**IEEE P802.11  
Wireless LANs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for RCM relevant CIDs | | | | |
| **Date**: Feb. 19, 2024 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **email** |
| Jay Yang | ZTE |  |  | Yang.zhijie@zte.com.cn |
| Yan Li |  |  |  |
| Yun Li |  |  |  |
| Graham Smith | SRT wireless |  |  |  |
| Jouni Malinen | Qualcomm |  |  |  |
| Mark Hamilton | Ruckus/CommScope |  |  |  |
| Jerome Henry | Cisco system |  |  |  |
| Binita Gupta | Cisco system |  |  |  |
|  |  |  |  |  |

**Abstract**

This submission proposes resolutions for following 3 CIDs received for TGbe SA:

22376, 22393 and 22394

**Revisions:**

* Rev 0: Initial version of the document.
* Rev1: use one IRM to identify non-AP MLD instead
* Rev2: Address some editorial issues and update the comment resolution on CID#22376
* Rev3: Rewording some sentences and add more co-authors in off-line discussion
* Rev4: address some editorial’s issue
* Rev5: Move IRM from TA to ML element in MLO case, change (Re)assocation to Association

***TGbe editor: The baseline for this document is P802.11beD5.0, P802.11bhD4.0 and P802.11REVmeD5.0***

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 TGbe Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe Draft (i.e., they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 22393 | 12.2.12 | 407/0 | According to the WG decision in Sep.2023 closing meeting, the timeline of 11bh is ahead of 11be, and thus the Non-AP MLD identification should be addressed in 11be draft, but this part is still missing according to 11be draft5.0. | extend IRM feature to cover non-AP MLD identification. | Revised.  Agree in principle.  **TGbe editor, please make the changes tagged by CID #22393 in 24/305r4.** |
| 22394 | 12.2.12 | 407/0 | According to the WG decision in Sep.2023 closing meeting, the timeline of 11bh is ahead of 11be, and thus the Non-AP MLD identification should be addressed in 11be draft, but this part is still missing. | extend Device ID further to cover the identification on non-AP MLD | Revised.  Agree in principle.  **TGbe editor, please make the changes tagged by CID #22393 in 24/305r4.** |
| 22376 | 12.2.12.2 | 0/0 | the non-AP MLD may have multiple IRMs, e.g. one IRM for MLD MAC address, another IRM for link MAC address, the IRM colision issue may happen on both the two IRMs. | the commenter will provide a resolution for the two IRMs colision issue. | Rejected.  The group agreed to use only one IRM to identify a non-AP MLD. The described issue by the commenter does not exist. |

**Discussion:**

At the very beginning, both non-AP STA and non-AP MLD with RCM identification issue were in scope and well discussed in 11bh group. But in Interim meeting in Sep. 2023, the 802.11 working group decided to switch the timeline of 11bh and 11be, which causes the solution for non-AP MLD identification moved from 11bh group to 11be group. And 11bh group only focus on non-AP STA identification.

See the following meeting minutes in 11-23-1452-01-0000-minutes-working-group-september-2023.doc

“34.1.The order of the 11bh amendment will be moved ahead of 11be and there are also some minor updates to be made. The timeline chart should be updated shortly.

34.2.Chair: The order of 11be and 11bh was decided by the chair, during the CAC meeting last night.”

Summarize the proposed text in this CR:

11bh draft defines two mechanisms: Device ID and IRM. Each of them can identify a non-AP STA in PASN、FILS mode and 4HS scenarios independently. But 11be draft only define MLO in 4HS scenarios. The simple extension manner like, “non-AP STA” to “non-AP STA or non-AP MLD” may cause some technical confusion when the sentence covers PASN and FILS case. Therefore, we duplicate the two mechanisms with a separate paragraph.

