IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 Collision CRs  |
| Date: 2025-07-24 |
| 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:

Revisions:

* Rev 0: Initial version of the document.

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** |
| 1066 | 10.71.2.5 | 81.01 | This clause identies actions when an non-AP MLD's affilaited STA has an OTA MAC address that collides with another STA MAC address. However, there is no clarification of what to do if an AP MLD's MAC address collides with another STA's MAC address. | Provide mechanism to deal wit scenario where an AP MLD's MAC address collides with another STA's MAC address. | RevisedTGbi editor to make the changes shown in the latest version of 11-25/1372 under all headings that include CID 1066 |
| 752 | 9.4.2.347 | 61.20 | The STA signals its DS MAC value, but there is no mechanism to avoid that the MAC collides with an existing address | Specify what happens if the signaled DS MAC already exists (or at least the AP knows it to exist) on the DS | RevisedTGbi editor to make the changes shown in the latest version of 11-25/1372 under all headings that include CID 752 |
| 213 | 10.71.2.5 | 82.22 | The collision warning should have rules for BPE STAs collision avoidance. The BPE AP address collision and a non-AP BPE STA address collisions should be considered separately. | Please add rules for BPE address collisions. | RevisedTGbi editor to make the changes shown in the latest version of 11-25/1372 under all headings that include CID 213 |

TGBI Editor: please implement the changes herein marked in red.

**Discussion**

CID 1066, 752

Revised

Discussion:

In CPE-only mode, the AP does not change its MAC address. Therefore the AP MAC collides with a STA’s MAC only if the STA picks that MAC for one epoch. The BPE case is handled with CID 213 below.

Clause 10.71.2.5 (this comment) is about MAC address collision avoidance. The collision with the MAC of another AP known by the local AP is already considered in the text (the AP is a STA):

The text could do a better job removing the confusion between STA and “client”.

**10.71.2.5 OTA MAC address collision avoidance**

A CPE AP MLD and a CPE non-AP MLD anonymize selected OTA MAC header fields of individually addressed frames of the CPE affiliated STAs within EDP epochs.

A CPE AP MLD may calculate that the OTA MAC address that a CPE non-AP MLD is anticipated to use in a subsequent epoch **may cause a collision with the OTA MAC address of another CPE non-AP MLD(s) or another STA** in the ESS. When such a collision is detected, the CPE AP MLD shall send to the CPE non-AP MLD an OTA MAC Collision Notification(#123) frame before the epoch where the collision is anticipated to risk occurring and indicated in the Colliding Epoch field, instructing the non-AP MLD to apply the non-AP MLD specific epoch offset signaled in the AP MLD OTA MAC Collision Notification(#123, #Ed) frame to avoid address collision.(#557)

However, the collision with the MAC of the local AP, albeit obviously necessary, is not mentioned. The local clause can be improved, when the collision is future:

A CPE AP MLD and a CPE non-AP MLD anonymize selected OTA MAC header fields of individually addressed frames of the CPE affiliated STAs within EDP epochs.

A CPE AP MLD may calculate that the OTA MAC address that a CPE non-AP MLD is anticipated to use in a subsequent epoch may cause a collision with the OTA MAC address of another CPE non-AP MLD(s) or an AP or non-AP (#1066) ~~another~~ STA in the ESS. When such a collision is detected, the CPE AP MLD shall send to the CPE non-AP MLD an OTA MAC Collision Notification(#123) frame before the epoch where the collision is anticipated to risk occurring and indicated in the Colliding Epoch field, instructing the non-AP MLD to apply the non-AP MLD specific epoch offset signaled in the AP MLD OTA MAC Collision Notification(#123, #Ed) frame to avoid address collision.(#557)

There are also several possible collisoon points, in the lifetime of a session:



The non-AP MLD associates, then starts using the MAC scheme it derived with the AP. We may need to say somwhere that the STA will start spinning its MAC at the start of the next epoch after successful allocation to a group. 10.71.2.2 is the best clause for that purpose:

**10.71.2.2 EDP group operations**

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

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

The non-AP MLD may include in an encrypted (Re)Association Request frame an EDP element indicating the parameters for the EDP group it requests to join.

If no EDP element is included in the encrypted (Re)Association Request frame, or if the EDP element does not include information defining the parameters for the EDP group, the CPE non-AP MLD is assigned to the default EDP(#1012) group. The first EDP epoch of an EDP epoch sequence is EDP epoch number 0.

