IEEE P802.11
Wireless LANs

|  |
| --- |
| D1.0 CIDs in clause 10.71.1 |
| Date: 2025-05-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

Abstract

This submission proposes resolution of comments received against the following sections of TGbi Draft 1.0:

* 10.71.1 (Introduction),

We propose draft specification text for TGbi draft D1.1.

Accepted/Revised CID with changes in this document: 66, 67, 156, 223, 224, 225, 336, 514, 515, 516, 517, 938, 957, 958, 959, 1024, 1029, 1030, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039

Accepted CID with changes addressed by other CID (shown in brackets) in this document:

221 (1024), 510 (156), 511 (66), 512 (223), 795 (514), 796 (514), 797(514), 798 (517), 941 (516), 1031 (223)

Rejected CID: 65, 513, 1025, 1026, 1027, 1028

Open CID: 153, 222

Revisions:

* Rev 0: Initial version of the document.

| **CID** | **Commenter** | **Page.Line** | **Duplicate of CID** | **Comment** | **Proposed Change** | **Done** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 512 | Mark RISON | 75.02 |  223 | At 25.1 we have "An AP MLD supporting BPE EDP features may reduce the availability of information about itself to a third party observer such as the ESS to which it belongs" but at 75.26 we have "Frame anonymization addresses unencrypted fields and elements in Beacon frames and individually addressed frames containing values that facilitate presence monitoring of a non-AP MLD", so it's not clear whether BPE is about the privacy of the AP or of the non-AP. Ooh, and in 10.71.8 it's both: "BSS Privacy Enhancement (BPE) operations protect privacy of BPE AP MLDs and associated BPE non-AP MLDs."! | Clarify the intent of BPE | **Dup** | DUPLICATE |
| 65 | Graham Smith | 75.18 |   | Frame anonymization has one aim, to counter "presence monitoring". It is not obvious what this is (i.e., how does it work such that a third party finds it useeful) or how effective FA is. The counter is simply to change the STAs parameters every now and then. Was any presentation given on how often the changes are needed in order to be effective, (1 day, 1 hour, 1 minute, 1 second?) or indeed what presence monitoring actually achieves (STAs are using random MACs)? Also, how many associated STAs are required to make FA effective (10, 100, 1000)? FA is a lot of work, and no indication is given as to how it really helps or what the criteria are. To convince me that this is useful, I would need to see an Annex at the least as to how it works and the criteria required for it to work | Either add an Annex or add text to introduction that shows the crtieria (e.g., min or max time slots, and number of assciated STAs) required that prove that FA is useful or delete the whole thing. | **Rej** | **Rejected**FA provides a range of parameters to provide a range of choices implementers and users. Recommendations on those parameters are best left to industry organizations, not 802.11.  |
| 958 | Robert Stacey | 75.20 |   | Historically, we have interpreted "Introduction" to imply "informative". I don't necessarily agree with this, but that is the reason we use "General" and not "Introduction". | Change "Introduction" to "General" (since this subclause clearly has normative requirements). | **Rev** | **Revised**.Principle: Keep clause 10.71.1 (Introduction) informative and add a new normative clause 10.71.1a (General). Changes:P75 line 23: replaces “when MLO is supported” to “when MLO is enabled”. Note that the remainder of this sentence is changed by CID 156.P76 line 17: Add new heading “10.71.1a (General).”Following heading, add following text:“The FA feature may be enabled if only if MLO is enabled.The FA feature shall be enabled if and only if dot11EDPGroupEpochActivated is true.“*[Phil] This last sentence is added because I can’t find any other description of how to enable FA.*Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #958 |
| 153 | Stephen McCann | 75.22 |   | If you expand "EDP CPE" you have "Enhanced Data Privacy Client Privacy Enhancements". I think some of this terminology can be optimised. | Replace "EDP CPE" with "CPE" and also at P81L44, P81L47 and P82L3. | **OPEN** | **OPEN**The change to P75 line 22 rejected – the correct change is shown in CID1024 in Document 25/0951r00. *[Phil] The remaining proposed changes in P81L44, P81L47 and P82L to be addressed with other 10.71.3 CIDs in a separate document..* |
| 510 | Mark RISON | 75.22 | 156 | "DS MAC address" is missing an article | Prepend "a " | **Dup** | DUPLICATE |
| 156 | Stephen McCann | 75.23 |   | What does "DS MAC address supported" mean? How can you support a MAC address? | Change "DS MAC address supported" to "the use of a destination MAC address is supported". | **Rev** | **Revised**. Principle: It is easier to refer to dot11DSMACAddressActivated. Also easier to refer to “enabled” rather than “support”. Change:P75: line 23: Delete “and DS MAC address supported” since this detail is not necessary in an introduction.P76 line 17 (after text added by CID 958) add: “The FA feature may be enabled if and only if dot11DSMACAddressActivated is true.“Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #156 |
