IEEE P802.11
Wireless LANs

|  |
| --- |
| AP rules on providing device ID and PASN ID |
| Date: 2024-07-17 |
| 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.

Revision 1 is updated based on the discussion and strawpolls in TGbh.

In addition, this document proposes changes to address CID 4002 and 4113 with REVISED. Incorporate changes from the Proposed changes – part 1 and 2 sections of <this document>.

**Review of the current draft language**

**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.
* Even if there is no strict requirement to updatre PASN ID in some cases, there has been prior discussion that prefers to update the shorter term PASN ID whenever the longer-term device ID is changed.
* SPs in TGbh indicated that there would be support for changing the initial connection case and not-recognized case to make it optional for the AP to provide a new device ID. This is to cover the exception cases where an AP cannot provide a new device ID.

**Proposed changes – part 1**

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

**12.2.13.1 Device ID**

An AP that has dot11DeviceIDActivated equal to true advertises support for the device ID mechanism by setting the Device ID Support field to 1 in the Extended RSN Capabilities field in the RSNXE (see 9.4.2.240 (RSNXE)) in Beacon and Probe Response frames.

A non-AP STA that has dot11DeviceIDActivated equal to true sets the Device ID Support field to 1 in the Extended RSN Capabilities field in the RSNXE to indicate that the device ID mechanism is supported. The RSNXE with the Device ID Support field equal to 1 is present in either (Re)Association Request frames or the first PASN frame that is sent to an AP that advertises support for the device ID mechanism.

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 uses PASN, i.e., when dot11PASNActivated is true, shall set dot11KEKPASNActivated to true.

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 Support 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 Support field set to 1.

— include an Extended RSN Capabilities element in the second PASN frame with the Device ID Support field set to 1.

For correct operation of the device ID mechanism, all APs in an ESS need to have dot11DeviceIDActivated set to true.

NOTE 1—The criteria and mechanism to distribute device IDs to the APs in the ESS is out of scope of this standard.

A STA should not send a frame containing a Device ID element or a PASN ID element to any STA unless the receiving STA has set the Device ID Support field to 1 in the Extended RSN Capabilities field.

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, the AP may provide both a device ID and, if dot11PASNActivated is true, 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 may provide a device ID in the Device ID element and if dot11PASNActivated is true 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 may provide a device ID in the Device ID KDE and, if dot11PASNActivated is true, a PASN ID in the PASN ID KDE in message 3 of the 4-way handshake.

NOTE 2—An AP is expected to provide a device ID and a PASN ID in the general case, but the AP might not be able to do that in some cases, e.g., due to not having sufficient resources or access to an external server to generate an identifier that is shared with all APs in the ESS.

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.

If a non-AP STA has been provided a device ID and a PASN ID by an ESS, then it may provide that device ID when returning to that ESS. It provides the device ID as follows:

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

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

P37 L63-P38 L5 Generic text that might have meant to be conditional on the previous paragraph or alternatively, this could be general rules that describes all cases where an AP provides a device ID. The latter is the direction proposed in the changes here. This paragraph could be moved to be earlier in this subclause.

When an AP provides a device ID, the AP shall provide both a device ID and, if dot11PASNActivated is true, a PASN ID as follows:

1) When using FILS authentication, the AP shall provide a device ID in a Device ID element and, if dot11PASNActivated is true, a PASN ID in a PASN ID element in the Association Response frame.

2) When using PASN, the AP shall provide a device ID in a Device ID subelement and, if dot11PASNActivated is true, a PASN ID in a PASN ID subelement encrypted in a PASN Encrypted Data element in the second PASN frame.

3) When not using PASN or FILS authentication, the AP shall provide a device ID in a Device ID KDE and, if dot11PASNActivated is true, a PASN ID in a PASN ID KDE in message 3 of the 4-way handshake.

If a non-AP STA has been provided with a device ID and a PASN ID, then it may provide the PASN ID in the PASN ID element in the first PASN frame, when using PASN authentication. An AP shall provide a PASN ID in the PASN ID subelement in the second PASN frame, when using PASN authentication.

The value of PASN ID shall be random and not shorter than 6 octets.

A STA may delete either or both of a stored device ID and a stored PASN ID at any point in time for implementation specific reasons.

When a non-AP STA sends a device ID or a PASN ID to an AP, it shall use the device ID or the PASN ID most recently received from any AP belonging to the same ESS.

P38 L22-L30 (association, recognized)

When an AP with dot11DeviceIDActivated equal to true receives an Association Request frame or a message 2 of the 4-way handshake, 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) in an Association Response frame or a message 3 of the 4-way handshake.

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 and, if dot11PASNActivated is true assign a new PASN ID value in the PASN ID field and set the PASN ID Status field of the PASN ID KDE or PASN ID element to 0, in in an Association Response frame or a message 3 of the 4-way handshake.

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.

When a non-AP STA receives a frame that contains a Device ID Status field in the Device ID KDE or Device ID element equal to 0, or a PASN ID Status field in the PASN ID element equal to 0, indicating Recognized, it proceeds with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.13 (Identifying a non-AP STA with changing MAC address)) is now bound to the MAC address in the Address 2 field in the Association Request frame or the first PASN frame most recently transmitted by the non-AP STA.

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.

NOTE 3—An AP is expected to provide a device ID and a PASN ID when the AP does not recognize the provided device ID or PASN ID, but the AP might not be able to do that in some cases, e.g., due to not having sufficient resources or access to an external server to generate an identifier that is shared with all APs in the ESS.

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.

When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Device ID element equal to 1, or a PASN ID status field in a PASN Status field in a PASN ID 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 12.2.13 (Identifying a non-AP STA with changing MAC address)).

