IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11 TGbhLB274 Misc CID resolutions |
| Date: 2023-10-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java Dr, Sunnyvale, CA 94089 | 303-818-8472 | mark.hamilton2152@gmail.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions to the following comments received from the initial working group ballot (LB274): 50, 54, 55, 74, 117, 122, 157, 165, 167, 190, 191, 209, 213, 215, 216, 217, 223, 230, 231, 242, 243, 267, 268, 273, 277, 278, 280, 283, 284, 286, 292, 293.

# Revision History

R0 – Iinitial version

# Draft version

Changes are relative to TGbh D1.0, unless stated otherwise.

# Ready for Discussion

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/****Line** | **Comment** | **Proposed Change** |
| 74 | Robert Stacey | 12.7.6.3 | 35.41 | This statement, by itself, is not true. There are additional constraints on including the Device ID KDE. | Change to "Additionally, may include a Device IDE KDE subject to conditions in 12.2.11.1." Similarly, for statements at 35.57, 35.59 |

Context:



Subclause 12.2.11.1 has constraints such as:

* Shall not send a device ID to any STA that does not indicate Device ID is active.
* Shall not send a device ID when the non-AP STA has not previously associated or used PASN with the ESS.
* The non-AP STA no longer has the device ID available (for implementation-specific reason)
* Etc.

Thus, the commenter is correct.

However, 12.2.11.1 is only behavior description for Device ID, while 12.2.11.2 is for IRM. So, the IRM KDE needs to reference 12.2.11.2.

**Proposed Resolution:**

Revised

Change to "Additionally, may include a Device IDE KDE subject to conditions in 12.2.11.1.” at the cited location, and at 35.57.

At 35.59, change to "Additionally, may include an IRM KDE subject to conditions in 12.2.11.2.”

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/****Line** | **Comment** | **Proposed Change** |
| 117 | Stephen McCann | 4.5.4.10 | 18.19 | The word "but" seems to imply that is disadvantage. The sentence should be made more positive. | Change "but protects" to "while protecting" |
| 223 | Antonio DeLaOlivaDelgado | 4.5.4.10 | 18.19 | The phrase "recognize the device and/or use a MAC address that it previously provided to the network, but protects theinformation from third parties." What information does it refer to, the device ID? please clarify | clarify |
| 273 | Mark Hamilton | 4.5.4.10 | 18.19 | "and/or" needs to be clarified. | Replace "and/or", with ", or can" |
| 286 | Liuming Lu | 4.5.4.10 | 18.18 | The description of this sentence is unclear: 1) what is identified by the device ID needs to be clarified; 2) what is the purpose of the usage of a MAC address that it previously provided to the network needs to be clarified. 3)since there are two options how to choose one or both of them needs to be clarified. | 1) suggest to modify this sentence as follows:Such a STA, when reconnecting to a network, can exchange a device ID and/or a MAC address that it previously provided to the network for identifying the STA, and the usage of the device ID and/or MAC address allows the network to recognize the STA. The information of the device ID and/or MAC address should be protected from third parties.2) The conditions for choosing one or both of the two options need to be clarifiled. |

Context:



Note that previous CIDs (156 and 240) have made some modification here already:

Change to:

“Such a STA, when reconnecting to a network, can exchange a device ID that allows the network to recognize the device and/or use a MAC address (IRM) that it previously provided to the network, while mitigating the abilities of third parties to do traffic analysis.”

This change resolves CID 117, by removing the “but” language.

This change also resolves CID 223, by rewording to no longer reference “the information” in the final phrase.

This already agreed change does \_not\_ address the “and/or” usage (per CID 273), however, and the points in CID 286 are only partially addressed. Thus some additional wording changes are suggested below.

The third point in CID 286, that how to choose between the two options needs to clarified, is rejected because this is only clause 4 text. The details on behavior, including how the mechanism is chosen, are captured in main body behavior clauses such as clause 12.

**Proposed resolution (all 4 CIDs):**

Revised.

Replace the cited sentence with:

“Such a STA, when reconnecting to a network, can exchange a previously provided device ID or can use a previously provided MAC address (IRM), either of which allows the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis.”

