IEEE P802.11
Wireless LANs

|  |
| --- |
| Periodic Frame Anonymization  |
| Date: 2024-03-14 |
| 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 |

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.

## 10.71.2.1 Introduction

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

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

Two EDP epochs are defined:

## — An individual(#Ed) EDP epoch(#Ed) sequence request is initiated by a non-AP MLD and the associated AP MLD shall send a response. The EDP epoch(#Ed) parameters of an individual EDP epoch(#Ed) are negotiated by a non-AP MLD with its associated AP MLD as defined in 10.71.2.2 (Individual EDP epoch #Ed)). The non-AP MLD applies the negotiated EDP epoch(#Ed) parameters(#Ed) of the individual(#Ed) EDP epoch(#Ed) to determine the(#Ed) corresponding EDP epoch(#Ed) sequence of one or more EDP epoch(#Ed) start times.

## — A group(#Ed) EDP epoch(#Ed) sequence is initiated by an AP MLD by advertising the EDP epoch(#Ed) parameters to a set of non-AP MLDs as defined in 10.71.2.3 (Group EDP epoch (#Ed))(#Ed). Each non-AP MLD of the set of non-AP MLDs applies the advertised EDP epoch(#Ed) parameters of the group(#Ed) EDP epoch(#Ed) to determine the same EDP epoch(#Ed) sequence of one or more EDP epoch(#Ed) start times.

If the group EDP epoch sequence is supported, the AP defines at least one group where all CPE STAs joining the BSS are placed by default. The default group, called automatic EDP epoch group, allows the AP to define a BSS specific schedule of anonymization events to anonymize the participating OTA AIDs and MAC Headers of individual addressed frames between the STAs and the AP. The automatic EDP epoch is defined in 10.7.2.4(Automatic EDP epoch).

All EDP epochs have a similar anonymization mechanism for the MAC Header fields of the individually addressed frames between the CPE STA and the CPE AP 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).

Individual and group EDP epoch assign new AID for the CPE STA at the beginning of the new epoch. A CPE STA using a group EDP epoch may request that CPE AP assigns new AID value for it. The AID assignment is described in clause 10.71.6(Frame anonymization and AID). Group EDP epoch uses BSS specific AID offset at the beginning of the new epoch to anonymize the AID as described in clause 10.71.2.4.3(OTA AID anonymization with BSS specific offset).

**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 Individual EDP epoch**

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

A CPE AP advertises support for individual EDP epoch in Beacon and Probe Response frames it transmits by setting value 1 to the STA-Specific Epoch Supported field of the Enhanced Privacy Capabilities element.

A CPE STA that desires to use individual EDP epoch sets STA-Specific Setting field.

A CPE STA that does not wish to use the epoch interval announced by the AP in the Periodic Anonymization element sends to the AP a STA-specific epoch setting action request frame, expressing the epoch duration requested by the STA. An epoch duration set to 0 indicates that the STA intends to stop the individual EDP epoch and join back the automatic EDP epoch group. The AP responds with a STA-specific epoch setting action response frame, that indicates the AP reception and acceptance, or refusal of the STA-specific epoch settings requested by the STA.

A CPE STA that does not wish to participate to any group epoch announced by the AP and does not wish to request a specific duration setting, sends to the AP a STA-specific epoch setting action request frame, with dialog field set to 4. The AP responds with acceptance or refusal of the STA request.

When the individual EDP epoch is setup, the STA and AP shall anonymize the AID of the STA and the MAC Header parameters of the individually addressed frames between the STA and the AP according to STA-specific 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).

**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 advertises support for group EDP epoch in Beacon and Probe Response frames it transmits by setting value 1 to the Group Epoch Supported field of the Enhanced Privacy Capabilities element.

Group EDP Epoch support is optional for the CPE AP and CPE STA.

Periodically a CPE AP advertises its set of group EDP epochs by means of a broadcast action frame that includes a Enhanced Privacy Group Capability element for each group EDP epoch in the BSS.