| 1024 | Philip Hawkes | 75.23 |   | FA provides CPE features and BPE features. | Replace "EDP CPE feature" with "EDP feature" | **Acc** | **Accepted**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1024 |
| 221 | Jarkko Kneckt | 75.23 | 1024 | The frame anonymization clause should introduce BPE MLDs. The BPE MLDs should be mentioned in the first sentence and there should be clear introduction to both operations easily available. | Change the first sentence to read:" Frame anonymization (FA) is an EDP feature available when MLO is supported." | **Dup** | DUPLICATE |
| 222 | Jarkko Kneckt | 75.23 |   | There DS address has value for non-MLO devices. For MLDs, i.e. operation with the CPE and BPE operations DS address does not have value. The DS address is very similar with MLD address.If a (CPE /BPE) non-AP MLD is identified by PMKID, then link address and MLD address can be selected freely. | Allow CPE and BPE MLDs to operate without the DS MAC Address. | **OPEN** | *[Phil] I am not clear about the difference between MLD address and DS address, so I cannot comment? Who should I work with on this?* |
| 938 | Srinivas Kandala | 75.26 | 959 | Based on the description here I am unable to comprehend how this presence monitoring (likely by some nebulous actor) is accomplished. Can you describe how this threat would develop? I agree that presence monitoring is a threat, but I could not figure out how one can get there. Unless this can be clarified and explained adequately I cannot be sure what problem this amendment is attempting to solve | Please clarify, preferably in clause 4 | **Rev** | **Revised**Principle: Include a note towards the start of the clause that explains presence monitoring using description suggested in 959 and describes what FA is doing. This text is based on the current text in lines p75 lines 26-47 – and that existing text is deleted. It then makes sense to move the note at p76 line 9 to this location as NOTE 3, to keep the notes in a single place. In that note, “presence monitoring” is replaced by “third parties detecting a person’s presence”. An additional NOTE 2 is added by CID 225.Changes:P75 line 24: append the following text to the end of the paragraph:“The objective of FA is that, for the set of values assigned to an MLD that are transmitted in unencrypted fields and elements, those values remain static or predictable only within configurable time windows called EDP Epochs.P75 line 25: add the following note:“NOTE 1—When values assigned to an 802.11 device are (a) static or predictable and (b) transmitted in unencrypted fields and elements, then those values can be used by a third party determining the long-term presence of a person at a location, even if the identity of the person cannot be determined. Without frame anonymization enabled, the values transmitted in these unencrypted fields and elements remain static or predictable until a new association is performed, even when other EDP features are enabled. Examples of unencrypted fields and elements that contain static or predictable values assigned to an 802.11 device include: Address fields, including transmitter address (TA), receiver address (TA), source address (SA) and receiver address (SA); Sequence Number (SN); Packet Number (PN); Timestamp; Association Identifier (AID) and fields and elements derived from the AID. A third party can monitor the values transmitted in these fields and, as long as the values remain static or predictable, the third party can determine that the 802.11 device continues to be present at that location. In some cases, the location could be fixed (relative to earth) while in other cases the location could be a vehicle in motion. FA improves user privacy by restricting the time windows within which unencrypted fields and elements remain static or predictable, thereby increasing the effort required for a third party to determine the long-term presence of the person.“*Parts of the NOTE 1 include changes suggested by CIDs 66, 67, 959, 1029 and 1030. Refer to those CIDs for details.*P75 line 25: add the following note after NOTE 1:“NOTE 3—The following list clarifies the scope of attacks that FA mitigates:— FA mitigates against third parties determining a person’s presence across multiple FA epochs. — FA does not mitigate against third parties determining a person’s presence within a single FA epoch. — FA does not mitigate identifying frames transmitted from a single MLD within a single FA epoch.— FA does not mitigate using third parties determining a person’s presence across multiple FA epochs via traffic analysis using known transmission behavior of upper layer protocols.“*Parts of the NOTE 3 include changes suggested by CIDs 336 and 1039. Refer to those CIDs for details.*p76 line 9: Delete Note.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #938 |
