IEEE P802.11
Wireless LANs

|  |
| --- |
| Establishing frame anonymization parameter sets text for 11bi |
| Date: 2024-07-31 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

Abstract

This submission proposes comments resolution of CID 1002 received for TGbi Draft 0.4:

We propose draft specification text for 10.71.3 (Establishing frame anonymization parameter sets) in TGbi draft D0.4.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Added rationale for proposed mechanism. No change to content

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause**  | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1002 | Thomas Handte | 10.71.3 | 58.11 | There is a TBD | Please describe the details. | Revised, Agree in principle:Document 1394r0 account for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1002 |

**Proposed spec text:**

***TGbi editor: Apply the following changes to 9.4.2.340 OTA MAC Collision Warning element. The baseline for this text is 11-24-1291-02-00bi-ota-collision-warning-fixes.***

* OTA MAC Collision Warning element (#604r11) (#1284, #1285)

The OTA MAC Collision Warning element (#1286) is used when an OTA MAC (#1288) address expected to be used by the by a non-AP EDP MLD in an upcoming epoch is calculated to collide with the MAC address of another STA (#1361).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Collision Status | Link ID Info | Colliding Epoch | EDP\_STA\_MAC\_Seed |
| Octets: | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

* OTA MAC Collision Warning element

The Link ID Info field is defined in 9.4.1.76 (Link ID Info field) (11be).

The Collision Status field indicates the intent of the OTA MAC Collision Warning element. The field takes value 0 when sent by the AP MLD, and values 1 or 2 when sent by the EDP non-AP MLD in response to the AP MLD OTA MAC Collision Warning action frame (#1141, #1291). Table 9-401h lists the possible values and their meaning. (#1291)

* OTA MAC Collision Warning values

|  |  |
| --- | --- |
| Collision Status field value | Meaning |
| 0 | AP MLD signals collision risk to the non-AP MLD and suggest a remediation action to skip the OTA MAC intended for one or more epochs where collision risk is expected |
| 1 | Non-AP MLD acknowledges collision warning message and will take suggested action |
| 2 | Non-AP MLD acknowledges collision warning message but will not take suggested action |
| 3-255 | Reserved (#1142) |

The Colliding Epoch field indicates the future epoch at which MAC collision is likely to occur. The value is indicated in units of epochs. A value of 1 indicates the next epoch (#1292).

The Colliding Epoch field identifies the epoch at which an OTA MAC collision is avoided by applying the OTA MAC Collision Warning element. The value is indicated in units of epochs relative to the epoch in which the OTA MAC Collision Warning element is transmitted. A value of 0 indicates that the EDP\_STA\_MAC\_Seed is an initial value for EDP\_STA\_MAC\_Seed(Link ID Info). A value of x indicates the next epoch after the epoch in which the OTA MAC Collision Warning element is transmitted

The EDP\_STA\_MAC\_Seedfield indicates the value to be assigned to EDP\_STA\_MAC\_Seed(Link ID Info) at the time indicated by the Colliding Epoch field,to mitigate the OTA MAC address collision.

***TGbi editor: Replace the text in 10.71.2.6 OTA MAC address collision avoidance with the following. The baseline for this text is Draft P802.11bi\_D0.4.***

**10.71.2.6. OTA MAC address collision avoidance** **mechanism**

The OTA MAC address collision avoidance mechanism shall be applied for all CPE non-AP MLD for which MAC header anonymization is negotiated during association or re-association.

The OTA MAC address collision avoidance mechanism shall be applied on each link independently of the OTA MAC address collisions avoidance mechanism applying on other links. The description in this clause describes the (per-link) OTA MAC address collision avoidance mechanism is applied on any link,.

The CPE AP MLD and a CPE non-AP MLD shall maintain a parameter EDP\_STA\_MAC\_Seed(Link ID Info) for each setup link with Link ID Info (see 9.4.1.76 (Link ID Info field)) identifying the link.

NOTE—The set of setup links of a non-AP MLD can change over time.

NOTE—The parameter EDP\_STA\_MAC\_Seed(Link ID Info) is an input to the computation of the EDP STA MAC for the corresponding setup link. If one value of EDP\_STA\_MAC\_Seed(Link ID Info) produces in a value for EDP STA MAC which result an OTA MAC address collision, then (with very high probability) there is another value of EDP\_STA\_MAC\_Seed(Link ID Info) which produces a value for EDP STA MAC does not result in an OTA MAC address collision.

The (per-link) OTA MAC address collision avoidance mechanism comprises the CPE AP MLD managing the value of EDP\_STA\_MAC\_Seed(Link ID Info) for each CPE non-AP MLD set up on the link, to ensure that there are never OTA MAC address collisions on the link. The CPE AP MLD initializes and subsequently changes the value of EDP\_STA\_MAC\_Seed(Link ID Info) of a CPE non-AP MLD by sending an OTA MAC Collision Warning element (see 9.4.2.340 (OTA MAC Collision Warning element)) to the CPE non-AP MLD.