1. MLO Device ID mechanism: Clarify the Device ID assignment and usage by MLD with the similar sentences as legacy device.
2. MLO IRM: Clarify IRM assignment and usage by MLD with the similar sentences as legacy device.
3. ~~MLO IRM: The non-AP MLD may provide a link IRM and an MLD IRM to the AP MLD, which the two IRMs are used in different scenarios,e.g.Link IRM is used in the discovery phase, while MLD IRM is used in authentication phase. The non-AP MLD may only provide an MLD IRM during the previous association, which indicates the MLD IRM is same to the Link IRM.~~
4. ~~Duplicated IRM: If the AP MLD grants two IRMs(MLD IRM and Link IRM) to the non-AP MLD, the collision issue may happened on the two IRMs. Extend current Duplicated IRM action frame and new IRM action frame to indicate which IRM(s) is collided.~~

**Proposed Texts:**

**3.2 Definitions specific to IEEE Std 802.11**

**identifiable random medium access control (MAC) address:** [IRM] A MAC address that can be used by

a non-access point (non-AP) station (STA) to identify itself to a network.

**4.5.4.10 MAC privacy enhancements**

TGbe editor: please insert the following proposed changes (CID #22393).

To mitigate this sort of traffic analysis, a STA or a non-AP MLD can support the ability to periodically and randomly change its

MAC addresses and reset counters and seeds prior to association. A non-AP MLD can also change the MAC address of an affiliated STA prior to an association. Such a STA or a non-AP MLD, upon reconnecting to anetwork, can provide either a device ID previously provided by the network or can use an identifiable

random MAC address (IRM) the STA or the non-AP MLD previously provided to the network or both. Either approach allows

the network to recognize the STA or the non-AP MLD while providing protection against third party tracking or traffic analysis.

While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames

containing SSIDs of favored BSS networks.

TGbe editor: please insert the following changes (CID #22393).

**9.4.2.313 Device ID element**

The Device ID element contains a device ID. The format of the Device ID element is shown in Figure 9-1057a (Device ID element format).

...existing context...

When sent from an AP to a non-AP STA, or when sent from an AP MLD to a non-AP MLD, the Device ID Status field contains one of the values shown in

Table 9-415a (Device ID Status field values).

...existing context...

TGbe editor: please insert the following changes (CID #22393).

**9.4.2.314 IRM element**

The format of the IRM element is shown in Figure 9-1057b (IRM element format)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID  Extension | IRM Status | IRM |

Octets: 1 1 1 0 or 1 0 or 6

**Figure 9-1057b—IRM element format**

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

When sent to an AP or an AP MLD, the IRM Status field is not present.

When sent from an AP or an AP MLD, the IRM Status field contains one of the values shown in Table 9-415b (IRM Status

field values)

**Table 9-415b—IRM Status field values**

|  |  |  |
| --- | --- | --- |
| **IRM Status** | **Name** | **Meaning** |
| 0 | Recognized | Indicates that the IRM has been recognized |
| 1 | Not Recognized | Indicates that the IRM has not been recognized |
| 2-255 | Reserved |  |

The IRM field contains a MAC address when sent from a non-AP STA to an AP, or when sent from a non-AP MLD to an AP MLD.

The IRM field is not present when sent from an AP to a non-AP STA, or when sent from an AP MLD to a non-AP MLD.

TGbe editor: please insert the following proposed changes (CID #22393).

**9.6.35 IRM Action frame details**

**9.6.35.1 General**

Two Action frames are defined for IRM purposes. These frames are identified by the single octet IRM

Action field, which follows immediately after the Category field. The values of the IRM Action field are

defined in Table 9-641a (IRM Action field).

**Table 9-641a—IRM Action field**

|  |  |
| --- | --- |
| **IRM Action field value** | **Meaning** |
| **0** | Duplicate IRM |
| **1** | New IRM |
| **2-255** | Reserved |

**9.6.35.2 Duplicate IRM**

The format of the Duplicate IRM frame Action field is shown in Figure 9-1265a (Duplicate

IRM frame Action field format).

|  |  |
| --- | --- |
| Category | IRM Action |

Octets: 1 1

**Figure 9-1265a—Duplicate IRM frame Action field format**

The Category field is defined in 9.4.1.1.1 (Action field).

The IRM Action field is defined in Table 9-641a (IRM Action field) in 9.6.35.1 (General).