Within the EDP element sent in (Re)Association Request frames, the CPE non-AP MLD shall include a Minimum Epoch Pacing Parameters field, indicating the minimum epoch interval length supported by the CPE non-AP MLD. If the value resulting of the multiplication of the Epoch Interval Length field by the Epoch Interval Unit field included in the Minimum Epoch Pacing field is greater than the value resulting of the multiplication of the Epoch Interval Length field by the Epoch Interval Unit field for the default EDP group (group 0) or of any other EDP group already created, then the CPE non-AP MLD is not assigned to any EDP group at (re)association.(#1012)

NOTE 1—The CPE non-AP MLD might remain associated without FA and might request the creation of a new EDP group (through the EDP Epoch Request frame).

The CPE AP MLD, upon reception of the EDP element in an encrypted (Re)Association Request frame may assign the CPE non-AP MLD to the EDP group with parameters that best match the parameters requested. In all cases, the assigned EDP epoch interval length shall not be shorter than indicated in the Minimum Epoch Pacing Parameters field. Once assigned to an EDP group following successful association, the non-AP MLD activates FA parameters as specified in 10.71.3 (Establishing frame anonymization parameters set) to start exchanges in the BSS during the current epoch. (#1066)

The parameters of the assigned EDP group are returned to the CPE non-AP MLD through an EDP element in the (Re)Association Response frame. If no EDP element is included in the (Re)Association Response frame, the CPE non-AP MLD is not assigned to any EDP group.

The CPE non-AP MLD may request creation of a new EDP group by sending an EDP Epoch(#859) Request frame with Epoch Request field indicating "Create" and indicating the parameters for the EDP group to be created in the EDP Epoch Settings field.

The CPE AP MLD may create the new EDP group with the received parameters. Alternatively, the CPE AP MLD may allocate the CPE non-AP MLD to an already existing EDP group with similar parameters. This may be signalled to the CPE non-AP MLD in an EDP Epoch(#859) Response frame indicating in the Status field, SUCCESS\_SIMILAR\_EPOCH, and providing the EDP Epoch Settings field with the parameters of the EDP group.

NOTE 2—In this context, an EDP group with "similar parameters" refers to an existing EDP group whose epoch duration is equal or smaller than the one requested by the CPE non-AP MLD (i.e., most privacy-preserving). This choice is made while ensuring adherence to any pacing limits indicated in the Minimum Epoch Pacing Parameters field that the CPE non-AP MLD has specified in (Re)Association Request frame.

Once the CPE non-AP MLD is associated and has been assigned an EDP group, it may request to join a different EDP group. Information on the available EDP group(s) may be distributed periodically by the CPE AP MLD transmitting EDP Groups(#1011, #Ed) Parameter frames. To join a different EDP group, the CPE non-AP MLD sends an EDP Epoch Request frame, indicating "Join" in the Epoch Request field and providing the EDP Epoch Settings field indicating the parameters of the EDP group it requests to join.

If the CPE AP MLD can fulfill the request, it will include the CPE non-AP MLD in the new EDP group and remove it from the previous EDP group. The result of the operation is indicated to the CPE non-AP MLD through an EDP Epoch(#859) Response frame. This frame includes a Status field, "SUCCESS", indicating the operation result and an optional EDP Epoch Settings field to indicate the parameters of the newly joined EDP(#1012) group.

At any point in time, the CPE AP MLD may request the associated CPE non-AP MLD to transition to a different EDP group, by sending an EDP Epoch Assignment(#859) frame to the associated CPE non-AP MLD(#859) including the EDP Epoch Settings field with the parameters of the suggested EDP group. The CPE non-AP MLD may report the status of the operation by responding with an EDP Epoch(#859) Response frame. This operation allows the CPE AP MLD to reorganize the EDP groups in use. Following this reorganization, the resulting EDP groups should maintain the same level of restrictiveness or be even more restrictive, i.e., shorter epoch durations, while also respecting any pacing limits indicated in the Minimum Epoch Pacing Parameters field that the CPE non-AP MLD has specified in (Re)Association Request frame.

A CPE non-AP MLD may leave an EDP group at any time by sending an EDP Epoch(#859) Request frame indicating "Leave" in the Epoch Request field. Upon reception of this message, the CPE AP MLD shall remove the CPE non-AP MLD from the EDP group.

The STA may also pick as its first MAC the MAC of the AP or another AP, at auth/assoc time. This event could cause issues as the STA sends an authentication frame from a MAC that is already known. In the association request, the proposed DS MAC may be a differentiator.