| 959 | Robert Stacey | 75.26 |   | The purpose should be stated upfront and more clearly. Then get into the means. | Change to "Frame anonymization helps minimize presence monitoring. Presence monitoring is the determination by a third party that a person is present at a location over a period of time even if the identity of the person cannot be determined. With frame anonymization unencrypted fields in a frame are periodically changed so that the long term presence of the sender cannot easily be determine." | **Rev** | **Revised**Agre in principledChangesP75 line 24. Append the following sentence to the paragraph“The objective of FA is that, for the set of values assigned to an MLD that are transmitted in unencrypted fields and elements, those values remain static or predictable only within configurable time windows called EDP Epochs.“In new text introduced by CID 938.Instead of “presence monitoring “:- The first time - use a full description: “a third party determining the long-term presence of a person at a location, even if the identity of the person cannot be determined”- Elsewhere refer to: “a third party determining the long-term presence of a person”.- For Note 3 (which is currently in p76 line 9) replace “presence monitoring” with “third parties determining the presence of a person”, since the remainder of the text qualifies the duration of the presence.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #959 |
| 1025 | Philip Hawkes | 75.26 | 959 | FA provides CPE features which apply to group addressed frames, in addition to the frames identified here. | Replace "Beacon frames and individuallyaddressed frames" with "frames" | **Rej** | **Rejected** This text would be part of new NOTE 1 at line 26, which no longer refers to frames at all, since all fields and elements are transmitted in frames.  |
| 224 | Jarkko Kneckt | 75.26 | 1 | The Beacon frames are anonymized only in the BPE mode. | Please clarify that Beacon and AP parameters in general are anonymized only in the BPE mode | **Rev** | **Revised**This is clarified as part of CIDs 1033, 1034, 1035, 1036, 1037, 1038-1038. See those CID for details.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #224 |
| 1026 | Philip Hawkes | 75.27 | 959 | BPE FA prevents presence monitoring of AP MLD (in addition to non-AP MLD already noted) | Replace "non-AP MLD" with "MLD" throughout the paragraph (4 occurences) | **Rej** | **Rejected** The text that was in this paragraph has been deleted by CID 938. The change is no longer applicable. |
| 66 | Graham Smith | 75.31 | 959 | "It is possible to limit presence monitoring..." I think this would be better as a NOTE. Not sure also "by doing (re)association" is correct. Reassociation uses the same MAC address. | At cited location, make the final 2 sentences a NOTE. Also at 75.32 replace "by doing (re) association" with "by performing a new assocation" and at 75.34 delete "(re)"; and at 75.34 replace "could" with "might". | **Rev** | **Revised**This text was deleted by CID 938. However, NOTE 1 inserted at line 25 as part of CID 938 includes similar text related to (re)association, so the similar text to that proposed was included i.e. “…until a new association is performed”.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #66 |
| 511 | Mark RISON | 75.31 | 66 | "It is possible to limit presence moni-toring time windows by doing (re)association as defined in 11.3 (Authentication and association). However, (re)association results in leaving State 4 and introduces a loss in connectivity that could create a negative user experience. " sounds like a NOTE | Prepend "NOTE---" | **Dup** | DUPLICATE |
| 1027 | Philip Hawkes | 75.32 | 66 | "doing" is an imprecise verb for this situation. | Replace "doing" with "performing" | **Rej** | **Rejected** This text has been modified by CID 938. The change is no longer applicable. |
| 1028 | Philip Hawkes | 75.32 | 959 | There is not a clear indiication of what is "leaving State 4". | Replace "leaving State 4" with "the non-AP MLD leaving State 4". | **Rej** | **Rejected** This text has been deleted as part of by CID 938. The change is no longer applicable. |
| 223 | Jarkko Kneckt | 75.36 |   | The frame anonymization levels (CPE and BPE) should be described in the introduction. | Please add CPE and BPE introduction. | **Rev** | **Revised**Added the following text at line p75 line 18“FA mechanisms are partitioned into Client Privacy Enhancement (CPE) frame anonymization that mitigates detection of a non-AP MLD, and BSS Privacy Enhancement (BPE) frame anonymization that mitigates detection of a BSS (the BPE AP MLD and its associated non-AP MLDs). CPE FA is “baseline” FA; that is, CPE FA mechanisms are enabled whenever FA is enabled. BPE FA is optional for FA; that is, BPE FA can only be enabled when CPE FA is additional enabled.“Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #223 |