**9.6.35.3 New IRM**

The format of the New IRM frame Action field is shown in Figure 9-1265b (New IRM frame Action field format).

|  |  |  |
| --- | --- | --- |
| Category | IRM Action | IRM |

Octets: 1 1 6

**Figure 9-1265b—New IRM frame Action field format**

The Category field is defined in 9.4.1.1.1 (Action field).

The IRM Action field is defined in Table 9-641a (IRM Action field) in 9.6.35.1 (General).

The IRM field contains a MAC address.

TGbe editor: please insert the following proposed changes (CID #22393).

**12.2.12 Identifying a non-AP STA or a non-AP MLD with changing MAC address**

To mitigate tracking and traffic analysis by third parties, a non-AP STA may randomly change its MAC

address while not associated. For MLO, a non-AP MLD may randomly change any of its affiliated non-AP STA MAC Address(es) or it’s MLD MAC address while not associated (see 4.5.4.10 (MAC privacy enhancements)).

This presents a problem for the network in that it is unable to identify a non-AP STA or a non-AP MLD that previously associated and is not able to apply cached information (“shared identity state”) from the previous association to the current association (see 12.2.10). Similarly, this presents a problem for the non-AP STA or a non-AP MLD in that it cannot assume the network can recognize the STA or the non-AP MLD as correlated to any cached information from previous association(s). Two mechanisms are defined to alleviate these problems.

The first mechanism is referred to as the device ID mechanism, where the AP provides an identifier to the non-AP STA during association or PASN authentication that the non-AP STA may then report back to the AP during a future association or PASN authentication as defined in 12.2.12.1.

For MLO, in the device ID mechanism, the AP MLD provides an identifier to the non-AP MLD during the 4-way handshake that the non-AP MLD may then report back to the AP MLD during a future association as defined in 12.2.12.X.

The second mechanism is referred to as the IRM mechanism, where the non-AP STA provides a random MAC address (different from the address it is currently using as TA for its own transmissions) to the AP during association or PASN authentication and then uses that MAC address as TA for its own transmissions for identification of the STA, during its next pre association exchanges, PASN authentication, and/or association and associated exchanges with that AP as defined in 12.2.12.2.

For MLO, in the IRM mechanism, the non-AP MLD provides a random MAC address (different from the current MLD MAC address) to the AP MLD during the 4-way handshake and then uses the new MAC address for identification of the non-AP MLD, during its next preassociation exchanges, and/or association and associated exchanges with that AP MLD as defined in 12.2.12.Y.

xxx

The two mechanisms both allow the network to recognize the STA or the non-AP MLD while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA or the non-AP MLD.

The two mechanisms may be used concurrently.

NOTE 1—The IRM mechanism and the device ID mechanism are independent. IRM allows an AP or an AP MLD to recognize a non-AP STA or a non-AP MLD respectively prior to and while it is associated. A device ID allows an AP or an AP MLD to identify a non-AP STA or a non-AP MLD respectively while it is associated. A device ID is allocated by an AP or an AP MLD, and an IRM is selected by a non-AP STA or a non-AP MLD.

If an AP and a non-AP STA both have both IRM and device ID activated, the non-AP STA might provide both an IRM and a device ID during association or PASN authentication.

For MLO, if an AP MLD and a non-AP MLD both have both IRM and device ID activated, the non-AP MLD might provide both an IRM and a device ID during association.

NOTE 2—The device ID and IRM mechanisms are not specified for use in PBSSs.[107, 103]

**12.2.12.1 Device ID mechanism**

An AP that has dot11DeviceIDActivated equal to true advertises activation of the device ID mechanism by

setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.240 (RSNXE)) in

Beacon and Probe Response frames. [230]

A non-AP STA that has dot11DeviceIDActivated equal to true indicates the device ID mechanism is activated

by setting the Device ID Active field to 1 in either the Extended RSN Capabilities field in (Re)Association

Request frames or the first PASN frame that is sent to any AP that advertises activation of the device ID

mechanism.[120, 143, 121, 230]

An AP that includes the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames,

i.e., when dot11PASNActivated is true, and has dot11DeviceIDActivated equal to true shall set

dot11KEKPASNActivated to true.