Scenario table

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario index | Frame | OTA TA | DS MAC |
| 1 | Authentication  | No collision | N.A. |
| 2 | Authentication | Collision | N.A. |
| 3 | (Re)association | No collision | No collision |
| 4 | (Re)association | Collision | No Collision  |
| 5 | (Re)association | No collision | Collision |
| 6 | (Re)association | Collision | Collision |

Easiest cases first: 1 and 3, no issue, and the above apply.

Case 2: a known MAC attempts authentication. “Known” means that the AP knows the MAC as belonging to either another AP (scenario a) or another STA in the ESS (scenario b). Scenario a] occurs if the AP, through out-of-specification methods discovers neighboring APs and records their BSSID. The AP can reject the auth request with a reason code:

(802.11-2024) Table 9-80 – Status Codes

|  |  |  |
| --- | --- | --- |
| Status Code | Name | Meaning |
| 143 | GAS\_QUERY\_REQUEST\_TOO\_ LARGE | GAS query request is larger than thedot11GASQueryRequestLengthLimit value. |
| 144 | ADDRESS\_2\_INVALID | Authentication frame or (re)association request denied because of an invalid SA/TA (#1066) |
| 145-65 535 |  | Reserved  |

Scenario b] is more difficult. There is no easy mechanism for the AP to know if the STA MAC is duplicate or not (may be duplicate, may be a STA roaming from elsewhere, may be a STA that had an internal reset, etc.)

The Standard does not solve this case today, even for STAs that send an authentication frame with the MAC of an already associated STA. Some implementations act upon such frame (e.g., accept and terminate the other one, or silently drop the new one). We may not want to invent new behavior for a problem that was coinciously left unaddressed.

Case 4: here again, scenarios a] and b] are possible. Scenario a]: the same message above solves this case.

Scenario b]: the colliding MAC may be another STA in another BSS, and the AP cannot know if it is a duplicate or a roam. No Standard action is possible/desirable (some implementations may have specific actions). The MAC may also be another STA in the AP BSS. This case solved with 802.11w, for a reassociation request coming from an already associated STA (in 802.11-2024 11.3.5.3). In essence, if a (re)assoc frame comes from a MAC that is already associated, the AP rejects the (re)assoc frame with a status code 30 (rejected temporarily, try again later), with an association comeback time IE with the value for the next attempt delay. We do not need a new action.

Case 5: this is a DS MAC collision, to be solved (with CID 752).

In case 5, a new MAC (no collision) undergoes authentication, then association, but in the association request sends an already existing DS MAC (i.e. the MAC of an already active system on the AP memory).

Easiest fix is to ask the STA to generate a new one.

(802.11-2024) Table 9-80 – Status Codes

|  |  |  |
| --- | --- | --- |
| Status Code | Name | Meaning |
| 143 | GAS\_QUERY\_REQUEST\_TOO\_ LARGE | GAS query request is larger than thedot11GASQueryRequestLengthLimit value. |
| 144 | ADDRESS\_2\_INVALID | Authentication frame or (re)association request denied because of an invalid SA |
| 145 | DS\_MAC\_INVALID | DS\_MAC is invalid or already in use. (#752) |
| 146-65 535 |  | Reserved  |

If the STA is new and collides its DS MAC by chance, then it spins up a new DS MAC and sends a new assoc rquest. If by any chance the STA is genuine (it knows that it had that same DS MAC before, it is trying to come back and is somehow just acting up), it can use the SA query mechanism to validate its already existing association with the AP.

**12. 16.5 IEEE 802.1X authentication utilizing Authentication frames**

If an AP sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field in the RSNXE that it transmits to 1, then a non-AP STA (originator) with dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true may signal its Supplicant to authenticate with the AP (responder) using IEEE Std 802.1X-2020 utilizing Authentication frames.

If any AP affiliated with an AP MLD sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field in the RSNXE that it transmits to 1, then a non-AP MLD (originator) with dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true may signal its Supplicant to authenticate with the AP MLD (responder) using IEEE Std 802.1X-2020 utilizing Authentication frames by transmitting the Authentication frames to the AP through a non-AP STA affiliated with the non-AP MLD.

When the originator is a non-AP MLD and the responder is an AP MLD, the RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer.

If an originator chooses to initiate IEEE 802.1X authentication utilizing Authentication frames, it first selects an IEEE 802.1X AKM that is supported by the responder.

The originator then shall construct(#676) the first Authentication frame of the exchange as follows:

Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).

Authentication Transaction Sequence Number field is set to 1.

The Encapsulation field carries an EAPOL PDU.

Include the AKM Suite Selector element indicating the selected IEEE 802.1X AKM.

