IEEE P802.11
Wireless LANs

|  |
| --- |
| Periodic Frame Anonymization  |
| Date: 2024-03-07 |
| 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 |

Abstract

This submission is normative text for the automated periodic anonymization and group anonymization. This normative text combines these anonymization schemes operation into a single scheme.

The periodic anonymization is presented in submission 11-24-579r0.

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

## *Note to the 802.11bi Editor: Please add the following new text to the 802.11bi draft specification. Renumber the clauses as appropriate.*

## 10.7.2.1 Introduction to frame anonymization

Three anonymization schemes for CPE STA and CPE AP to are defined:

* Individual anonymization allows a STA to schedule an event or periodic events to anonymize its assigned AID and MAC Header of individual addressed frames between the STA and the AP. The individual anonymization is defined in 10.7.2.3(group and individual anonymization).
* Group anonymization allows a group of STAs to schedule a joint event or periodic joint events to anonymize their assigned AIDs and MAC Headers of individual addressed frames between the STAs and the AP. The group anonymization is defined in 10.7.2.3(group and individual anonymization).
* Periodic anonymization allows 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 periodic anonymization is defined in 10.7.2.2(Periodic anonymization).

A CPE STA may use one or more anonymization schemes.

All anonymization schemes have the same anonymization mechanism for the MAC Header fields of the individually addressed frames between the STA and the AP as defined in XX.

The anonymization schemes operate independently. The anonymization events scheduled at different times are performed according to their TSF order.

A periodic anonymization event and an individual or a group anonymization event may be scheduled at the same time. In these cases, the MAC Header of the individually addressed frames between the STA and the AP is anonymized as defined in XX. The assigned AID is changed to the value signaled in individual or group obfuscation and the OTA AID value is obtained by applying the AID offset on the recently updated assigned AID value.

## 10.7.2.2 Periodic Frame anonymization

Periodic anonymization is optional for CPE AP and CPE STA. Periodic anonymization allows 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 10.7.2.3(Anonymization event). The OTA AID anonymization uses BSS specific offset as described in 10.7.2.4(OTA AID anonymization with BSS specific offset). An overview of the periodic anonymization is shown in Figure XX(Overview of periodic anonymization flow).



**Figure XX – Overview of periodic anonymization flow.**

A CPE AP advertises support for periodic anonymization in Beacon and Probe Response frames it transmits by setting value 1 to the Periodic Anonymization Supported field of the Enhanced Privacy Capabilities element.

Pseudorandom offset: TBD.

## 10.71.2.2.1 Periodic anonymization setup

A CPE STA may signal use of periodic anonymization by setting the Periodic Anonymization Activated field of the Enhanced Privacy element in the (Re)Association Request frame.

If a CPE AP, that supports periodic anonymization, receives a (Re)Association Request frame with the Periodic Anonymization field of the Enhanced Privacy element equal to value 1, then the AP shall use periodic anonymization in the association with the STA, if the AP accepts the association. The association is accepted by transmitting a (Re)Association Response frame with Enhanced Privacy element including the Periodic Anonymization field and the Periodic Anonymization Activated 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 periodic anonymizing STAs as described in 10.7.2.4(OTA AID anonymization with BSS specific offset).

## 10.7.2.2.2 Anonymization event

All periodic anonymizing 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 epochs of one or multiple TBTT(s).

In order to mark the beginning of each new epoch, the AP increases the Anonymization Event Number value. The Current Anonymization Number field in the Periodic Anonymization field of the Enhanced Privacy Element of the (Re)Association Response frame contains the Anonymization Number of the previous periodic anonymization event.

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 *dot11PeriodicAnonymizationTransitionTime* 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 *dot11PeriodicAnonymizationTransitionTime* after the epoch.

## 10.7.2.2.3 OTA address collision avoidance

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, periodic anonymization 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.

## 10.7.2.2.4 OTA AID anonymization with BSS specific offset

The AP shall assign an AID value to periodically anonymizing 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 periodic anonymization. The periodically anonymizing 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 Anonymization Event Number (6 octets)
* The eleven (11) least significant bits of the encrypted cipher text are used as AID\_Offset.

NOTE, the assigned AID of the CPE STA may be changed by using other anonymization schemes.

## 10.7.2.2.5 Concurrent operation of multiple anonymization schemes

A CPE STA may setup an individual or group specific anonymization event when it has periodic anonymization ongoing.

All anonymization schemes have the same anonymization mechanism for the MAC Header fields of the individually addressed frames between the STA and the AP as defined in XX. The individual or group anonymization event changes the assigned AID value, while the periodic anonymization applies the BSS specific offset to the AID value as described in 10.7.2.4(OTA AID anonymization with BSS specific offset).

The anonymization schemes operate independently. The anonymization events scheduled at different times are performed according to their TSF order. The anonymization events scheduled at the same time anonymize the MAC Header of the individually addressed frames between the STA and the AP as defined in XX and change the assigned AID value to the value signaled in individual or group obfuscation and apply AID offset to the new changed assigned AID value.

## 10.7.2.3 Group and individual anonymization

A CPE STA that desires to use individual or group anonymization 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 participate to the epoch interval announced by the AP in the Periodic Anonymization element. 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.

## 9.x.1 Enhanced Privacy (EP) element

The Enhanced Privacy (EP) element signals in (re)association request and response frames the privacy protection mode and its parameters.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element Id | Length | Element Id Extension  | EP Control  | Periodic Anonymization  | Current Anonymization Number | Participating STAs |
| Octets:  | 1 | 1 | 1 | 2 | 0 or 4 | 0 or 6 | 0 or 3 |

## Figure -XX Enhanced Privacy (EP) element

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Periodic Anonymization Activated | STA-Specific Setting | Reserved |
| Bits: | 1 | 1 | 14 |

## Figure XX – EP Control field

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

The Periodic Anonymization Activated field is set to 1 to signal that the STA uses periodic anonymization and set to 0 otherwise.

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 | Anonymization Epoch | Next Anonymization | Reserved |
| Bits: | 11 | 11 | 4 | 4 | 2 |

## Figure XX – Periodic Anonymization element

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 Anonymization Epoch field contains the number of TBTTs -1 between periodic anonymization events. Value 0 signals that periodic anonymization event is every TBTT.

The Next Anonymization field signals number of TBTTs until the next anonymization. Value 0 signals that the next anonymization is performed at the next TBTT.

The Current Anonymization Number field signals the anonymization number used in the last periodic anonymization.

The Participating STAs field is present when the STA-specific setting bit in the EP Control field is set, and signals the number of STAs currently participating to the periodic anonymization scheme 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 scheme without STA\_specific settings.

## 9.x.2 Enhanced Privacy Capabilities element

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

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

## Figure -XX Enhanced Privacy Capabilities element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Periodic Anonymization Supported  | STA-Specific Setting | Group Epoch Supported |  Reserved |
| Bits: | 1 | 1 | 1 | 13 |

## Figure -XX EP Capabilities field

The Periodic Anonymization Supported field is set to 1 to signal that AP supports periodic anonymization. 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.

The Group Epoch Supported field is set to 1 to signal that AP supports Group Epochs.

## 9.x.3 otaMAC collision warning element

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

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.

dot11PeriodicAnonymizationTransitionTime 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}