A non-AP STA that has dot11DeviceIDActivated equal to true and intends to use PASN, i.e., when

dot11PASNActivated is true, shall set dot11KEKPASNActivated to true. [208]

An AP that has dot11DeviceIDActivated equal to true and that receives a (Re)Association Request frame or the

first PASN frame that includes an Extended RSN Capabilities field with the Device ID Active field equal to 1

shall do one of the following:

— include an Extended RSN Capabilities element in the (Re)Association Response frame with the

Device ID Active field set to 1.

— include an Extended RSN Capabilities element in the second PASN frame with the Device ID Active

field set to 1.

For correct operation of the device ID mechanism, all APs in the ESS need to have

dot11DeviceIDActivated set to true.[122]

NOTE—The criteria and mechanism to distribute device IDs throughout the ESS is out of scope for this standard. [145,

50]A STA should not send a frame containing a device ID (sub)element to any STA unless the receiving STA

sets the Device ID Active field to 1 in the Extended RSN Capabilities field.[210, 123, 238]

If a non-AP STA has a device ID configured, then it shall provide a device ID using the procedures described

below:[57, 73]

1) When using PASN authentication, in the Device ID element in the first PASN frame.

2) When using FILS authentication, in the Device ID element in the Association Request frame.

3) When not using PASN or FILS authentication, in the Device ID KDE in message 2 of the 4-way

handshake.[263]

An AP shall provide a device ID using the procedures described below:[58]

1) When using PASN authentication, in the Device ID subelement in the second PASN frame.[210]

2) When using FILS authentication, in the Device ID element in the Association Response frame.

3) When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4-way

handshake.[264]

A STA may delete a stored device ID at any point in time for implementation specific reasons (for example,

configuration changes have lost the device ID, or some time has passed since the last association to the

ESS).[125, 240, 37, 126]

When a non-AP STA sends a device ID to an AP, it shall use the device ID most recently received from the

ESS of which the AP is a member . [38, 127, 265]

When an AP with dot11DeviceIDActivated equal to true receives a frame containing a device ID from a

non-AP STA and the AP recognizes the received device ID, the AP shall perform one of the following

actions:[25, 13, 39, 266, 40, 223, 128, 129, 226]

1) Set the Device ID Status field of the Device ID KDE or Device ID (sub)element to 0 to indicate

that the AP recognizes the non-AP STA and set the Device ID field to zero length (indicating the

current device ID is maintained).[267, 210, 41, 130]

2) Assign a new device ID value in the Device ID field and set the Device ID Status field of the

Device ID KDE or Device ID (sub)element to 0 in the appropriate frame.[210]

When an AP with dot11DeviceIDActivated equal to true receives a first PASN frame containing a device ID

that it recognizes, the AP shall assign a new device ID value to the non-AP STA and include this new device ID

in a Device ID element in the second PASN frame, setting the Device ID Status field of the Device ID

subelement to 0 to indicate Recognized. [268, 210, 132, 42]

When a non-AP STA receives a frame that contains a Device ID Status field in the Device ID KDE or Device

ID (sub)element equal to 0, indicating Recognized, it may proceed with the assumption that the shared identity

state with the AP or ESS (as per the concepts of 12.2.12 (Identifying a non-AP STA with changing MAC

address)) is now bound to the Address 2 field in the Association Request frame or the first PASN frame most

recently transmitted by the non-AP STA.[137, 210, 227, 116, 135]

If an AP sets Device ID (sub)element or Device ID KDE with the Device ID Status field set to 1, indicating Not

Recognized, then the AP may also provide in that same Device ID (sub)element or Device ID KDE a new

device ID, thus establishing a new shared identity. An AP may set a Device ID Status field to 1 indicating

“Not Recognized” if the AP cannot unequivocally identify the non-AP STA shared identity state. [210, 135]

When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Device ID

(sub)element equal to 1, indicating Not Recognized, it shall assume that no shared identity state exists with the

AP or ESS (as per the concepts of 12.2.12 (Identifying a non-AP STA with changing MAC address)).

