is described in 10.71.2.4 (Group EDP epoch setup).

A CPE non-AP MLD may subsequently send a EDP epoch request to join a specific group EDP epoch or the CPE non-AP MLD can request the AP MLD to start a new group EDP epoch that matches specified EDP epoch settingsby sending an EDP epoch setting protected action request frame.

The AP MLD shall respond with an EDP epoch setting protected action response frame, accepting or rejecting the request.

A CPE non-AP MLD may leave the group EDP epoch by sending an EDP epoch setting protected action request frame.

**10.71.2.3 Group EDP epoch**

*Instructions to the 802.11bi Editor: Please add this clause and renumber the following clauses.*

A CPE AP MLD advertises group EDP epoch support in Beacon and Probe Response frames by setting value 1 to the Group EDP Epoch Supported field of the Extended RSN Capabilities field.

A CPE non-AP MLD advertises group EDP epoch support in (Re)-Association Request frames by setting value 1 to the Group EDP Epoch Supported field of the Extended RSN element.

Group EDP Epoch support is mandatory for the CPE AP MLD and the CPE non-AP MLD.

A CPE AP MLD advertises group EDP epochs by sending an unicast protected action frame containing an Enhanced Group Privacy Availability element for each relevant group EDP epoch in the BSS. A CPE AP MLD shall advertise group EDP epochs to each non-AP MLD that joins the BSS and may advertise group EDP epochs when significant changes have affected one or more groups.

A CPE non-AP MLD may be a member of only one group EDP epoch at a time.

A CPE non-AP MLD may request to join a group EDP epoch by sending an EDP epoch setting protected action request frame, containing the group ID that the non-AP MLD wishes to join.

The AP MLD responds with an EDP epoch setting protected action response frame, accepting or rejecting the request.

A CPE non-AP MLD may leave the group EDP epoch by sending EDP epoch setting protected action request frame.

If a CPE non-AP MLD is a member of a group EDP epoch, the non-AP MLD and the AP MLD shall anonymize the selected OTA fields of the individually addressed frames according to group epoch settings as defined in 10.71.3 (Establishing frame anonymization parameter sets), 10.71.4 (Frame anonymization transmitting functions), 10.71.5 (Frame anonymization receiving functions) and 10.71.6 (Frame anonymization and AID). An overview of the group EDP epoch is shown in Figure XX (Overview of an EDP epoch).



**Figure XX – Overview of group EDP epoch.**

## 10.71.2.4 Group EDP epoch setup

*Instructions to the 802.11bi Editor: Please add this clause and renumber the following clauses.*

A CPE non-AP STA signals support for group EDP epoch by setting the Group EDP Epoch Supported field in the RSNXE in the (Re-)Association Request Frame.

A group EDP epoch has a BSS Specific Epoch Number and non-AP MLD Specific Epoch Number that are signaled to the non-AP MLD at the group EDP epoch setup. The BSS Specific Epoch Number is an input parameter of the BSS specific offset calculation. The non-AP MLD Specific Epoch Number is an input parameter of the non-AP MLD specific offset calculation.

If a CPE AP MLD supports group EDP epoch and receives a (Re)Association Request frame with the Group EDP Epoch Supported field set, then the AP MLD shall assign the CPE non-AP MLD to the default group EDP Epoch if association succeeds.

The protected Association Response frame provides the default group EDP information in the EDP Epoch Settings field of the Group Enhanced Privacy Element.

After the affiliated STAs of thr non-AP MLD have associated, the CPE AP MLD sends to the CPE non-AP MLD one or more protected action frames that include the Enhanced Group Privacy Availability Element, to signal the list of group EDP epochs supported in the BSS. The non-AP MLD may request to join another group EDP epoch, or provide EDP epoch settings, by sending a non-Ap MLD Specific Epoch Setting action frame.

## 10.71.2.6 Epoch boundaries

*Instructions to the 802.11bi Editor: Please add this clause and renumber the following clauses.*

The affiliated STAs of a CPE MLD anonymize their EDP OTA fields of individually addressed frames at the beginning of each new epoch. The next epoch boundary occurs at a Next Epoch Start Time defined in the EDP Epoch Setting field of the Group Enhanced Privacy element of the (re)-association response frame or the EDP epoch setting action response frame. The Epoch Duration field of the same fields and frames defines the interval of the following group EDP epochs.

Each EDP epoch has Group and non-AP MLD specific Epoch Numbers, which values are increased by 1 for each epoch.

A CPE non-AP MLD and CPE AP MLD may calculate the anonymized OTA values before the EDP epoch during which they are to be used.

At the start of the new EDP epoch, the new anonymization parameters are used to anonymize the selected OTA fields of all transmitted individually addressed frames.