The originator sends the first Authentication frame to the responder.

Upon receiving the first Authentication frame, the responder shall(#676):

Validate(#676) that the AKM indicated in AKM Suite Selector element is an IEEE 802.1X AKM.

Validate(#676) that the selected IEEE 802.1X AKM indicated in AKM Suite Selector element is supported. Otherwise processing status is set to STATUS\_INVALID\_AKMP.

Validate(#1066) that the Authentication frame address 2 is not a known BSSID or invalid.

Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

The responder then shall construct(#676) the second Authentication frame of the exchange as follows:

Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).

Authentication Transaction Sequence Number field is set to 2.

Status Code field indicates the processing status.

The Encapsulation Length field indicates 0 if the status is set to STATUS\_INVALID\_AKMP or ADDRESS\_2\_INVALID. (#1066)

The Encapsulation field (if present) carries an EAPOL PDU.

Include(#676) the AKM Suite Selector element indicating the same IEEE 802.1X AKM indicated in the first Authentication frame.

Once the processing is complete, the responder sends the second Authentication frame to the originator. If the processing status returned in the frame was not SUCCESS, the responder shall terminate the authentication.

Upon receiving the second Authentication frame, the originator shall(#676):

Validate(#676) that the AKM indicated in AKM Suite Selector element is the same as the one indicated in the first Authentication frame. Otherwise,(#676) processing status is set to STATUS\_INVALID\_AKMP.

Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

The originator then shall construct(#676) the third Authentication of the exchange as follows:

Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).

Authentication Transaction Sequence Number field is set to 3.

Status Code field indicates the processing status.

The Encapsulation Length field indicates 0 if the status is set to STATUS\_INVALID\_AKMP.

Once the processing is complete, the originator sends the third Authentication frame to the responder. If the processing status returned in the frame was not SUCCESS, the originator shall terminate the authentication.

Upon receiving the Authentication frame with Authentication Transaction Sequence Number field set to a value that(#848) is larger than or equal to 3, the originator or the responder:

Extract(#676) an EAPOL PDU from the Encapsulation field, and process(#676) it.

The originator or the responder then shall construct(#676) the Authentication frame of the exchange in response to the Authentication frame with Authentication Transaction Sequence Number field set to a value that(#848) is larger than or equal to 3, as follows:

Authentication Algorithm Number field is set to 8 (IEEE 802.1X authentication).

Authentication Transaction Sequence Number field is set to the value of the Authentication Transaction Sequence Number field of the Authentication frame being responded to(#848, #Ed) +1.

Status Code field indicates the processing status.

The Encapsulation field (if present) carries an EAPOL PDU.

NOTE —The number of Authentication frame exchanges depends on the EAP method in use.(#Ed)

Once the processing is complete, the originator or the responder sends the Authentication frame in response to the Authentication frame with Authentication Transaction Sequence Number field set to a value that is larger than or equal to 3,(#848) to its peer (if needed by the EAP method). If the processing status returned in the frame was not SUCCESS, the originator or the responder shall terminate the authentication.

**12.16.6. (Re)Association Request/Response Frame Encryption**

This subclause defines rules to encrypt the Frame Body field of the (Re)Association Request/Response frame and to include a DS MAC Address element in the encrypted (Re)Association Request frame.

An EDP STA that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall set the MFPC subfield in the RSN Capabilities field in the RSNE to 1.(#167)

**12.16.6.1 Non-MLO procedure**(#945)

An EDP non-AP STA that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 (see 12.16.8 (Key derivation with Authentication frame exchange) and 12.16.9 (Enhanced Data Privacy Key Exchange)).(#849)

An EDP non-AP STA shall randomize its STA MAC address during a BSS transition if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP STA and a temporal key (TK) is derived during Authentication frame exchange between the EDP non-AP STA and an EDP AP, the EDP non-AP STA shall encrypt the (Re)Association Request frame transmitted to the EDP AP using the TK and the pairwise cipher indicated in the Authentication frame exchange.

If the FT initial mobility domain association is used, then the EDP non-AP STA shall include the MDE and the FTE in the (Re)Association Request frame. MDE and the FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.3 (FT initial mobility domain association(#176)). (#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Request frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

For the RSNE included in the (Re)Association Request frame, other than the Length field, the PMKID Count field and the PMKID List field, shall be identical to those in the RSNE present in the first Authentication frame.(#176)

If the FT protocol is used, then the EDP non-AP STA shall not calculate the MIC for the MIC field of the FTE in the Reassociation Request frame. The length of the MIC field of the FTE in the Reassociation Request frame shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

If dot11DSMACAddressActivated is true and the EDP AP sets the DS MAC Address Support field in the RSNXE to 1, the EDP non-AP STA shall include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP for the mapping to the DS.

