IEEE P802.11
Wireless LANs

|  |
| --- |
| AP rules on providing device ID and PASN ID |
| Date: 2024-07-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses IEEE P802.11bh/D5.0 rules on when an AP provides a device ID and PASN ID to a non-AP STA.

**12.2.13 Identifying a non-AP STA with changing MAC address**

**12.2.13.1 Device ID**

P37 L37-48 (association with capability indicated, but device ID not provided)

If an AP with dot11DeviceIDActivated equal to true receives an Association Request frame that includes an Extended RSN Capabilities field with the Device ID Support field equal to 1 from a non-AP STA (should this be limited to a cases where device ID was not provided since that is the only case included in the procedure below?), the AP shall provide both a device ID and a PASN ID using the procedure described below:

1) When using FILS authentication and the non-AP STA did not provide a device ID in the Device ID element in the Association Request frame, the AP shall provide a device ID in the Device ID element and a PASN ID in the PASN ID element in the Association Response frame.

2) When not using PASN or FILS authentication and the non-AP STA didn’t provide a device ID in the Device ID KDE in message 2 of the 4-way handshake, the AP shall provide a device ID in the Device ID KDE and a PASN ID in the PASN ID KDE in message 3 of the 4-way handshake.

P37 L50-54 (PASN with capability indicated, but PASN ID not provided)

If an AP with dot11DeviceIDActivated equal to true receives from a non-AP STA a first PASN frame that includes an Extended RSN Capabilities field with the Device ID Support field equal to 1 but no PASN ID element, the AP shall provide a device ID in the Device ID element and a PASN ID in the PASN ID element in the second PASN frame.

P37 L63-P38 L5 (something generic? Or should this have a condition of the previous paragraph (STA provided a device ID)?

An AP shall provide a device ID as follows:

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

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

P38 L22-L30 (association, recognized)

When an AP with dot11DeviceIDActivated equal to true receives a frame that is not a PASN frame (this feels overly generic.. any frame that happens to contain a device ID?!), 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:

1) Set the Device ID Status field of the Device ID KDE or Device ID 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) (Which frame is this talking about? Should this have “in the appropriate frame” similarly to the next action?).

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 element to 0 in the appropriate frame.

(in other words, either (1) do not provide a new device ID or (2) provide a new Device ID)

(note: no new PASN ID is needed in this case since the previously provided one is still valid as-is)

P38 L32-L36 (PASN, recognized)

When an AP with dot11DeviceIDActivated equal to true receives a first PASN frame containing a PASN ID that it recognizes, the AP shall assign a new PASN ID value to the non-AP STA and include this new PASN ID in a PASN ID element in the second PASN frame, setting the PASN ID Status field of the PASN ID element to 0 to indicate Recognized.

(note: no new device ID is needed in this case since the previously provided one is still valid as-is)

P38 L47-L52 (association, not recognized)

If an AP provides a Device ID 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 element or Device ID KDE a new device ID and, in a PASN ID element or PASN ID KDE, a new PASN ID, thus establishing a new shared identity state. An AP shall set a Device ID Status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

P38 L54-L58 (PASN, not recognized)

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

**Discussion**

Three cases (not provided, recognized, not recognized) for association and PASN cases:

* Association, no device ID provided: AP shall provide a new device ID and a new PASN ID
* PASN, no PASN ID provided: AP shall provide a new device ID and a new PASN ID
* Association, recognized: AP may provide a new device ID; no new PASN ID is provided
* PASN recognized: AP shall provide a new PASN ID; no new device ID is provided
* Association, not recognized: AP may provide a new device ID and a new PASN ID
* PASN, not recognized: AP may provide a new device ID and a new PASN ID (note: 1271r2 CID 4113 proposes to make this “may” a “shall”)

**CID 4002**

Comment:

[On behalf of Yan Li]the notes of PASN ID indicate PASN ID is only present if Device ID present,which can be interpreted as PASN ID should be mandatory if Device ID present.However, in clause 12 both of Device ID and PASN ID would be provided only in the case of initial connection and 'not recognized'case. There is no similar requirement for 'recognized'case.

Please clarify it

Proposed Change:

as the comments

Observations:

* PASN ID being allowed only if device ID is present does not imply that PASN ID shall be present if device ID is present.
* Initial connection does indeed have “shall provide both”.
* Not recognized case has “may provide both” (so not mandatory to provide, but if one is provided, so is the other).
* Recognized case has “may provide device ID” for the association case and “shall provide PASN ID” for the PASN case
* These differences seem to be appropriate for the actual use cases. Recognized device ID remains valid for future uses (since it is encrypted when STA provides it) and as such, there is no shall requirement to update. A new PASN ID is not needed when the previously one was not used (the association case). In the PASN case, a new PASN ID shall be provided (since the old one was sent without encryption), but there is no need to change the device ID since the previously provided value remains valid.