The CPE non-AP MLD and CPE AP MLD shall begin to accept individually addressed frames that use the new anonymization parameters for a *dot11EpochTransitionTime* before the start of new epoch. The CPE non-AP MLD and CPE AP MLD shall accept individually addressed frames with the old anonymization parameters for a *dot11EpochTransitionTime* after the start of the new epoch. The rules of clause 10.71.2.1 apply for frame retransmissions and acknowledgments.

The MAC Header parameters of the individually addressed frames are anonymized as defined in 10.71.3 (Establishing frame anonymization parameter sets), 10.71.4 (frame anonymization transmitting functions) and 10.71.5 (frame anonymization receiving functions).

## 10.71.2.8 OTA address collision avoidance

*Instructions to the 802.11bi Editor: Please add the following new clause.*

A CPE AP MLD may calculate that the OTA MAC address that a CPE non-AP MLD is bound to use in a subsequent epoch may cause a collision with the OTA MAC of other CPE non-AP MLD(s). When such collision is detected, the AP shall send to the CPE non-AP MLD an otaMAC collision warning action frame before the collision epoch, instructing the non-AP MLD to apply the signaled non-AP MLD specific Epoch Number to avoid address collision.

NOTE, the non-AP MLD participating to an EPD epoch applies the BSS-specific AID offset to OTA AID, when the Epoch Number changes.

## 9.4.2.240 RSNXE

*Instructions to the 802.11bi Editor: Please add the bit 8 and 9 text to the clause and remove the bits from the reserved bits.*

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 8 | Group EDP Epoch Supported | A non-AP MLD sets the Group Epoch Support field to 1 when dot11GroupEpochActivated is true and sets it to 0 otherwise.  |
|  |  |  |

## 9.6.38.4 Group Enhanced Privacy (EP) element

*Instructions to the 802.11bi Editor: Please add the following new clause. Please renumber the new clause and other clauses accordingly.*

The Group Enhanced Privacy (EP) element signals epoch parameters in protected action frames. The Group EP element signals the default privacy epoch parameters in the protected Association Response frame. The Group EP element signals specific group epoch settings in non-AP MLD Specific Setting Epoch action frames.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | EDP Epoch Settings |
| Octets:  | 1 | 1 | 1 | 0 or 12 |

## Figure -XX Group Enhanced Privacy (EP) element

The Element Id, Length and Element Id Extension fields are defined in 9.4.2.1 (General).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Reserved | Reserved | Group Epoch Interval  | Next Epoch Start Time  | Time Range | Reserved | Epoch Duration | Current Epoch Number |
| Bits: | 11 | 11 | 14 | 64 | 16 | 4 | 8 | 48 |

## Figure XX – EDP Epoch Settings field

The EDP Epoch Settings field defines the anonymization mode of the non-AP STAs.

The Smallest Anonymized AID field signals the smallest AID value that is periodically anonymized.

The AID Range field signals the number of AID values that are periodically anonymized.

|  |  |  |
| --- | --- | --- |
|  | Group Epoch Interval Unit | Group Epoch Interval |
| Bits: | 3 | 11 |

## Figure XX – Group Epoch Interval length field

The Group Epoch Interval field contains the duration of the EDP epoch. The 3 MSBs signal the Group Epoch Interval Unit, as shown in table XX. The 11 LSBs signal the duration of each epoch, in units specified on the Group Epoch Interval Units.

Table XX: Group Epoch Duration Units and epoch durations

|  |  |  |  |
| --- | --- | --- | --- |
| Group Epoch Interval Unit field value | Group Epoch Interval Unit  | Min Epoch Duration  | Max Epoch Duration (approx.) |
| 0 | 1000 s | 16 min 40 s | 23 d 16 h 36 min 40 s |
| 1 | 1 s | not shorter than 1s | 34 min 7 s |
| 2 | Reserved | N/A | N/A |
| 3 | Reserved | N/A | N/A |
| 4 | Reserved | N/A | N/A |
| 5 | Reserved | N/A | N/A |
| 6 | Reserved | N/A | N/A |
| 7 | Reserved | N/A | N/A |

The Next Epoch Start Time field signals the start time of the next EDP epoch, using the reference start time GT0 of the EDP Epoch indicated in the “Start Time” subfield of the EDP Epoch Sequence parameters element.

The effective start time GET of the EDP Epoch is computed according to the formula:

GET = GT0 + ∆IT

where ∆IT = PRF-128\64(GTK\*, “ERCM”, GT0) mod (RandTR)

and where:

PRF-Length is the pseudorandom function defined in 12.7.1.2

GT0 is the value indicated in the Start Time field of the advertised EDP Epoch Sequence parameters element

RandTR is the value indicated in the Time Range field of the advertised EDP Epoch Sequence parameters element

GTK\* is a key derived from GTK, where GTK\* = KDF-Hash-256(GTK, “EDP”, BSSID)

At any point of time, for the next EDP Epoch, the start time is computed according to the formula:

GETn+1 = GTn+1 + ∆IT

∆IT = PRF-128\64(GTK\*, “ERCM”, GTn+1) mod (RandTR)

With:

GTn+1 =GTn+ GEI

Or

n = ⌊(TSF – GT0) / GEI⌋

GTn+1 =GT0+ (n+1) x GEI

Where:

n is the current iteration of the sequence.