The EDP non-AP STA may randomize the DS MAC address. To construct a random DS MAC address, the EDP non-AP STA shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP STA shall use the same DS MAC address for the duration of its connection across an ESS.

The EDP AP shall decrypt the (Re)Association Request frame received from the EDP non-AP STA using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP AP shall discard the frame.(#139)

The EDP AP MLD shall validate that the DS MAC in the (re)association request is not already known by the AP MLD as actively used by another device. If the DS MAC is already used, the AP MLD shall respond with an association response with status code DS\_MAC\_INVALID. (#752)

If the FT initial mobility domain association is used, then the FTE and the MDE in the (Re)Association Request frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.3 (FT initial mobility domain association(#176)). If the MDE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_MDE. If the FTE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_FTE.(#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Request frame is checked to be included and calculated according to the procedures of 12.7.1.6.4 (PMK-R1). If the check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_PMKID.(#176)

The EDP AP shall verify that the RSNE fields other than the Length field, the PMKID Count field and the PMKID List field in the (Re)Association Request frame is identical to the RSNE fields included in the first Authentication frame. The EDP AP shall also verify that the RSNXE in the (Re)Association Request frame is identical to the RSNXE included in the first Authentication frame. If the validation fails, the EDP AP shall reject the association.(#176)

If the FT initial mobility domain association is used, then EDP AP shall include the MDE, the FTE, TIE[ReassociationDeadline], and TIE[KeyLifetime] in the (Re)Association Response frame. The MDE and the FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.3 (FT initial mobility domain association(#176)). The reassociation deadline timeout is set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime].(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

If the FT protocol is used, then the EDP AP shall not wrap the Key field of the subelements in the FTE in the Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE in the Reassociation Response frame. The length of the MIC field of the FTE in the Reassociation Response frame shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

The EDP AP shall encrypt the (Re)Association Response frame transmitted to the EDP non-AP STA in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated in the Authentication frame exchange.

If the FILS authentication protocol and the FT protocol are not used, the EDP AP shall include a Key Delivery element in the (Re)Association Response frame.(#677)

If a Key Delivery element is included in the (Re)Association Response frame, the EDP AP shall construct the Key Delivery element indicating the current GTK PN in the RSC subfield, with the GTK KDE, with the IGTK KDE if management frame protection is enabled, with the BIGTK KDE if beacon protection is enabled, and with the WIGTK KDE if WUR frame protection is enabled.

The EDP non-AP STA shall decrypt the (Re)Association Response frame received from the EDP AP using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP non-AP STA(#678) shall discard the frame.(#139)

If the FT protocol is not used, the FT initial mobility domain association is not used,(#176) and in the (Re)Association Response frame the RSNE fields are not identical to the corresponding RSNE fields in the Beacon or(#680) Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response.(#679)

If the FT protocol is not used,(#176) the EDP non-AP STA shall verify that the RSNXE included in the (Re)Association Response frame(#176) is identical to the RSNXE included in the Beacon or(#680) Probe Response frames received from the EDP AP. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP STA shall discard the response.(#679)

If the FT initial mobility domain association is used, then the FTE and the MDE in the (Re)Association Response frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.3 (FT initial mobility domain association(#176)). If the check fails, the EDP non-AP STA shall discard the response.(#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Response frame is checked to be included and identical to the value that is sent in the Association Request frame. If the check fails, the EDP non-AP STA shall discard the response.(#176)

If the FT initial mobility domain association is used and in the (Re)Association Response frame the RSNE fields other than the Length field, the PMKID Count field and the PMKID List field are not identical to the corresponding RSNE fields in the Beacon or Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response.(#176)

If IEEE 802.1X Authentication utilizing Authentication frame is used, and the RSN capabilities fields of the RSNE received in the (Re)Association Response frame is not identical to the RSN capabilities fields of the RSNE received in the second Authentication frame, the EDP non-AP STA shall discard the response.(#176)

On a successful (re)association,

The EDP non-AP STA shall process the Key Delivery element in the (Re)Association Response frame if present.

The EDP non-AP STA shall install the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true.

The EDP AP and the EDP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)).