**12.2.12.2 Identifiable random MAC address (IRM) operation**

An AP that has dot11IRMActivated equal to true advertises activation of the IRM mechanism by setting the

IRM Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.240 (RSNXE)) in Beacon and Probe

Response frames.[228] A non-AP STA that has dot11IRMActivated equal to true indicates the IRM

mechanism is active by setting the IRM Active field to 1 in either the Extended RSN Capabilities field in

(Re)Association Request frames or the first PASN frame that is sent to any AP that advertises activation of the

IRM mechanism. [143, 121, 230]

An AP that has dot11IRMActivated equal to true and that receives a (Re)Association Request frame or the first

PASN frame that includes an Extended RSN Capabilities field with the IRM Active field equal to 1 shall do

one of the following:

- include an Extended RSN Capabilities element in the (Re)Association Response frame with the

IRM Active field set to 1.

- include an Extended RSN Capabilities element in the second PASN frame with the IRM Active

field set to 1.

An AP that includes the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames,

i.e., when dot11PASNActivated is true, and has dot11IRMActivated equal to true shall set

dot11KEKPASNActivated to true. [208]

A non-AP STA that has dot11IRMActivated equal to true and intends to use PASN, i.e., when

dot11PASNActivated is true, shall set dot11KEKPASNActivated to true. [208]

Correct operation of the IRM mechanism depends on all APs in the ESS being configured with

dot11IRMActivated set to true. Activation of the IRM mechanism needs to be advertised by all APs in an ESS

in Beacons and Probe Response frames. [230]

NOTE 1—The criteria and mechanism to distribute IRMs throughout the ESS is out of scope for this standard. [145, 46,

47, 51, 283, 50]

An IRM is a MAC address that is constructed from the locally administered address space.[146] A non-AP

STA should construct randomized IRMs according to IEEE Std 802-2014 and IEEE Std 802c-2017. [60]

When associating or authenticating using PASN for the first time to an ESS, the non-AP STA may use any

MAC address. [76] Each time the non-AP STA associates with an AP in an ESS, it may provide a new IRM to

the AP during association.That IRM may be shared with all the APs in the ESS. [9, 77] The non-AP STA may

then use that IRM as its TA the next time it requests association to any AP in that same ESS. The non-AP STA

may also use that IRM as its TA for any probes, directed or broadcast, public Action frames, Authentication

and (Re)Association frames, that it may transmit when it intends to be identified.[149]

When associating to an AP that advertises activation of the IRM mechanism, the non-AP STA may provide a

new IRM to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS

authentication, including the IRM element in the Association Request frame. When using PASN, the non-AP

STA may provide a new IRM to the AP by including the IRM subelement in the third PASN frame.[210, 230]

If a newly provided IRM is already in use within the ESS, or is identical to an IRM stored by the AP for another

STA, then, after association or authentication using PASN, the AP should send a Duplicate IRM frame (see

9.6.35.2 (Duplicate IRM)) to the non-AP STA indicating to the STA that the provided IRM is a duplicate. [244,

152, 245, 10] The non-AP STA may then respond with a New IRM frame (see 9.6.35.3 (New IRM)) which

provides a new IRM to the AP.

The non-AP STA should store the newly allocated IRM as an identifier for use with the AP(s) in that ESS and

the AP(s) in that ESS should store the IRM as an identifier for that non-AP STA. The non-AP STA then should

use that allocated IRM as its TA when it next associates or uses PASN to preassociate with that same AP or

another AP in the same ESS. In so doing, the AP identifies the non-AP STA.[197]

A non-AP STA indicates the IRM mechanism is activated in a (Re)Association Request frame or in the first

PASN frame and the AP indicates the IRM mechanism is activated in the corresponding (Re)Association

Response frame or in the second PASN frame. [154, 155, 221, 231, 230] If a non-AP STA indicates the IRM

mechanism is activated in an Association Request frame or first PASN frame and the AP indicates the IRM

mechanism is activated in the corresponding Association Response frame or second PASN frame, then the AP

shall support the following options:[230]

— the AP shall include an IRM KDE in message 3 of the 4-way handshake if executing a 4-way hand

shake.