NOTE 4—When using PASN authentication, the Device ID element is included in the Encrypted Data field of the PASN Encrypted Data element (see 12.13.11 (Encrypting the Encrypted Data field for PASN)).

An AP may use the procedure in Annex , or any other procedure (including nothing if the device ID or PASN ID is encrypted by the AP itself), to keep the device ID or PASN ID content private (opaque) from third parties when sent over the air.

**Proposed changes – part 2**

**P21L25 Please note changes of PASN ID are related to MLME-ASSOCIATION.confirm and .response primitive based on the CR doc 24/789r9, while the changes occur in the MLME-ASSOCIATION.request and .response primitive of D5.0(Please check it,Carol)**

**6.5 MLME SAP primitives**

**6.5.7 Associate**

**6.5.7.2 MLME-ASSOCIATE.request**

**6.5.7.2.2 Semantics of the service primitive**

***Change the primitive parameters list as follows (not all parameters are shown):***

**The primitive parameters are as follows:**

**MLME-ASSOCIATE.request(**

**...**

**Device ID,**

**IRM,**

**VendorSpecificInfo**

**)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| **Device ID** | **Device ID element** | **As defined in 9.4.2.316 (Device ID element)** | **Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |
| **IRM** | **IRM element** | **As defined in 9.4.2.317 (IRM element)** | **Specifies the IRM for the requesting** **STA. Optionally present if dot11FIL-****SActivated is true and dot11IRMActi-****vated is true, otherwise not present.** |
|  |  |  |  |

**6.5.7.3 MLME-ASSOCIATE.confirm**

**6.5.7.3.2 Semantics of the service primitive**

***Change the primitive parameters list as follows (not all parameters are shown):***

**The primitive parameters are as follows:**

**MLME-ASSOCIATE.confirm(**

**...**

**Device ID,**

**IRM,**

**PASN ID,**

**VendorSpecificInfo**

**)**

***Add the following rows to the parameter description table before the VendorSpecificInfo row (header row***

***shown for convenience):***

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| **Device ID** | **Device ID element** | **As defined in 9.4.2.316 (Device ID element)** | **Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.** |
| **IRM** | **IRM element** | **As defined in 9.4.2.317 (IRM element)** | **Specifies the IRM for the requesting** **STA. Optionally present if dot11FIL-****SActivated is true and dot11IRMActi-****vated is true, otherwise not present.** |
| **PASN ID** | **PASN ID element** | **As defined in 9.4.2.xxx (PASN ID element)** | **Specifies the PASN ID for the requesting STA.PASN ID is only present if Device ID is present.** |

***P32L40 please note this is a typo***

**9.4.2.320 PASN ID element**

**The PASN ID element contains a PASN ID. The format of the PASN ID element is shown in Figure 9-**

**1074h (PASN ID element format).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Element ID** | **Length** | **Element ID Extension** | **PASN ID Length** | **PASN ID Status** | **PASN ID** |

**Octets: 1 1 1 1 0 or 1 variable**

**Figure 9-1074h -**PASN ID element format

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

**The PASN ID Length field contains the length of the PASN ID field.**

**When the element is sent from an AP, the PASN ID Status field is defined in Table 9-417d (PASN ID Status field values).**

**When the element is sent from a non-AP STA, the PASN ID Status field is not present.**

**12.7.2 EAPOL-Key frames**

**P42L1 please note cited sentence(P38L12) :*the value of PASN ID shall be random and not shorter than 6 octets*.**

**The format of the PASN ID KDE is shown in Figure 12-50c (PASN ID KDE format).**

|  |  |
| --- | --- |
| **PASN ID Status** | **PASN ID** |

**Octets: 0 or 1 variable**

**The PASN ID Status field is defined in 9.4.2.320 (PASN ID element).**

**The PASN ID field contains a PASN ID.**

**Please note PASN ID KDE may carried in the message 3 of 4-way handshake based on the CR doc 24/789r9, (Please check it,Carol)**

**12.7.6 4-way handshake**

**12.7.6.1 General**

***Modify the following text as shown.***

**RSNA defines a protocol using EAPOL-Key frames called the 4-way handshake. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:**

**Message 1:Authenticator  Supplicant: EAPOL-Key(0 or 1,0,1,0,P,0,0,ANonce,0,{[PMKID]})**

**Message 2:Supplicant  Authenticator: EAPOL-Key(0 or 1,1,0,0,P,0,0,SNonce,MIC,{RSNE [,RSNXE]**

**[,OCI] [, Device ID KDE]})**

**Message 3:AuthenticatorSupplicant:**

**EAPOL-Key(1,1,1,1,P,0,RSC,ANonce,MIC,{RSNE [, RSNXE] [, OCI], GTK(N) [, IGTK(M,**

**IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R. WIPN)] [, SSID] [, Device ID KDE] [, IRM KDE] [, PASN ID KDE]})**

**Message 4:Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC, {[IRM KDE]}).**

**Please note PASN ID KDE may also carried in the message 3 of FT 4-way handshake**

**13.4.2 FT initial mobility domain association in an RSN**

**Change the following text as shown.**

**The R1KH and S1KH then perform an FT 4-way handshake. The EAPOL-Key PDU notation is defined in**

**12.7.4 (EAPOL-Key PDU notation).**

**R1KH->S1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {})**

**S1KH->R1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE(PMKR1Name) [, RSNXE], MDE,**

**FTE [, Device ID KDE]})**

**R1KH->S1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE(PMKR1Name) [, RSNXE], [,**

**OCI], MDE, FTE, TIE(ReassociationDeadline), TIE(KeyLifetime), GTK(N) [, IGTK(M, IPN)] [,**

**BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, Device ID KDE] [, IRM KDE] [, PASN ID KDE]})**

**S1KH->R1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {[IRM KDE]})**