| 1029 | Philip Hawkes | 75.37 |   | This list applies to individual addressed frames only | Replace "The encrypted fields and elements..." with "The encrypted fields and elements of individually addressed frames..." | **Rev** | **Revised**It is simpler if this introduction provides a list of example encrypted fields and elements without referring to the type of frame. This list is now part of the new NOTE 1 inserted at line 25.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1029 |
| 1030 | Philip Hawkes | 75.44 |   | Lines 37-43 identified unencrypted fields and elements that facilitate presence monitoring of a non-AP MLD. Text is needed that identifies unencrypted fields and elements that facilitate presence monitoring of an AP MLD. | Insert the following text at line 44:"The unencrypted fields and elements that facilitate presence monitoring of an AP MLD are:--For all frames: Address 2 (on the downlink) and Address 1 (on the uplink).--For group addressed frames: Address 1 (on the downlink), Sequence Number (SN), Packet Number (PN).--For Beacon frames: Timestamp." | **Rev** | **Revised**It is simpler if this introduction provides an informative list of example unencrypted fields and elements without referring to the type of frame, and without providing the details for processing those fields and elements. This list is now part of the new NOTE 1 inserted at line 25.P75 line 59:“Address 1 field” 🡪 “Address 1 field of an individually addressed frame”P76 line 01:“Address 1 (on the downlink) or Address 2” 🡪 “the Address 1 field of an individually addressed frame (on the downlink), or the Address 2 field”P75 line 62: Inset new item- If BPE is enabled, then: - The value in the Address 1 field of a group addressed frame is transformed into an over-the-air value. - The Address 2 field (on the downlink), or the Address 1 field (on the uplink), is set to the temporary random MAC address of the affiliated AP of the AP MLD.P75 line 4: Inset new item- If BPE is enabled, then: - The over-the-air value in Address 1 field of a group addressed frame is transformed back to the original group MAC address assigned by the transmitting MLD. - The over-the-air value in Address 2 field (on the downlink), or the Address 1 field (on the uplink), is matched to the temporary random MAC address of the affiliated AP of the AP MLD.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1030 |
| 1031 | Philip Hawkes | 75.45 |  223 | There is no text explaining what FA provides with and without BPE enabled. | Insert the following text:"If an AP MLD does not have BPE enabled, then FA mitigates presence monitoring of non-AP MLDs only. If an AP MLD has BPE enabled, then FA mitigates presence monitoring of both non-AP MLDs only. " | **Dup** | DUPLICATE |
| 67 | Graham Smith | 75.46 |   | "FA enables restricting presence monitoring time windows..." It does not enable it, it actually does it. Suggest a rewrite of this para. | Replace cited paragraph with "FA defines time windows, known as EDP epochs, during a single association such that the parameters of unencrypted fields and elements are used for restricted time periods. In each EDP epoch, new parameter sets are used. EDP epoch operation is described in 10.71.2. The establishment of the FA new parameter set is described in 10.71.3" | **Rev** | **Revised**:“In each EDP epoch, a new frame anonymization parameter set (FA parameter set) is used. EDP epoch operation is described in 10.71.2 (EDP epoch operation). The establishment of the new FA parameter set is described in 10.71.3 (Establishing frame anonymization parameter sets).” Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #67 |
| 513 | Mark RISON | 75.46 |   | "presence monitoring time windows" should be "presence-monitoring time windows" now that the prohibition on using hyphens has been rescinded | As it says in the comment | **Rej** | **Rejected** This text has been deleted as part of by CID 938. The change is no longer applicable. |
| 1032 | Philip Hawkes | 75.52 |   | There is no text about AID anonymization | Insert the following text:The AP MLD anonymizes AID by assigning random temporary AID for each non-AP MLD. | **Rev** | **Revised**Add the following paragraph at list 7 (after the list)“The AID of a non-APMLD, and fields and elements derived from the AID, are anonymized using temporary, random AIDs assigned by the AP MLD.”Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1032 |
| 514 | Mark RISON | 75.57 |   | "over the air values" should be "over-the-air values". Also 75.65, 76.1/5 | As it says in the comment | **Acc** | **Accepted**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #514 |