TSF is the current value of the internal TSF counter of the receiving link.

GT0 is the value indicated in the Start Time field of the advertised EDP Epoch Sequence parameters element

RandTR is the value indicated in the Time Range field of the advertised EDP Epoch Sequence parameters element

GEI is the value indicated in the Interval field of the advertised EDP Epoch Sequence parameters element

GTK\* is the key derived from GTK.

The time range field is the range used by the stations to determine a random delay added to the EDP Epoch reference start time.

The Epoch Duration field indicates the number of EDP Epochs left to run, after the current epoch finishes. The length of the Duration field is 1 octet. The settings of the value in the Duration field are defined in Table 9-bbb

**Table 9-bbbb - Duration field values**

|  |  |
| --- | --- |
| Value | Meaning |
| 0 | Undetermined (unlimited) duration |
| 1 | The duration corresponds to one more iteration  |
| N | The duration corresponds to N more iterations between [1..255] |

The Current Epoch Number field signals the current epoch number, modulo 48

## 9.6.38.6 Enhanced Group Privacy Availability Element (EGPA) element

*Instructions to the 802.11bi Editor: Please add the following new clause. Please renumber the new clause and other clauses accordingly.*

The Enhanced Group Privacy Availability Element signals the list of EDP epoch groups supported in the BSS, in addition to the default group.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Group Count | Group ID | Length | EDP Epoch Settings  | Number of Participating MLDs |
| Octets:  | 1 | 1 | 1 | 1 | m \* 1 | m \* 1 | m \* 12 | 0 or m \* 3 |
|  |  |  |  |  |  | $$m\geq 1$$ |

## Figure -XX Enhanced Group Privacy Availability Element

The Element Id, Length and Element Id Extension fields are defined in 9.4.2.1 (General).

The Group Count field indicates the number of groups signaled in the EGPA element, each group described with a tuple Group ID, EDP Epoch Settings and Number of Participating MLDs fields. The AP MLD advertises some or all of the configured groups.

The EPGA element contains m ( m = 1 or more) tuples of Group ID field, EDP Epoch Settings field and Number of Participating MLDs field.

The Group ID field signals an identifier of the group EDP Epoch. Value 0 indicates the default group. Value 255 is reserved.

The EDP Epoch Settings field defines the parameter of this group EDP Epoch, as described in 9.6.38.4.

The Participating MLDs field is optional. When present, the field signals an indication of the number of MLDs currently participating to this group EDP epoch.

|  |  |  |
| --- | --- | --- |
|  | Participating MLD Count | Participating MLD Percentage |
| Octets: | 2 | 1 |

## Figure -XX Number of Participating MLDs field

The first two octets of the Participating MLD Count field represent an indication of the number of MLDs participating in the signaled group. The third octet values, in the range of 0 to 100, represent an indication of the percentage of the associated MLDs participating to the signaled group. Values 101-255 are reserved.

## 9.6.38.7 otaMAC collision warning element (oMCWE)

*Instructions to the 802.11bi Editor: Please add the following new clause. Please renumber the new clause and other clauses accordingly.*

The otaMAC collision warning element is present in the otaMAC Collision Warning protected action frame and signals that an otaMAC address expected to be used by the receiving MLD in an upcoming epoch is calculated to collide with another MLD.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Collision Status | Colliding Epoch  | MLD Specific Epoch Number Offset |
| Octets:  | 1 | 1 | 1 | 1 | 1 | 1 |

## Figure -XX otaMAC collision warning element

The Element Id, Length and Element Id Extension fields are defined in 9.4.2.1 (General).

The Collision Status field indicates the intent of the oMCWE. The AP MLD shall set the Collision Status to 1 when signaling to a non-AP MLD the risk of otaMAC collision in a future epoch. The non-AP MLD shall set the Collision Status to 0 when responding to an AP MLD otaMAC Collision Warning action frame, acknowledging the warning and indicating that the non-AP MLD will skip epoch parameters as suggested by the AP MLD. The non-AP MLD shall set the Collision Status to 2 when responding to an AP MLD otaMAC Collision Warning action frame, and rejecting the AP MLD’s suggestions.

The Colliding Epoch field indicates the future epoch at which MAC collision is likely to occur. The epoch is indicated in units of epochs. A value of 0 indicates the current epoch.