— the AP shall include an IRM element in the Association Response frame if using FILS authentica

tion.

— the AP shall include an IRM element in the second PASN frame if using PASN authentication.

[157,231]

If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the IRM Status

field of the IRM KDE or IRM element is set to indicate Recognized and the IRM field is not present. If the AP

does not recognize the IRM, the IRM Status field of the IRM KDE or IRM element is set to indicate Not

recognized and the IRM field is not present.[158] The non-AP STA, on receipt of an IRM Status field of value

1, indicating that the AP has not recognized the IRM, may either continue to associate or authenticate using

PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or,

when using FILS authentication optionally provide an IRM element in the Association Request frame, or when

using PASN authentication optionally provide an IRM element in the third PASN frame, else disassociate/

deauthenticate.[232, 233] An AP may set an IRM status field to 1 indicating Not Recognized if the AP cannot

unequivocally identify the non-AP STA shared identity state.

NOTE 2—In the case of an initial association to an AP in an ESS, the AP indicates that the non-AP STA is not

recognized, but the non-AP STA would ignore that. [197]

If a non-AP STA has previously provided an IRM to an AP in as ESS, and the non-AP STA sends an

Authentication frame using that IRM as the TA to any AP in the ESS, then the AP receiving the Authentication

frame is able to identify the non-AP STA before association is started or completed. [274, 159, 234, MDR]

A non-AP STA may use that address for active scanning for an AP or ESS that was provided that address, such that the AP may identify the non-AP STA. [11] A non-AP

STA that has provided an IRM to an ESS may use that address in a Public Action frame (e.g., a GAS frame)

such that APs in that ESS may identify the non-AP STA. [12]

NOTE 3—To enhance STA privacy, a non-AP STA ought to change its IRM in each association or PASN preassociation.

[207]

TGbe editor: please insert the following paragraph in appropriated place (CID #22393).

**12.2.12.X Device ID mechanism for MLO**

Each affiliated AP that has dot11DeviceIDActivated equal to true, advertises activation of the device ID mechanism by setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.240 (RSNXE)) in Beacon and Probe Response frames.

An non-AP MLD that has dot11DeviceIDActivated equal to true, advertises that the device ID mechanism is activated by setting the Device ID Active field to 1 in the the Extended RSN Capabilities field in Association request frames transmitted by an affiliated non-AP STA.

An AP MLD that has dot11DeviceIDActivated equal to true and that receives a Association Request frame that includes an Extended RSN Capabilities field with the Device ID Active field equal to 1 through an affiliated AP, shall include an Extended RSN Capabilities element in the (Re)Association Response frame with the Device ID Active field set to 1.

For correct operation of the device ID mechanism, all the AP MLDs and all the APs not affiliated with AP MLDs in an ESS need to have dot11DeviceIDActivated to true.

NOTE—The criteria and mechanism to distribute device IDs throughout the ESS is out of scope for this standard.

A non-AP MLDshould not send a frame containing a device ID to h another MLD, unless the other MLD, sets the Device ID Active field to 1 in the Extended RSN Capabilities field when transmitted through an affiliate STA.

If a non-AP MLD has a device ID configured, it shall provide the device ID in the Device ID KDE in message 2 of the 4-way handshake. An AP MLD shall provide a device ID in the Device ID KDE in message 3 of the 4-way handshake in response to the receipt of a Device ID KDE in message 2 of the four-way handshake.

An MLD may delete a stored device ID at any point in time for implementation specific reasons (for example, configuration changes have lost the device ID, or some time has passed since the last association to an AP MLD in the ESS). When a non-AP MLD sends a device ID to an AP MLD, it shall use the device ID most recently received from any AP MLD belonging to the ESS of which the AP MLD is a member.