A CPE STA that associates a CPE BSS that supports group EDP epochs is automatically assigned to the default group, whose ID is 0.

A CPE STA can join or leave any of the group EDP epochs advertised by the CPE AP by sending to the AP a STA-specific epoch setting action request frame, containing the group IDs that it wishes to participate in, in the form of a bitmap (group EDP epoch bitmap).

The AP responds with a STA-specific epoch setting action response frame, accepting the request.

If a CPE STA participates to at least one group EDP epoch, including the default one, the STA and AP shall anonymize the AID of the STA and the MAC Header parameters of the individually addressed frames between the STA and the AP 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).

EDP epoch setup periodic epochs that allow CPE AP and CPE STA to anonymize the OTA AID of the CPE STA and the OTA MAC Headers of individually addressed frames between the CPE AP and the CPE STA as described in 10.7.2.4.2(Anonymization event). The OTA AID anonymization uses BSS specific offset as described in 10.7.2.4.3(OTA AID anonymization with BSS specific offset). An overview of the groupEDP epoch is shown in Figure XX(Overview of automatic EDP epoch).

 

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

Pseudorandom offset: TBD.

## 10.71.2.4.1 Group EDP epoch setup

A CPE STA signals the support for group EDP epoch by setting the group EDP epoch supported field in the Enhanced Privacy Capability Element in the (Re)Association Request Frame.

If a CPE AP, that supports group EDP epoch, receives a (Re)Association Request frame with the group EDP Epoch field of the Enhanced Privacy element, then the AP shall assign the CPE STA to the default group EDP Epoch if the AP accepts the association. The association is accepted by transmitting a (Re)Association Response frame with Enhanced Privacy element including the group EDP Epoch field set to 1. The CPE AP shall assign AID value to the associating CPE STA on the range that is applied only for the automatic EDP epoch STAs as described in 10.7.2.4.3(OTA AID anonymization with BSS specific offset).

During the 4-way handshake (TBD exactly when) the CPE AP provides the group EDP Epoch field defined in the Enhanced Group Capability Element to signal the group EDP information to the STA.

The group Epoch Length field signals the length of the group EDP Epoch and the Next Epoch field signals the number of TBTTs until the next Epoch boundary.

## 10.7.2.4.2 Epoch boundaries

All automatic EPD epoch CPE STAs anonymize their OTA AID of the CPE STA and OTA MAC Header fields of individually addressed frames between the CPE non-AP STA and CPE AP at the same time. The OTA AID and OTA MAC Header are anonymized at a TBTT, and the anonymization repeats every BSS specific periodic anonymization epoch of one or multiple TBTT(s).

Each epoch is identified by the Epoch Number value that is increased by 1 for each epoch. The Current Epoch Number field in the Periodic Anonymization field of the Enhanced Privacy Element of the (Re)Association Response frame contains the Epoch Number of the previous epoch.

A CPE STA and CPE AP may calculate the OTA AID and OTA MAC Header values in advance before they are taken into use at the next periodic anonymization event.

At the start of the new epoch, the new OTA AID identifies the CPE STA, and the new OTA MAC Header offset are applied to all transmitted individually addressed frames between the CPE STA and CPE AP.

The CPE STA and CPE AP shall begin to receive individually address frames with the new OTA AID and new OTA MAC Header values a *dot11AutomaticEpochTransitionTime* before the start of new epoch. The CPE STA and CPE AP shall continue to receive individually addressed frames with the old OTA AID and old OTA MAC Header values for a *dot11AutomaticEpochTransitionTime* after the epoch.

The MAC Header parameters of the individually addressed frames between the STA and the AP 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).

## 10.7.2.4.3 OTA AID anonymization with BSS specific offset

The AP shall assign an AID value to automatic EDP epoch STAs in a specific range of the AID values. The CPE AP shall assign AID values on this range only to the CPE STAs that use automatic EDP epoch.