The non-AP MLD Specific Epoch Number Offset field indicates the Epoch count that the non-AP MLD skips to mitigate the otaMAC address collision. Thus, if the current epoch is 0, the colliding epoch is m, indicating that the collision is expected to occur m epochs after the current epoch, and if the non-AP MLD Specific Epoch Number Offset is n, then when the epoch is m, the CPE non-AP MLD is expected to use the non-AP MLD Specific value for Epoch Number m+n. The following epoch m+n+1 will use non-AP MLD Specific values of epoch ID m+n+1 unless the AP MLD also signals a collision warning for epoch m+n+1. Value 0 is reserved.

## 9.6.38.8 EDP epoch setting element

*Instructions to the 802.11bi Editor: Please add the following new clause. Please renumber the new clause and other clauses accordingly.*

The EDP epoch setting element is present in the non-AP MLD Specific Epoch Setting action frame, and indicates a request or a response for EDP epoch settings.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Dialog Token | Dialog Value | Target Group ID | EDP Epoch Settings  |
| Octets:  | 1 | 1 | 1 | 1 | 1 | 1 | 0 or 12 |

## Figure -XX EDPepoch setting element

The Element Id, Length and Element Id Extension fields are defined in 9.4.2.1 (General).

The Dialog Token field is used for matching action responses with action requests.

The Dialog Value field indicates the status of the frame carrying the element. A value of 0 is reserved. The field shall be set to 1 when the element is carrying a request from a CPE non-AP MLD to a CPE AP MLD to join the Group EDP specified in Target Group ID if the Group ID is in the range 0-254 or to initiate an EDP epoch if the Group ID is 255. The field shall be set to 2 when the element is carrying a response from the CPE AP MLD to the CPE non-AP MLD accepting the EDP epoch requested by the CPE non-AP MLD. The field shall be set to 3 when the element is carrying a response from the CPE AP MLD to the CPE non-AP MLD rejecting the EDP epoch requested by the CPE non-AP MLD. The field shall be set to 4 when the element is carrying a request from the CPE non-AP MLD stating its intention not to participate to any periodic group epoch. The field shall be set to 5 if the CPE non-AP MLD is notifying the CPE AP that the non-AP MLD will leave the Group EDP specified in Target Group ID if the Group ID is in the range 0-254 or to cancel a previously initiated EDP epoch if the Group ID is 255.

The Target Group ID field indicates the identifier for the group that the non-AP MLD is requesting to join. The value 255 indicates that the non-AP MLD does not request to join a particular group, but requests EDP settings.

The EDP Epoch Settings field is described in clause 9.6.38.4 (Group Enhanced Privacy (EP) element).

When the Dialog field is 1, and the group ID is in the range 0-254, the non-AP MLD is requesting to join a particular group, and the EDP Epoch Settings field is not present.

When the Dialog field is 1 and the Group ID is 255, the non-AP MLD does not request to join a specific group, but requests instead parameters specific to that non-AP MLD, and the EDP Epoch Settings field is present.

When the dialog field is 2, and the group ID is in the range 0-254, the AP MLD accepts the non-AP MLD request. The EDP Epoch Settings field is present and indicates the parameters of the group that the non-AP MLD requested to join.

When the dialog field is 2, and the group ID is 255, the AP MLD accepts the EDP settings requested by the non-AP MLD. The EDP Epoch Settings field is present. TheGroup Epoch and Next Epoch fields indicate the epoch parameters allocated by the AP MLD.

When the dialog field is 3, the AP MLD rejects the non-AP MLD requests. The group ID value is reserved and the EDP Epoch Settings field is not present.

When the dialog field is 4, the non-AP MLD is notifying the AP MLD it will not participate in any group. The group ID is reserved and the EDP Epoch Settings field is not present.

When the dialog field is 5, the non-AP MLD is notifying the AP MLD it will not participate in a specific group. The EDP Epoch Settings field is not present.

|  |  |  |  |
| --- | --- | --- | --- |
| Dialog | Group ID | Context | EDP Epoch Settings |
| 1 | 0-254 | non-AP MLD is requesting to join a particular group | Not Present |
| 1 | 255 | non-AP MLD is requesting non-AP MLD \_specific parameters | Present |
| 2 | 0-255 | AP MLD is accepting non-AP MLD request | Present |
| 3 | Reserved | AP MLD is rejecting non-AP MLD request | Not Present |
| 4 | Reserved | non-AP MLD is requesting to not participate to any group | Not Present |
| 5 | 0-255 | non-AP MLD is requesting not to participate to a specifc group | Not Present |
|  |  |  |  |

*Instructions to the 802.11bi Editor: Please add the new MIB parameters.*

dot11GroupEpochActivated 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.”

DEFVAL { false }

dot11EpochTransitionTime 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 when the STA receives individually addressed frames that use the anonymization parameters before an EPOCH boundary or the new anonymization parameters after the EPOCH boundary."

DEFVAL {100}