The CPE AP MLD shall transmit an OTA MAC Collision Warning in the (Re)Association Response frame (see 35.3.5 (ML (re)setup)) providing a new initial value of EDP\_STA\_MAC\_Seed(Link ID Info) for every setup link resulting from ML (re)setup. In this case, the Colliding Epoch field shall be set to 0 (initial value).

If a CPE non-AP MLD receives an OTA MAC Collision Warning element in the (Re)Association Response frame with

* Collision Status field set to 0,
* Link ID Info field indicating a link which has been requested by the CPE non-AP MLD in the (Re)Association Reqeuest frame and accepted by the CPE AP MLD in the (Re)Association Response frame, and
* Colliding Epoch field set to 0 (initial value),

then

* the CPE non-AP MLD shall set EDP\_STA\_MAC\_Seed(Link ID Info) to the value of the EDP\_STA\_MAC\_Seed field of the OTA MAC Collision Warning element, and
* the CPE non-AP MLD shall not return a corresponding OTA MAC Collision Warning.

The CPE AP MLD shall transmit an OTA MAC Collision Warning in the Link Reconfiguration Response frame (see 35.3.6.4 (Link reconfiguration to the setup links)) providing an initial value of EDP\_STA\_MAC\_Seed(Link ID Info) for every setup link added by multi-link reconfiguration. In this case, the Colliding Epoch field shall be set to 0 (initial value).

If a CPE non-AP MLD receives an OTA MAC Collision Warning element in the Link Reconfiguration Response frame with

* Collision Status field set to 0,
* Link ID Info field indicating a link whose addition has been accepted by the CPE AP MLD in the Link Reconfiguration Response frame, and
* Colliding Epoch field set to 0 (initial value),

then

* the CPE non-AP MLD shall set EDP\_STA\_MAC\_Seed(Link ID Info) to the value of the EDP\_STA\_MAC\_Seed field of the OTA MAC Collision Warning element, and
* the CPE non-AP MLD shall not return a corresponding OTA MAC Collision Warning.

The CPE AP MLD may transmit an OTA MAC Collision Warning element in an OTA MAC Collision Warning action frame that provides a new value of EDP\_STA\_MAC\_Seed(Link ID Info) for a setup link which comes into effect at the start of a future epoch. In this case, the Colliding Epoch field shall be set to a value of 1 or greater (indicating a future epoch).

If a CPE non-AP MLD receives an OTA MAC Collision Warning element in the Link Reconfiguration Response frame with

* Collision Status field set to 0,
* Link ID Info field indicating a setup link, and
* Colliding Epoch field set to a value of 1 or greater (indicating a future epoch),

then

* The CPE non-AP MLD shall send a response with an OTA MAC Collision Warning element with Collision Status field set to 1, and
* At the start of the identified epoch, the CPE non-AP MLD shall set EDP\_STA\_MAC\_Seed(Link ID Info) to the value of the EDP\_STA\_MAC\_Seed field of the OTA MAC Collision Warning element.

In all other scenarios, the EDP\_STA\_MAC\_Seed(Link ID Info) shall continue to take the most recently value set by a OTA MAC Collision Warning element.

***TGbi editor: Apply the following changes to 10.71.3 (Establishing frame anonymization parameter sets). The baseline for this text is Draft P802.11bi\_D0.4.***

* Establishing frame anonymization parameter sets

This subclause describes how an AP MLD and associated non-AP MLD establish the FA parameter set for each EDP epoch for the non-AP MLD.

The non-AP MLD and AP MLD establish(#Ed) the EDP epochs used for frame anonymization as described in 10.71.2 (EDP epoch operation)(#Ed).

* The generation of EDP\_STA\_MAC values is defined in 10.7.3.1 (Generating EDP\_STA\_MAC).
* The generation of the set of EDP\_SN\_offset values is defined in 10.7.3.2 (Generating EDP\_SN\_offset).
* The generation of the set of EDP\_PN\_offset values is defined in 10.7.3.3 (Generating EDP\_PN\_offset).

#### Generating EDP\_STA\_MAC

For a given EDP Epoch, and a given Link ID Info the value of EDP\_STA\_MAC for the corresponding setup link is generated according to the following algorithm:

EDP\_STA\_MAC( Link ID Info) ← KDF-*Hash-Length*( KDK, “EDP\_STA\_MAC”, Group ID || GTn || EDP\_STA\_MAC\_Seed(Link ID Info) || Link ID Info)

where:

EDP\_STA\_MAC(Link ID Info) is the value of EDP\_STA\_MAC used to identify the Affiliated STA of the non-AP MLD on the link identified by Link ID Info

Link ID Info is defined in 9.4.1.76 (Link ID Info field) (11be)

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))

KDK is the Key Derivation Key

Group ID is the identifier of the group EDP Epoch (see 9.4.2.339 (Enhanced Group Privacy Availability (EGPA) element)

GTn is the reference start time of the EDP Epoch (see 9.4.2.337 (Enhanced Data Privacy (EDP) element) )

EDP\_STA\_MAC\_Seed(Link ID Info) is used for OTA MAC collision avoidance (see 10.71.2.6. (OTA MAC address collision avoidance)).

