IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution CID 122 - Reassociation  |
| Date: 2023 - November |
| 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 |
| Graham Smith | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Proposed resolution for CID 122

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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.

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.

In addition, there is no 4w HS carried out in a reassocation, so a new IRM cannot be provided encrypted.

Similarly, the device ID cannot be provided encrypted.

Hence, it is proposed to remove device ID and IRM from the reassocation process.

The following changes are required to D1.0:

**Proposed Resolution:**

REVISED

**Instructions for TGbh editor**

**Delete**

From P21.26 To P23.47

“6.3.7.5 MLME-REASSOCIATE.request”, “6.3.7.5 MLME-REASSOCIATE.confirm”, “6.3.7.5 MLME-REASSOCIATE.indication”, and “6.3.7.5 MLME-REASSOCIATE.response”.

**Note to Editor: The clause numbers for this section were changed to agree with 11me in CIDs 34 and 241. Please delete the named clauses.**

**Delete**

From P25.45 to P26.15 “9.3.3.7 Reassociation Request frame body format”, and “9.3.3.8 Reassociation Response frame body format”

**At 30.39, edit as follows:**

“A non-AP STA shall send a device ID when required by the procedures described below via the following frames (known as “non-AP Identity frames”):

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 ~~(Re)~~Association Request frame.

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

handshake.

An AP shall send a device ID when required by the procedures described below via the following frames

(known as “AP Identity frames”):

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

2) When using FILS authentication in the Device ID element in the ~~(Re)~~Association Response frame.

3) When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.”

**At 32.46 edit as follows:**

“Each time the non-AP STA associates with an AP/ESS, it provides a new IRM MAC address to the AP/ESS during the RSN association. The non-AP STA may then use that IRM MAC address as its TA the next time it requests association to that same AP/ESS. The non-AP STA may also use that IRM MAC address as its TA for any probes, directed or broadcast, public action frame, and authentication ~~and (re)association~~ frame, that it may transmit when it intends to be identified.”

**At 33.35 edit as follows:**

“NOTE 3—In State 1 and State 2, the IRM MAC address is recommended to be used only in authentication and ~~(re)~~association frames. To ensure good STA privacy, a non-AP STA is recommended to change its IRM MAC Address in every 4-way handshake.”