IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bh D0.2 CRs related to 12.2.11 |
| Date: 2024-02-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Kurt Lumbatis | Arris/CommScope |  |  | Kurt.lumbatis@commscope.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions to the following CIDs.

CID 2, CID 3, ~~CID 4~~, CID 6, CID 10, CID 11, CID 25, ~~CID 26~~, CID 30, CID 31, CID 33, CID 49, CID 50, CID 51, CID 52, CID 53, CID 54, CID 55, CID 63, CID 65

Revisions:

* Rev 0 – Initial version of the document
* Rev 1 – Updated and cleaned up text
* Rev 2 – Updated text based on comments received for 22/1218
* Rev 3 – Incorporated edits and comments offered by Mark Rison, as well as edits made in the 09/06/2022 session.
* Rev 4 – add original text and edits based on review in the 09/12 Plenary meeting
* Rev 5-7 Additional wordsmithing and changes per comments received.
* Rev 8 – Edits made in first November session.
* Rev 9 – Edits to comment resolution table.
* Rev 10 – Further Edits to comment resolution table and text changes per comments received.
* Rev 11 – Comment resolution table fixes, and text modifications.
* Rev 12 – Updates based on IEEE 802.11-23/0083r1
* Rev 13 – Add straw poll and update per discussions of 01/17/2023
* Rev 14 – Re-written to clarify Actions and add Recognized vs Unrecognized from 23/0083r3
* Rev 15 – Added Identity state to text for clarity. Ready for motion.
* Rev 16 – Replaced generic Identity with device ID when referencing the actual device identifier being exchanged.

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 TGbh D0.2 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbh D0.2 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