If the DS MAC Address element is included in the (Re)Association Request frame, the EDP non-AP STA shall use the indicated DS MAC address rather than the MAC address of the EDP non-AP STA for the EDP non-AP STA to the EDP AP mapping to the DS.(#681)

If the DS MAC Address element is included in the (Re)Association Request frame, the EDP AP shall process the DS MAC Address element and use the indicated DS MAC address rather than the MAC address of the EDP non-AP STA to establish the EDP non-AP STA to the EDP AP mapping to the DS.(#681)

NOTE 1—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP STA are set to the DS MAC address, which is the identity of the non-AP STA known by the DS.

On a failed (re)association, the established PTKSA shall be irretrievably deleted.

**12.16.6.2 MLO procedure**

A non-AP MLD that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP MLD if APs affiliated with the EDP AP MLD set the (Re)Association Frame Encryption Support field in the RSNXE to 1 (see 12.16.8 (Key derivation with Authentication frame exchange) and 12.16.9 (Enhanced Data Privacy Key Exchange)).(#850)

NOTE 1—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

An EDP non-AP MLD shall randomize the STA MAC addresses of its affiliated STAs and its MLD MAC address during a BSS transition if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP MLD and a TK is derived during Authentication frame exchange between the EDP non-AP MLD and an EDP AP MLD, the EDP non-AP MLD shall encrypt the (Re)Association Request frame transmitted to the EDP AP MLD using the TK and the pairwise cipher indicated in the Authentication frame exchange.(#682)

If the FT initial mobility domain association is used, then the EDP non-AP MLD shall include the MDE and the FTE in the (Re)Association Request frame. The MDE and the FTE shall be the same as the ones in the second Authentication frame as defined in 12.16.8.3 (FT initial mobility domain association(#176)).(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Request frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK-R1).(#176)

For the RSNE included in the (Re)Association Request frame, other than the Length field, the PMKID Count field and the PMKID List field, shall be identical to the RSNE fields in the first Authentication frame.(#176)

The (Re)Association Request frame shall:

Have the Address 1 field equal to the Address 1 field of the Authentication frame used by the non-AP MLD to establish the PTKSA.(#683, #Ed)

Have the Address 2 field equal to the Address 2 field of the Authentication frame used by the non-AP MLD to establish the PTKSA.(#683, #Ed)

Include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP MLD for the mapping to the DS if dot11DSMACAddressActivated is true and the APs affiliated with the EDP AP MLD set the DS MAC Address Support field in the RSNXE to 1.

If the FT protocol is used, then the EDP non-AP MLD shall not calculate the MIC for the MIC field of the FTE in the Reassociation Request frame. The length of the MIC field of the FTE in the Reassociation Request frame shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

An EDP non-AP MLD may randomize its DS MAC address. To construct a random DS MAC address, the EDP non-AP MLD shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP MLD shall use the same DS MAC address for the duration of its connection across an ESS.

The EDP AP MLD shall decrypt the (Re)Association Request frame received from the EDP non-AP MLD using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP AP MLD shall discard the frame.(#139)

The EDP AP MLD shall validate that the DS MAC in the (re)association request is not already known by the AP MLD as actively used by another device. If the DS MAC is already used, the AP MLD shall respond with an association response with status code DS\_MAC\_INVALID. (#752)

If the FT initial mobility domain association is used, then the FTE and the MDE in the (Re)Association Request frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.3 (FT initial mobility domain association(#176)). If the MDE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_MDE. If the FTE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_FTE.(#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Request frame is checked to be included and calculated according to the procedures of 12.7.1.6.4 (PMK-R1). If the check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_PMKID.(#176)

The EDP AP MLD shall verify that the RSNE fields other than the Length field, the PMKID Count field and the PMKID List field in the (Re)Association Request frame is identical to the RSNE fields included in the first Authentication frame. The EDP AP MLD shall also verify that the RSNXE in the (Re)Association Request frame is identical to the RSNXE included in the first Authentication frame. If the validation fails, the EDP AP MLD shall reject the association.(#176)

If the FT initial mobility domain association is used, then EDP AP MLD shall include the MDE, the FTE, TIE[ReassociationDeadline], and TIE[KeyLifetime] in the (Re)Association Response frame. The MDE and the FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.1a (FT initial mobility domain association). The reassociation deadline timeout is set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime].(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 12.7.1.6.4 (PMK-R1).(#176)

If the FT protocol is used, then the EDP AP MLD shall not wrap the Key field of the subelements in the FTE in the Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE. The length of the MIC field shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

The EDP AP MLD shall encrypt the (Re)Association Response frame transmitted to the EDP non-AP MLD in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated in the Authentication frame exchange.