NOTE TO EDITOR: This is a modification of the changes made in CIDs 156 and 240.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/****Line** | **Comment** | **Proposed Change** |
| 54 | Jerome Henry | 12.2.11 | 30.9 | The text "To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address " implies that the STA may change its MAC address while associated (as randomly can happen at any time). This conflicts with 11aq/12.2.10 | Replace with "To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address whole not associated" |
| 55 | Jerome Henry | 12.2.11 | 30.11 | The sentence " For some services, however, it may be desired by the user that the non-AP STA is identified by an AP and network services." does not mean much if the reader does not have in mind the context of 802.11bh work. This could very well mean 802.1X, which is not what the setence intent is. | Replace with " For some services, however, it may be desired by the user that the non-AP STA is identified by an AP and network services at reconnection time." |
| 165 | Mark RISON | 12.2.11 | 30.11 | What are "network services"? | Clarify |
| 167 | Mark RISON | 12.2.11 | 30.15 | "Exchanges of the device ID areprotected from third parties." -- not clear enough. A MIC is protection too | Change to "... are protected from eavesdropping by third parties." |
| 190 | Mark RISON | 12.2.11 |  | "sent to any AP in the ESS" is ambiguous. It might mean you have to send it to whichever AP you're connecting with, or that you only have to send it to one of the APs, at some point | Delete "to any AP" at 30.31 and 32.40 |
| 267 | Mark Hamilton | 12.2.11 | 30.14 | Clarify what "returns" to the ESS means. | Change to "returns to that ESS using a new association, even if the non-AP STA changes its MAC address." |
| 293 | Liuming Lu | 12.2.11 | 30.10 | The description of "some services" is unlear. | Please clariy "some services" |
| 268 | Mark Hamilton | 12.2.11 | 30.19 | Clarify what "may provide a random MAC address" means. | Change to "a non-AP STA may provide to an AP a random MAC address that it will use in the future with the AP's ESS, either when it ..." |
| 292 | Liuming Lu | 12.2.11 | 30.8 | The description is unlear. | Suggest to modify this sentence as follows:To mitigate tracking and traffic analysis by the third parties, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)) |

Cited text in CID 54 (second sentence):



From 12.2.10:



Thus, CID 54 is correct (unless TGbi changes it), so the added text is likely useful. Note the typo, however, and hence “Revised.”

For CIDs 55 and 165, this text (this second sentence) has already been completely re-written as part of CID 49, etc.

For CID 167, it is noted that the text provided as resolution to CID 49 has left off the (previously included) concept that the mechanisms provide protection from tracking by third-parties. There is text to this effect in the text proposed for CIDs 156 and 240, for subclause 4.5.4.10, however, and similar text can be added here addressing the wording concern of CID 167.

For CIDs 190, 267 and 293, the rewrite for CID 49 has already removed the problematic phrases and replaced with better wording.

For CID 268, the rewrite for CID 49 already made similar changes to describe the random MAC address provided by IRM and how that address is used in the next association/PASN authentication.

For CID 292, the proposed change is simply adding “by third parties” to the introductory sentence in 12.2.11. With some editorial correction, this change is effectively accepted, in the text proposed below.

**Proposed Resolution (CIDs 54, 55, 165, 167, 190, 267, 268, 292 and 293):**

Revised

At Page 30.8 replace entire text in 12.2.11 with following

“To mitigate tracking and traffic analysis by third parties, a non-AP STA may randomly change its 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 that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem.

The first mechanism, referred to as device ID, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as IRM, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.

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

The two mechanisms device ID and IRM, may be used concurrently.”

NOTE TO EDITOR: This is the same resolution as for CID 49, except for the addition of (and shown with underscore):

* “by third parties” and “while not associated” in the first paragraph, and
* the paragraph: “The two mechanisms, device ID and IRM, both allow the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA.”

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/****Line** | **Comment** | **Proposed Change** |
| 122 | Stephen McCann | 12.2.11 | 30.19 | I think the phrase "when it associates" also applies to re-association. | Change "when it associates" to "when it (re)associates". |

Context:



The comment explicitly calls out the usage on line 19. Since, per subclause 12.2.10 (and this is related to the discussion just above on CID 54), the non-AP STA cannot change its MAC address while connected to an ESS, that would say that Reassociation is not a legal time at which a new random MAC address can be used.

That said, there is provision for a device ID and/or an IRM in the MLME-REASSOCIATE primitives and the Reassocaiton frames in the current TGbh Draft 1.0. There is no text that explicitly describes how this usage (in a reassociation context) relates to the identification provided in the (initial) association with the current ESS. This ambiguity seems to be an error in the current draft. Until/unless 12.2.10 is changed, we must assume that the rule still holds that the MAC address shall be retained constant across the entire duration of the ESS connection.

**Proposed Resolution:**

Rejected

Per subclause 12.2.10, a non-AP STA’s MAC address shall remain constant for the duration of its connection to an ESS. Thus, there is no need for the provisioning of a (new) random MAC address at reassociation.