An associated (state 4) STA using in automatic EDP epocs may request AP to assign new AID value. This request may be done to improve STA privacy within the associated BSS. If the associated AP receives such a request, then the AP shall assign a new AID value within the range of AID values. The AID assignment is described in clause 10.71.6(frame anonymization and AID.

The automatic EDP epoch STAs randomize their OTA AID values within the range by using the following formula:

OTA AID = Smallest\_anonymized\_AID + ((AID\_assigned + Offset\_AID) Modulo (AID

\_range\_size)), where:

* The smallest anonymized AID value and AID range size are signaled in the Enhanced Privacy element of the (Re)Association Response frame.
* The AID\_Offset is calculated with the following formula:

AID\_Offset = GCMP-256((“802.11bi MAC Header Anonymization. Protecting privacy of the STAs and APs” | GAK | Nonce)

* GCMP-256 encrypts the following text: (“802.11bi MAC Header Anonymization. Protecting privacy of the STAs and APs”.
* The STA and AP use Group Anonymization Key (GAK)
* The Nonce has:
	+ A2 that is set to the BSSID (6 octets)
	+ The Epoch Number (6 octets)
* The eleven (11) least significant bits of the encrypted cipher text are used as AID\_Offset.

## 10.7.2.8 OTA address collision avoidance

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

A CPE AP may calculate the OTA MAC addresses that CPE STAs will use in a subsequent epoch. A CPE AP may detect that some OTA MAC addresses of the CPE STAs may collide in the coming epoch. In this case, the AP shall avoid the collision. The AP shall send an otaMAC collision warning action frame before the epoch, instructing selected STA(s) to skip the anonymization of the MAC Header parameters at the coming epoch as instructed in the otaMAC collision warning frame.

NOTE, automatic EPD epoch applies the BSS specific AID offset to OTA AID, even if the MAC Header parameters anonymization is skipped.

A CPE AP may calculate that the OTA MAC address that a CPE STA is bound to use in a subsequent epoch may cause a collision with the OTA MAC of other CPE STA(s). In that case, the AP shall send to the CPE STA an otaMAC collision warning action frame before that target epoch, instructing the STA to skip the parameters of the target epoch, and to directly apply the parameters of the following epoch.

## 9.x.1 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 Enhanced Privacy (EP) element signals in protected action frames

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | EP Control  |
| Octets:  | 1 | 1 | 1 | 2 |

## Figure -XX Enhanced Privacy (EP) element

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Group EDP epoch bitmap | STA-Specific Setting | Reserved |
| Bits: | 8 | 1 | 5 |

## Figure XX – EP Control field

The EP Control field defines the anonymization mode of the STA.

The group EDP Epoch bitmap has a bit for each group EDP epoch and each bit is set to 1 to signal that the STA wishes to join the group.

The STA-Specific Setting bit is set if the AP supports STA-specific periodic-anonymization epoch durations. The bit is unset otherwise.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Smallest Anonymized AID  | AID Range | Group Epoch Length | Next Epoch | Reserved |
| Bits: | 11 | 11 | 4 | 4 | 2 |

## Figure XX – Group EDP Epoch field

The Periodic Anonymization element is present in association responses only.

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.

The Automatic Epoch Length field contains the length of the automatic EDP epoch as a number of TBTTs -1. Value 0 signals that automatic EDP epoch length is one TBTT interval.

The Next Epoch field signals number of TBTTs until the beginning of the next automatic EDP epoch. Value 0 signals that the next automatic EDP epoch begins at the next TBTT.

The Current Epoch Number field signals the epoch number used in the last automatic EDP epoch.