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

| **CID** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- |
| 2 | Jay Yang | please clarify what's the meaning of "opt-in" | as the comments | Revised:Resolve by removing opt-in and replacing with text in 12.2.11 describing actions taken by the non-ap STA indicating Device ID activated per submission 11-22-1599r3TGbh Editor: Incorporate the Text changes in 11-22-1599r3 and 11-22-1329r15  |
| 3 | Jay Yang | """When using FILS authentication, the non-AP STA sends the identifier"", need to clarify the identifier here, | as the comments | Revised:Text changes provided to the editor with the breakout of FILS and non-FILS sections in the provided text for both non-AP STA and AP.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| ~~4~~ | Jay Yang | "AP sends a new identifier", before AP send a new one, AP shall verify the old one, need to add verification sucessful and failure case. | as the comments | Revised:Resolve by edits to the baseline text describing the process utilized by the AP when it has received a Device ID from a non-AP STA.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 6 | Jay Yang | the device ID verification proceudre is missing, need to add this part | as the comments | Revised:Text changes provided with the addition of added text which states recognized and non-recognized Identifier use cases.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 10 | Jay Yang | """if it has one and opts-in to using it"" | as the comments | Revised:Resolved with changes to the baseline text defining what Device ID active means, (11-22-1599r3) as well as a may statement for the non-ap STA to provide the Identifier to the AP.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 11 | Jay Yang | the device ID doesn't need to be updated in each assocation as it's exchanged in protected frame, it's very safe. | change to "and the AP may sends a new identifier in the EAPOL-Key message 3/4". also, add some sentece to say"if the identifier is not updated in the association, the STA will use the old one." | Revised:Additional text added to where the Identifier is passed for the differing use cases and in which frames. There is no stipulation that an AP send a new Identifier per association.An AP sends an Identifier if it has activated Device ID per the following: 1) When using FILS authentication in the Device ID element in the (Re)Association Response frame. 2) When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 15 | Antonio DeLaOlivaDelgado | There should be normative text explaining what to do with the Device ID and most importantly what to do if the Device ID does not match a previous registration | as the comments | Revised:TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 25 | Okan Mutgan | "When the non-AP STA sends the opaque identifier, it shall send the most recently received value from anAP in the ESS without modification."This sentences uses "opaque identifier", whereas the rest of the paragraph uses "identifier". To be compatible within the paragraph, I suggest to change it to "identifier".Generally speaking, there are various definitions in the protocol such as "identifier" , "opaque identifier", "blob", "ID". All of them need to be explained clearly in the context. | "When the non-AP STA sends the identifier, it shall send the most recent received value from an AP in the ESS" | Revised: A non-AP STA shall return the most recently received Identifier for an ESS when associating with any AP in that ESS when Device ID is active for both the non-AP STA and the AP.Awaiting final definition of what Identifier is and what terms need to be defined.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 26 | Okan Mutgan | Generally speaking, device ID verification (fail ,success) should be considered in the protocol. | as the comment | Revised:Text changes provided with the addition of added text which states recognized and non-recognized Identifier use cases.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 30 | Chaoming Luo | Does this mean an AP shall indicate support for this capability? | Please Clarify | Revised:Text added defining how the non-AP STA and AP indicates support for Device ID active and in which frames this indication shall reside.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 31 | Chaoming Luo | It's not clear how the transition (ie., has no ID -> has one ID) happens, because at the very beginning the non-AP STA does have one identifier and the ID staff described in this paragragh does not occur. | Please Clarify | Revised:When a non-AP STA with Device ID active associates to any AP in an ESS and does not provide an Identifier, the AP shall assign an Identifier to the non-AP STA. TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 33 | Amelia Andersdotter | At the risk of me word-smithing, maybe the discussions are better reflected by the following wording: "An AP may provide an identifier to a non-AP STA and the non-AP STA may optionally return that identifier to any AP in the same ESS..." | as in comment | Revised:Text changes in the provided text utilizing the terms may and shall in the appropriate text.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 49 | Robert Stacey | "Opt-in to providing" is cumbersome. "In the same ESS" -- there is no precedent for "same". | Change to "During association, an AP may provide an identifier to a non-AP STA. The non-AP STA may include that identifier in a future association exchange with any AP in the same ESS as the AP that originally provided the identifier. This allows the AP with which the non-AP STA is associating to recognize the non-AP STA from a prior association even though the MAC address might have changed." | Revised:An AP may provide an Identifier to a non-AP STA to allow any AP in the ESS to recognize the non-AP STA when it returns to that ESS even if the non-AP STA changes its MAC Address. The non-AP STA may provide that Identifier to any AP in the same ESS upon a new association. Exchanges of the Identifier are protected from third parties.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 50 | Robert Stacey | "If inclusion of the identifier in an Association Request frame is restricted to FILS authentication then we need a shall statement to that effect. | Replace 1st sentence of paragraph with"A non-AP STA may include the identifier in an Association Request frame if FILS authentication is used and shall not include the identifier an Association Request frame if FILS authentication is not used.An AP may include an identifier that has not previously been used in an Association Response frame if FILS authentication is used and shall not include include an identifier in an Association Response frame if FILS authentication is not used." | Revised:Modified text to clarify FILS, vs non-FILS passage of the Identifier and what the mechanisms are to pass the Identifier for both AP and non-AP STA.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 51 | Robert Stacey | "If inclusion of the identifier is restricted to the EAPOL Key messages for FT, then we need a shall statement to that effect. | For FT association the following applies:- A non-AP STA may include the identifier in EAPOL-Key Message 2 frame of the initial mobility domain association- An AP may include an identifier that has not previously been used in the EAPOL-Key Message 3 frame- An identifier shall not be included in EPOL Key messages exchanged during FT protocol reassociations. | Revised:Modified text to clarify FILS, vs non-FILS passage of the Identifier and what the mechanisms are to pass the Identifier for both AP and non-AP STA.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 52 | Robert Stacey | """For other cases"" might not be clear enough; better to enumerate. | Change to "If neither FILS authentication nor FT association are used, then the following apply:- The non-AP STA may include an identifier in the EPOL Key Message 2 frame of the initial 4-way handshake.- An AP may include an identifier that has not previously been used in the EPOL Key Message 3 frame of the initial 4-way handshake." | Revised:Modified text to clarify FILS, vs non-FILS passage of the Identifier and what the mechanisms are to pass the Identifier for both AP and non-AP STA.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 53 | Robert Stacey | "opaque identifier" is not defined and it is not clear how it differs from an "identifier'. Similarly, what distinguishes a "new identifier" from an "identifier" | Either substitute "opaque identifier" with something meaningful or define the term. Replace "new identifier" with "identifier that has not previously been used" (or similar) | Revised:Removed text and replaced all with Identifier. TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 55 | Robert Stacey | "for this capability" is vague | "A non-AP STA indicates support for device ID indication in the Device ID Support subfield in the ..." | Revised:Revised the text to indicate the fields where support is indicated for both AP and non-AP STA. Additionally added which frames shall contain these support fields.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 63 | Mark Hamilton | Clarify "and the non-AP STA may opt-in" | Replace "STA may opt-in to providing" with "STA may provide". Replace "opts-in to using it" with "chooses to use it", at P26.19, P26.22 and P26.26. At P17.17, replace "can opt-in" with "can choose". At P26.13, add a "NOTE--It is recommended that the non-AP STA device provide the end user or administrator with a mechanism to control when the device will choose an identifer, or provide no identifier, for a given network. | Revised:Not completely resolved but modified text with Device ID active No text is added regarding administrator control but added a MIB in 11-22-1599r3 to control whether the upper layers have activated Device ID on a per SSID basis.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |
| 65 | Jarkko Kneckt | The STA Identifier should be taken into use only if the STA opts-in to use the identifier. Currently AP may just push a STA ID for the STA even if the STA does not want to have it. | Please allow the STA to have control on whether it desires to use STA identifier in the following authentications and associations. | Revised:Added the following:A STA shall not send an Identifier to any STA that does not indicate Device ID is active.TGbh Editor: Incorporate the text changes in 11-22-1329r15 |