If the FILS authentication protocol and the FT protocol are not used, the EDP AP MLD shall include a Key Delivery element in the (Re)Association Response frame.(#677)

If a Key Delivery element is included in the (Re)Association Response frame, the EDP AP MLD shall construct the Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled, and with the PGTK KDE if the Group EDP Epoch Supported field in the RSNXE is set to 1 by both the APs affiliated with the AP MLD and the non-AP MLD.(#685)

The EDP non-AP MLD shall decrypt the (Re)Association Response frame received from the EDP AP MLD using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), the EDP non-AP MLD shall discard the frame.(#139)

If the FT protocol is not used, the FT initial mobility domain association is not used,(#176) and in the (Re)Association Response frame the RSNE fields corresponding to each link are not identical to the corresponding RSNE fields of the link in the Beacon or(#680) Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD, the EDP non-AP MLD shall discard the response.(#679)

If the FT protocol is not used,(#176) the EDP non-AP MLD shall verify that the RSNXE corresponding to each link in the (Re)Association Response frame(#176) is identical to the corresponding RSNXE of the link in the Beacon or(#680) Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP MLD shall discard the response.(#679)

If the FT initial mobility domain association is used, then the FTE and the MDE in the (Re)Association Response frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.3 (FT initial mobility domain association(#176)). If the check fails, the EDP non-AP MLD shall discard the response.(#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Response frame is checked to be included and identical to the value that is sent in the (Re)Association Request frame. If the check fails, the EDP non-AP MLD shall discard the response.(#176)

If the FT initial mobility domain association is used and in the (Re)Association Response frame the RSNE fields other than the Length field, the PMKID Count field and the PMKID List field corresponding to each link are not identical to the corresponding RSNE fields of the link in the Beacon or Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD, the EDP non-AP MLD shall discard the response.(#176)

If IEEE 802.1X Authentication utilizing Authentication frame is used, and the RSN capabilities fields of the RSNE received in the (Re)Association Response frame is not identical to the RSN capabilities fields of the RSNE received in the second Authentication frame, the EDP non-AP MLD shall discard the response.(#176)

On successful (re)association,

The EDP non-AP MLD shall process the Key Delivery element in the (Re)Association Response frame if present.

The EDP non-AP MLD shall install the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and PGTK if the Group EDP Epoch Supported field in the RSNXE is set to 1 by both the APs affiliated with the AP MLD and the non-AP MLD.(#685)

The EDP AP MLD and the EDP non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)).

If the DS MAC Address element is included in the (Re)Association Request frame, the EDP non-AP MLD shall use the indicated DS MAC address rather than the MLD MAC address of the non-AP MLD for the EDP non-AP MLD to the EDP AP MLD mapping to the DS.(#681)

If the DS MAC Address element is included in the (Re)Association Request frame, the EDP AP MLD shall process the DS MAC Address element and use the indicated DS MAC address rather than the MLD MAC address of the EDP non-AP MLD to establish the EDP non-AP MLD to the EDP AP MLD mapping to the DS.(#681)

NOTE 2—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP MLD are set to the DS MAC address, which is the identity of the non-AP MLD known by the DS.

On failed (re)association, the established PTKSA shall be irretrievably deleted.

CID 213

Revised

**10.71.2.5 OTA MAC address collision avoidance**

An EDP (CPE or BPE) (#213) AP MLD and an EDP (CPE or BPE) non-AP MLD anonymize selected OTA MAC header fields of individually addressed frames they transmit to each other (#555, 121).

An EDP ~~CPE~~ AP MLD shall determine whether the OTA MAC address that an EDP ~~CPE~~ non-AP MLD will use in a subsequent epoch will cause a collision with the OTA MAC address of another non-AP MLD(s) or another STA (#556, 92, 288) on a link (#1067, 214). When such a collision risk is anticipated with the OTA MAC of a non-CPE or non-BPE STA or non-AP MLD (#91, 350), the EDP ~~CPE~~ AP MLD shall send to the EDP ~~CPE~~ non-AP MLD an OTA MAC Collision Notification (#558) frame before the epoch when (#349) the collision is anticipated to risk occurring and indicated in the Colliding Epoch field, instructing the EDP ~~CPE~~ (#91) non-AP MLD to apply the non-AP MLD specific FA parameters (#1068) epoch offset signaled in the AP MLD OTA MAC Collision Notification frame to avoid address collision. When such a collision risk is anticipated (#350) with the MAC address of a EDP ~~CPE~~ STA affiliated with a EDP ~~CPE~~ non-AP MLD, the AP shall send the OTA MAC Collision Notification (#558) frame to both EDP ~~CPE~~ STAs affiliated with the EDP ~~CPE~~ non-AP MLDs (#91, 811, 93)).