When an AP MLD with dot11DeviceIDActivated equal to true receives a frame containing a device ID from an non-AP MLD and the AP MLD recognizes the received device ID, the AP MLD shall perform one of the following actions:

1) Set the Device ID Status field of the Device ID KDE to 0, to indicate that the AP MLD recognizes the non-AP MLD and set the Device ID field to zero length (indicating the current device ID is maintained).

2) Assign a new device ID value in the Device ID field and set the Device ID Status field of the Device ID KDE to 0 in the appropriate frame.

When an non-AP MLD receives a frame that contains a Device ID Status field in the Device ID KDE equal to 0, indicating Recognized, it may proceed with the assumption that the shared identity state with the AP MLD or ESS (as per the concepts of 12.2.12 (Identifying a non-AP MLD with changing MAC address)) is now bound to the MLD MAC Address in the Basic Multi-Link element in the Association Request frame most recently transmitted by the the non-AP MLD.

If an AP MLD sets Device ID KDE with the Device ID Status field set to 1, indicating Not Recognized, then the AP MLD may also provide in that same Device ID KDE, a new device ID, thus establishing a new shared identity. An AP MLD may set a Device ID Status field to 1 indicating “Not Recognized” if the AP MLD cannot unequivocally identify the non-AP MLD shared identity state.

When an non-AP MLD receives a frame that contains a Device ID Status field in a Device ID KDE equal to 1, indicating Not Recognized, it shall assume that no shared identity state exists with the AP MLD or ESS (as per the concepts in 12.2.12 (Identifying a non-AP MLD with changing MAC address)).

**12.2.12.Y Identifiable random MAC address (IRM) operation for MLO**

Each AP MLD that has dot11IRMActivated equal to true, advertises activation of the IRM mechanism by setting the IRM Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.240 (RSNXE)) in Beacon and Probe Response frames transmitted by the affiliated AP(s). A non-AP MLD that has dot11IRMActivated equal to true, indicates the IRM mechanism is active by setting the IRM Active field to 1 in the Extended RSN Capabilities field in Association Request frames transmitted through an affiliated STA sent to any AP MLD that advertises activation of the IRM mechanism.

An AP MLD that has dot11IRMActivated equal to true, and that receives a (Re)Association Request frame that includes an Extended RSN Capabilities field with the IRM Active field equal to 1 through an affiliated AP, shall include an Extended RSN Capabilities element in the Association Response frame with the IRM Active field set to 1.

Correct operation of the IRM mechanism depends on all the AP MLDs in an ESS and all the APs not affiliated with AP MLDs in the ESS being configured with dot11IRMActivated set to true. Activation of the IRM mechanism needs to be advertised by all AP MLDs through affiliated APs in the ESS in Beacons and Probe Response frames.

NOTE 1—The criteria and mechanism to distribute IRMs throughout the ESS is out of scope for this standard.

An IRM is a MAC address that is constructed from the locally administered address space. A non-AP MLD should construct randomized IRMs according to IEEE Std 802-2014 and IEEE Std 802c-2017.

Each time a non-AP MLD associates with an AP MLD in an ESS, it may provide an IRM to the AP MLD during the 4-way handshake. That IRM may be shared with all the AP MLDs in the ESS. Any non-AP MLD may set the MLD MAC address field to the IRM in the Basic Multi-Link element in Authentication and Association frames, that it may transmit when it intends to be identified. When associating to an AP MLD that advertises activation of the IRM mechanism, the non-AP MLD may provide a new IRM to the AP MLD by including an IRM KDE in message 4 of the 4-way handshake.

If any newly provided IRM by a non-AP MLD is already in use within the ESS, or is identical to an IRM stored by the AP MLD for another non-AP MLD, then, after association and the 4-way handshake, the AP MLD should send a Duplicate IRM frame (see 9.6.35.2(Duplicate IRM)) to the non-AP MLD through an affiliated STA, indicating to the non-AP MLD that the provided IRM is a duplicate. The non-AP MLD may then respond with a New IRM frame (see 9.6.35.3 (New IRM)), providing a new IRM to the AP MLD.