# Not ready yet

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/****Line** | **Comment** | **Proposed Change** |
| 50 | Robert Stacey |  |  | The term "device ID" is being used refer to both the mechanism and the identifier (value). | Use one term for the mechanism (e.g., device ID mechanism) and another term for the value (e.g., device ID). |
| 157 | Mark RISON |  |  | "Device ID" should be "device ID" (except when name of field or at start of sentence, etc.) | Fix at 19.31 (rightmost), 20.3/38 (rightmost), 21.12/48 (rightmost), 22.23 (rightmost), 23.1/37 (rightmost), 27.5 (middle row), 30.31/37, 31.2/7(2x), 32.32/34, 39.54 |
| 191 | Mark RISON |  |  | There's stuff about associating with an "AP/ESS". Association is with an AP | Delete "/ESS" throughout. In contexts like "association to that same AP/ESS" change to "association within that ESS" |
| 209 | Mark RISON | 12.7.6 |  | For M4 we have "includes an IRM KDE when dot1IRMActivated is true" but there is no dot11 condition for M2+M3 | Add for M2+M3 too |
| 213 | Mark RISON | 12.7.6.1 | 35.23 | Frankly, with the zoo of options this is now unmanageable | Recast in terms of optional and mandatory parts (and since the number of possible combinations is not a power of 2 there must be some rules linking the various possible components) |
| 215 | Mark RISON | 12.13.3.2 | 36.20 | This "if any" is not clear. When will there be a device identifier | Clarify. Ditto at lines 31 and 49 |
| 216 | Mark RISON | 12.2.11 | 30.6 | "Changing MAC Address" -- but the baseline already has stuff about changing MAC address. What this new stuff is about is identifying STAs despite changing the MAC address | Change the title. Also fix the corresponding PICS entry. Also add a separate PICS for just changing MAC address (with a xref to a suitable subclause) |
| 217 | Mark RISON | C.3 | 39.39 | "This attribute, when true at a non-AP STA, indicates that the STA mightsend a device ID. This attribute when true at an AP, indicates that the APmight send a device ID." can be simplified | Change to "This attribute, when true, indicates that the STA might send a device ID." |
| 230 | Alfred Asterjadhi |  | 19.34 | Ambiguous terminology. When referring to "Device ID is active" i think you mean the protocol, as oppose to the Device ID itself. | Please rephrase |
| 231 | Alfred Asterjadhi |  | 27.61 | is the Device ID contained in an IE sent by both AP and non-AP STA? Good to clarify. Also wondering why the need of two different elements. Seem they are almost identical. | Suggest using one element instead of two and have maybe a bit to differentiate between the two (although i dont think you would need since the MAC address is technically a device ID as well. |
| 242 | Joseph Levy | 3 | 17.1 | Device ID should be defined in Clause 3, as the term is used in several locations in the draft, Clauses: 4, 6, and 12; and Annexes B, C, and AD. | Insert the following suggested definition:device identification (ID): [device ID] An ID that a non-access point (AP) station (STA) can provide to a known network to identify itself to the network. A device ID is protected from third parties. |
| 243 | Joseph Levy | 3 | 17.1 | IRM should be defined in Clause 3, as it is in several locations in the draft, Clauses: 4, 6, and 12; and Annexes B, C, and AD. | Insert the following suggested definition:identifiable random medium access control (MAC) address: [IRM] A MAC address that can be used by a non-access point (AP) station (STA) to identify itself to a network. An IRM is know to both the non-AP STA and the network and is unknown to third parties. |
| 277 | Mark Hamilton | C.3 | 39.52 | Does an AP have a dot11DeviceID MIB attribute (per non-AP STA, presumably)? This is very confusing in the MIB attribute definition which makes no distinction for AP versus non-AP STA. It's probably best to just remove this MIB attribute, and the SME manage the (local and implmentation-dependent) process for managing Device ID. | Remove the dot11DeviceID attribute from Annex C. In the body text, clarify that the SME manages the Device ID values using local and implementation-dependent methods. |
| 278 | Mark Hamilton | C.3 | 39.52 | If the non-AP STA has a dot11DeviceID MIB attribute, it needs to be a set of such IDs, stored per ESS (SSID). | Correct the MIB definition text such that on a non-AP STA, the dot11DeviceID values are stored per ESS/SSID. |
| 280 | Mark Hamilton | 12.7.6.1 | 35.13 | The list of contents of the EAPOL-Key frames (the 4 Messages) is getting impossible to understand. | Restructure the 4 Messages into a tabular structure that lists the components that (may be) included, with a description of any combination or other usage restrictions |
| 283 | Mark Hamilton | 12.13.3.2 | 36.45 | Should the Device ID element be encrypted (with AES-128-CMAC?) like the IRM element? | Add a sentence, "The IRM element shall be encrypted with the cipher suite of AES-128-CMAC." to the end of the Device ID paragraph. |
| 284 | Mark Hamilton | 12.13.3.2 | 36.37 | The additional items in the third PASN frame go before the MIC element (not "at the end of the list"). | Change the editing instructions to be similar to the second PASN frame (on page 194 of 802.11az-2022) |

# Completed

**References:**

<https://mentor.ieee.org/802.11/dcn/23/11-23-1152-24-00bh-ieee-802-11bh-lb274-comments.xlsx>

<https://mentor.ieee.org/802.11/dcn/23/11-23-1245-24-00bh-cid-resolutions-irm-1.docx>