# Proposed text(Proposed text modifications are based on Draft 11bh 0.2)

TGbh editor: Make the following changes in 4.5.4.10:

To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. While discovering network, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks. Such a STA, when reconnecting to a participating network may exchange a device ID that allows the network to recognize the device but protects the information from third parties.

TGbh editor: Make the following changes in 12.2.11 Device ID indication with the following:

This text incorporates the changes of 11-22/1082, and 11-22/1069

**12.2.11 Device ID indication**

An AP may provide a device ID to a non-AP STA to allow any AP in the ESS to recognize the non-AP STA when it returns to that ESS even if the non-AP STA changes its MAC Address. The non-AP STA may provide that device ID to any AP in the same ESS upon a new association. Exchanges of the device ID are protected from third parties.

A non-AP STA indicates activation of device ID for a particular ESS by setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.241 - RSNExtension Element) in (Re)Association Request frames sent to any AP in the ESS. An AP indicates activation of Device ID by setting the Device ID Active field to 1 in the Extended RSN Capabilities field in Beacon, (Re)Association Response, and Probe Response frames. All APs in a given ESS shall set this field to the same value.

A STA shall not send a device ID to any STA that does not indicate Device ID is active.

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

1. When using FILS authentication in the Device ID element in the (Re)Association Request frame.
2. When not using 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 FILS authentication in the Device ID element in the (Re)Association Response frame.
2. When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

A non-AP STA that is associating with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP and the non-AP STA has not previously associated with any AP in the ESS, shall not send a device ID in the non-AP STA Identity frame. Similarly, if the non-AP STA is associating with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP but the non-AP STA no longer has a device ID for that ESS for implementation-specific reasons (for example, configuration changes have lost the device ID, or sufficient time has passed since the last association to the ESS so that the device ID has been deleted), then the non-AP STA shall not send a device ID in the non-AP STA Identity frame.

A non-AP STA that is associating with any AP in an ESS with Device ID active for both the non-AP STA and the AP and the non-AP STA has a saved device ID for the ESS shall send the most recently received device ID for that ESS in the non-AP STA Identity frame.

When an AP with Device ID active receives a non-AP STA Identity frame from a non-AP STA with Device ID active and the received device ID is recognized, the AP shall perform one of the following actions:

1. Send a zero-length device ID and set Identifier Status to “Recognized” in the appropriate AP Identity frame.
2. Assign a new device ID to the non-AP STA, send the device ID, and set Identifier Status to “Recognized” in the appropriate AP Identity frame.

When a non-AP STA receives an AP Identity frame with Identifier Status equal to “Recognized” it can proceed with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.10) is now bound to the non-AP STA’s current MAC address.

When a non-AP STA receives an AP Identity frame with the Identifier Status equal to “Not Recognized”, it must assume that no shared state exists with the AP or ESS (as per the concepts of 12.2.10) and the non-AP STA must (re)establish any desired, shared identity state.

**Straw Poll**

**Shall we approve resolutions of the following CIDs and incorporate the text changes in 11-22/1329r15 and 11-23/0083r5 into the latest TGbh draft?**

**CIDs: 2, 3, 4, 6, 10, 11, 25, 26, 30, 31, 33, 49, 50, 51, 52, 53, 54, 55, 63, 65**

**No objection**

**References:**

***11-22/1082***

***11-22/1069***

***11-23/0083***

***11-22/1599***