The non-AP MLD should store the newly allocated IRM as an identifier for use with the AP MLDs in that ESS. The AP MLDs in the ESS should store the newly updated IRM as an identifier for that non-AP MLD. The non-AP MLD should then use that allocated IRM as its MLD MAC address when it next associates with that an AP MLD in the same ESS. In so doing, the AP MLD identifies the non-AP MLD.

If a non-AP MLD indicates that the IRM mechanism is activated in a Association Request frame and an AP MLD indicates the IRM mechanism is activated in the corresponding Association Response frame, then the AP MLD shall include an IRM KDE in message 3 of the 4-way handshake.

If an AP MLD recognizes the IRM in a received frame from a non-AP MLD, the IRM Status field of the IRM KDE is set to indicate Recognized and the IRM field is not present.

If the AP MLD does not recognize the IRM, the IRM Status field of the IRM KDE is set to indicate Not Recognized and the IRM field is not present. The non-AP MLD, on receipt of an IRM Status field equal to 1, indicating that the AP MLD has not recognized the IRM, may either continue the 4-way handshake with the AP MLD or optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake. An AP MLD may set an IRM status field to 1 indicating Not Recognized if the AP MLD cannot unequivocally identify the non-AP MLD shared identity state.

NOTE 2—In the case of an initial association to an AP MLD in an ESS, the AP MLD might indicate that the non-AP MLD is not recognized.If a non-AP MLD has previously provided an IRM to an AP MLD in an ESS and the non-AP MLD sends an Authentication frame using that IRM as the as the MLD MAC address to any AP MLD in the ESS, then the AP MLD receiving the Authentication frame is able to identify the corresponding non-AP MLD before association is started or completed. A non-AP MLD may set the MLD MAC address field to the IRM in the Basic Multi-Link element in Authentication and Association frames sent to AP MLDs within the ESS so that the AP MLD may identify the corresponding non-AP MLD using the IRM.

NOTE 3—To enhance STA privacy, a non-AP MLD ought to change its IRM in each association.

**B.4 PICS proforma—IEEE Std 802.11-2020**

**IUT configuration**

TGbe editor: please insert the following proposed change (CID #22393).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **IUT configuration** | **References** | **Status** | **Support** |
| CFDID | Device ID mechanism for non-MLO | 12.2.12.1  (Device ID  mechanism) | PC34 AND  CFAP:O  PC34 AND  CFSTAofAP:  O | Yes  No  |
| CFIRM | IRM operation for non-MLO | 12.2.12.2  (Identifiable random  MAC address (IRM)  operation) | PC34 AND  CFAP:O  PC34 AND  CFSTAofAP:  O | Yes  No  |

TGbe editor: please insert Insert two new entries in the table in appropriated place (CID #22393).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **IUT configuration** | **References** | **Status** | **Support** |
| CFMLODID | Device ID mechanism for MLO | 12.2.X.1  (Device ID  Mechanism for MLO) | PC34 AND  CFEHTMLD:O | Yes  No  |
| CFMLOIRM | IRM operation for MLO | 12.2.X.2  (Identifiable random  MAC address (IRM)  Operation for MLO) | PC34 AND  CFEHTMLD:O | Yes  No  |

TGbe editor: please insert the following proposed changes (CID #22393).

**C.3 MIB detail**

....exist text....

dot11DeviceIDActivated OBJECT-TYPE

SYNTAX TruthValue

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, when true, indicates that the STA or MLD implementation is capable of transmitting a device ID.” [20]

DEFVAL { false }

::= { dot11StationConfigEntry <ANA> }

dot11IRMActivated OBJECT-TYPE

SYNTAX TruthValue

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, when true at a non-AP STA or a non-AP MLD, indicates that the

STA or the non-AP MLD implementation is capable of transmitting an IRM.[21] This attribute,

when true at an AP or an AP MLD indicates that the AP or the AP MLD supports IRM."

DEFVAL { false }

::= { dot11StationConfigEntry <ANA> }

....exist text....