## 9.x.2 Enhanced Privacy Capabilities element

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

The Enhanced Privacy Capabilities element signals AP support for EDP epochs and privacy protection features.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | EP Capabilities  |
| Octets:  | 1 | 1 | 1 | 2 |

## Figure -XX Enhanced Privacy Capabilities element

|  |  |  |  |
| --- | --- | --- | --- |
|  | Group EDP Supported | STA-Specific SettingSupported |  Reserved |
| Bits: | 1 | 1 | 14 |

## Figure -XX EP Capabilities field

The group EDP Epoch Supported field is set to 1 to signal that AP supports group EDP epochs. Otherwise, the field is set to 0.

The STA-Specific Setting field is set to 1 to signal that AP supports STA-specific settings for different epoch time intervals.

## 9.x.2.1 Enhanced Group Capability Element (EGCP) element

The Enhanced Group Capability Element signals the list of EDP epoch groups in the BSS.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Group ID | Group EDP Epoch Field | Number of Participating STAs |
| Octets:  | 1 | 1 | 1 | 1 | 2 | 1 |

## Figure -XX Enhanced Group Capability Element

The Group ID signal an identifier of the group EDP Epoch.

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

The Participating STAs field signals the number of STAs currently participating to this group EDP

epoch and that have not requested STA-specific settings. The first two octets represent the count of participating STAs. The third octet values 0 to 100 represent the percentage of associated STAs participating to the epoch without STA\_specific settings.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Smallest Anonymized AID  | AID Range | Group Epoch Length | Next Epoch | Reserved |
| Bits: | 11 | 11 | 4 | 4 | 2 |

## Figure XX – Group EDP Epoch field

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.

The group Epoch Length field contains the length of the group EDP epoch as a number of TBTTs -1. Value 0 signals that automatic EDP epoch length is one TBTT interval.

The Next Epoch field signals number of TBTTs until the beginning of the next automatic EDP epoch. Value 0 signals that the next group EDP epoch begins at the next TBTT.

The Current Epoch Number field signals the epoch number used in the last automatic EDP epoch.

## 9.x.3 otaMAC collision warning element

*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 signals that an otaMAC address expected to be used by the receiving STA in an upcoming epoch is calculated to collide with another STA.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Colliding Epoch  | Jump Offset |
| Octets:  | 1 | 1 | 1 | 2 | 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 Colliding Epoch indicates the Anonymization Number at which MAC collision is likely to occur.

The Jump Offset indicates the number of epochs that the STA should skip in its calculation of its parameters for the target epoch. Thus, if the current anonymization number is m, the colliding epoch is n, indicating that the collision is expected to occur when the anonymization number is m+n, and if the jump offset is o, then when the anonymization number is m+n, the CPE STA is expected to use skip the parameters of epoch m+n, and use directly the parameters of epoch m+n+o.

## 9.x.3 STA-specific 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 STA-specific epoch setting element indicates a request or a response for STA-specific epoch settings.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | Dialog | STA-Specific Epoch  |
| Octets:  | 1 | 1 | 1 | 1 | 0 or 2 |

## Figure -XX STA-specific epoch setting element

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

The Dialog 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 STA to a CPE AP for a STA\_specific epoch value. The field shall be set to 2 when the element is carrying a response from the CPE AP to the CPE STA accepting the STA-specific epoch requested by the CPE STA. The STA-specific epoch field is not present in that case. The field shall be set to 3 when the element is carrying a response from the CPE AP to the CPE STA rejecting the STA-specific epoch requested by the CPE STA. The STA-specific epoch field may be present in that case.

The field shall be set to 4 in the element carrying a request from the CPE STA stating its intention not to participate to the periodic group epoch. The STA-specific epoch field shall not be present in this case.

The STA-Specific Epoch field indicates the duration of the epoch requested by the STA. The 4 MSB of the field indicate the unit time value of the epoch. The 12 LSB of the field indicate the duration of the STA-specific epoch, in the specified unit.

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

dot11AutomaticEpochTransitionTime OBJECT-TYPE

SYNTAX Unsigned32 (1..100 000)

UNITS “microseconds”

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 frames that include one of the two OTA AID values and individually addressed frames that include one of the two MAC Header values."

DEFVAL {10 000}