*Length* is the total number of bits to derive and is equal to ( *MAC\_addr\_size* − 2)

*MAC\_addr\_size* is the number of bits in a MAC address and is equal to 48.

#### Generating EDP\_SN\_offset

For a given EDP Epoch and a given sequence number space supported by the association between the non-AP MLD and AP MLD, the set of value(s) of EDP\_SN\_offset transmitted by the non-AP MLD and AP MLD are generated according to the following algorithm:

EDP\_SN\_offset\_block← KDF-*Hash-Length*( KDK, “EDP\_SN\_offset\_block”, *sns\_id,* GTn)

*start* ← 0

*finish* ← ( *ctr\_size* − 1 )

**do** *tx* in {“non-AP MLD”, “AP MLD”}

**do** *ctr\_index* = 0 to ( *ctr\_num* − 1 )

EDP\_SN\_offset(*tx*, *sns\_index*, *ctr\_index*) ← EDP\_SN\_offset\_block[ *finish* : *start* ]

*start* ← ( *start* + *ctr\_size* )

*finish* ← ( *finish* + *ctr\_size* )

**od**

**od**

where:

EDP\_SN\_offset\_block is the KDF output subsequently partitioned into the values of EDP\_SN\_offset for the counters in a given sequence number space for both the non-AP MLD and AP MLD

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))

KDK is the Key Derivation Key

*sns\_id* is the Sequence Number Space Identifier in ASCII for the sequence number space as defined in Table 10-5 (Transmitter sequence number spaces); e.g., “SNS2” for individually addressed QoS Data

GTn is the reference start time of the EDP Epoch (see 9.4.2.337 (Enhanced Data Privacy (EDP) element) )

*Length* is the total number of bits to derive and is equal to ( 2 × *ctr\_num* × *ctr\_size* )

*start* is a state variable identifying the bit position within EDP\_SN\_offset\_block where the value starts being copied to an EDP\_SN\_offset

*finish* is a state variable identifying the bit position within EDP\_SN\_offset\_block where the value finishes being copied to an EDP\_SN\_offset

*tx* identifies the transmitter for the sequence number space,

*ctr\_index* is an index to one of the counters in the sequence number space

*ctr\_num* is the number of counters in the sequence number space

EDP\_SN\_offset( *tx*, *sns\_index*, *ctr\_index* ) is the value of EDP\_SN\_offset used for frames transmitted by *tx* using the counter identified by *ctr\_index* in the sequence number space identified by *sns\_id*

*ctr\_size* is the number of bits in the counters of the sequence number space Table 10-x provides the values of *ctr\_num* and *ctr\_size* for the sequence number spaces defined in Table 10-5 (Transmitter sequence number spaces)

Table 10-x Sequence Number values for *ctr\_num* and *ctr\_size*

|  |  |  |  |
| --- | --- | --- | --- |
| **Sequence Number Space Identifier** | **Sequence Number Space** | *ctr\_num* | *ctr\_size* (in bits) |
| SNS1 | Baseline | TBD if an offset is needed for SNS1 |
| SNS2 | Individually addressed QoS Data | 16 | 12 |
| SNS3 | Time Priority Management | 16 | 12 |
| SNS4 | QMF | 4 | 10 |
| SNS5 | QoS (+)Null | Not applicable. SNS5 does not have a counter |
| SNS6 | Individually addressed PV1 Data frame | 8 | 12 |
| SNS7 | Individually addressed PV1 Management frame | 1 | 12 |
| SNS8 | Protected Fine Timing frame and Public Action LMR | TBD if an offset is needed for SNS8 |

#### Generating EDP\_PN\_offset

For a given EDP Epoch, the set of values of EDP\_PN\_offset transmitted by the non-AP MLD and AP MLD are generated according to the following algorithm:

EDP\_PN\_offset\_block ← KDF-*Hash-Length*( KDK, “EDP\_PN\_offset”, GTn)

*start* ← 0

*finish* ← ( *PN\_size* − 1 )

**do** *tx* in {“non-AP MLD”, “AP MLD”}

EDP\_PN\_offset( *tx* ) ← EDP\_PN\_offset\_block[ *finish* : *start* ]

*start* ← ( *start* + *PN\_size* )

*finish* ← ( *finish* + *PN\_size* )

**od**

where:

EDP\_PN\_offset\_block is the KDF output subsequently partitioned into the values of EDP\_PN\_offset for both the non-AP MLD and AP MLD

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))

KDK is the Key Derivation Key

GTn is the reference start time of the EDP Epoch (see 9.4.2.337 (Enhanced Data Privacy (EDP) element) )

*Length* is the total number of bits to derive and is equal to ( 2 × *PN\_size* ) = 96

*start* is a state variable identifying the bit position within EDP\_PN\_offset\_block where the value starts being copied to an EDP\_PN\_offset

*finish* is a state variable identifying the bit position within EDP\_PN\_offset\_block where the value finishes being copied to an EDP\_PN\_offset

*tx* identifies the transmitter for the sequence number space

EDP\_PN\_offset( *tx* ) is the value of EDP\_PN\_offset used for frames transmitted by *tx*

*PN\_size* is the number of bits in a Packet Number and is equal to 48

(#1002)