In general, the operation is as follows. If the collision is expected to occur m epochs after the current epoch, then the EDP ~~CPE~~ AP MLD sends an OTA Collision Warning element to the EDP ~~CPE~~ non-AP MLD with the value of the Colliding Epoch field in the Collision Warning element equal to m, the Collision Status field set to 0, indicating the collision risk, and the non-AP MLD Specific Epoch Number Offset field (#559) set to n, where n is the epoch count that the non-AP MLD is requested to skip. The EDP ~~CPE~~ AP MLD is therefore requesting that for the epoch occurring after m epochs, the EDP ~~CPE~~ AP MLD uses (#94) the EDP ~~CPE~~ non-AP MLD FA parameters that the EDP ~~CPE~~ non-AP MLD had planned to use for the epoch occurring m+n epochs later. Then (#94), in the subsequent epoch, the EDP ~~CPE~~ non-AP MLD is expected to use the EDP ~~CPE~~ non-AP MLD FA parameters (#1068) that the EDP ~~CPE~~ non-AP MLD had planned to use m+n+1 epochs later, unless the EDP ~~CPE~~ AP MLD also signals a collision notification for that epoch. The sum m+n cannot be larger than the value of the Epochs Remaining field signaled during the epoch when the AP sent the OTA MAC Collision Notification (#558) frame. A non-AP MLD that received an OTA MAC Collision Notification frame (#812) shall respond with an OTA MAC Collision Response frame with the Collision Status field set to either 1 (#94, 289, 290), accepting the EDP ~~CPE~~ AP MLD proposed remediation, thus applying the offset requested by the EDP ~~CPE~~ AP MLD, or 2 (#94, 289, 290), rejecting the EDP ~~CPE~~ AP MLD proposed remediation, (#970) thus using the EDP ~~CPE~~ non-AP MLD FA parameters(#1068) that the EDP ~~CPE~~ non-AP MLD had planned to use for that epoch before receiving the EDP ~~CPE~~ AP MLD OTA MAC Collision Notification (#558) frame. The AP may not accept traffic from, or forward traffic to, a EDP ~~CPE~~ STA affiliated with the non-AP MLD that rejected the proposed remediation for the affected link, during the epoch when the collision occurs. Alternatively, the AP may disassociate a EDP ~~CPE~~ non-AP MLD that rejected the proposed remediation (#91).

NOTE – A non-AP MLD might decline to apply the requested offset for procedural reasons, e.g., the inability to skip epoch FA parameter sequences, or internal privacy configuration or policy reasons (#560).

A BPE AP MLD shall determine whether the BSSID it will use in a subsequent epoch will cause collision with the BSSID of another AP MLD on a link. When such a collision risk is anticipated, the BPE AP MLD shall send to its associated BPE non-AP MLDs an OTA MAC Collision Notification frame before the epoch when the collision is anticipated to risk occurring and indicated in the Colliding Epoch field, and informing the non-AP MLDs that the BPE AP MLD shall apply the BPE AP MLD specific MHA parameters epoch offset signaled in the AP MLD OTA MAC Collision Notification frame to avoid address collision. The default offset value is 1. (#213)

**9.4.2.350 OTA MAC Collision Warning element**

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

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

**OTA MAC 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 OTA MAC Collision Warning element. The field takes value 0 when sent by the AP MLD in an OTA MAC Collision Notification frame(#123), ~~and~~ values 1 or 2 when sent by the EDP non-AP MLD in an OTA MAC Collision Response frame(#123), and value 3 when sent by the AP MLD for a BSSID collision notification (#213). Table 9-401h lists the possible values and their meaning.(#557)

**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 | AP MLD signals collision risk to the non-AP MLD and and will apply a remediation action to skip the BSSID intended for one or more epochs where collision risk is expected (#213) |
| ~~3~~4-255 | Reserved |

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.

When collision Status field value is 0, 1 or 2, The non-AP MLD Specific Epoch Number Offset field indicates the epoch count that the non-AP MLD skips to mitigate the OTA MAC address collision. When collision Status field value 3, the non-AP MLD Specific Epoch Number Offset field indicates the epoch count that the AP MLD skips to mitigate the BSSID or OTA MAC address collision (#213). The value 0 is reserved.

The sum of the Colliding Epoch field value and the non-AP MLD Specific Epoch Number Offset value cannot be larger than the Epoch Sequence Duration field.