| 515 | Mark RISON | 75.57 |   | "safely transmitted in the clear while maintaining anonymity" -- not clear what "safely" means here | Delete "safely" | **Acc** | **Accepted**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #515 |
| 1033 | Philip Hawkes | 75.59 |  1030 | Update this item to indicate that it applies to individually addess frames, and identify processing of affiliated AP addresses when BPE is enabled. | The Address 1 field and/or the Address 2 field of individually address frames are set to a temporary random MAC address for the affiliated STA of the non-AP MLD on the link on which the frame is transmitted and, if the AP MLD has BPE enabled, then a temporary random MAC address for the affiliated AP of the AP MLD on the link on which the frame is transmitted. | **Rev** | **Revised**P75 line 59:“Address 1 field” 🡪 “Address 1 field of an individually addressed frame”P75 line 62: Insert new item- If BPE is enabled, then: - The Address 2 field (on the downlink), or the Address 1 field (on the uplink), is set to the temporary random MAC address of the affiliated AP of the AP MLD.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1033 |
| 1034 | Philip Hawkes | 75.62 |  1030 | There is no text about group addressed frames. | Insert the following bullet in the list:- For group addressed frames transmitted by an AP MLD with BPE enabled, the Address 1 field transformed into over the air values that can be safely transmitted in the clear while maintaining anonymity. and the Address 2 field is set to a temporary random MAC address for the affiliated AP of the AP MLD on the link on which the frame is transmitted. | **Rev** | **Revised**P75 line 62: Insert new item after change in CID 1033 - The value in the Address 1 field of a group addressed frame is transformed into an over-the-air value.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1034 |
| 1035 | Philip Hawkes | 75.62 |   | There is no text about Timestamp anonymization when BPE is enabled | Append the following bullet to the list:- If the AP MLD has BPE enabled, then the Timestamp in Privacy Beacon frames are transformed into over the air values that can be safely transmitted in the clear while maintaining anonymity. | **Rev** | **Revised**P75 line 62: Insert new item after change in CID 1034 - The Timestamp (assigned by the AP MLD) in the Privacy Beacon is transformed into an over-the-air value that can be transmitted in the clear while maintaining anonymity of the AP MLD.Document 25/0951r00 accounts for resolution of this CID. Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1035 |
| 516 | Mark RISON | 75.63 |   | "The intended receiving MLD" is normally just known as "The receiving MLD" | Change as suggested | **Acc** | **Accept**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1035 |
| 941 | Robert Stacey | 75.63 | 516 | The word "intended" in "intended receiving" is superfluous. If the intended receiving MLD does not receive anything how can it know what it is supposed to do? It only makes sense to define behavior for the device that actually receives something. | Delete "intended" | **Dup** | DUPLICATE |
| 795 | John Wullert | 75.65 | 514 | When used as a single adjective, "over the air" should be hyphenated | Change "over the air" to "over-the-air" | **Dup** | DUPLICATE |
| 796 | John Wullert | 76.01 | 514 | When used as a single adjective, "over the air" should be hyphenated | Change "over the air" to "over-the-air" | **Dup** | DUPLICATE |
| 1036 | Philip Hawkes | 76.01 |   | Update this item to indicate that it applies to individually addess frames, and identify processing of affiliated AP addresses when BPE is enabled. | Replace the bullet text with the following:During address filtering of individually addressed frames, the over the air value(s) in the Address 1 field and/or the Address 2 field are matched to the temporary random MAC address for the affiliated STA of the non-AP MLD on the link on which the frame is transmitted and, if the AP MLD has BPE enable, the temporary random MAC address for the affiliated AP of the AP MLD on the link on which the frame is transmitted. | **Rev** | **Revised**P76 line 01:“Address 1 (on the downlink) or Address 2” 🡪 “the Address 1 field of an individually addressed frame (on the downlink), or the Address 2 field”P75 line 4: Insert new item- If BPE is enabled, then: - The over-the-air value in Address 2 field (on the downlink), or the Address 1 field (on the uplink), is matched to the temporary random MAC address of the affiliated AP of the AP MLD.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1036 |
| 1037 | Philip Hawkes | 76.04 |   | There is no text about filtering group addressed frames. | Insert the following bullet in the list:During address filtering of group addressed frames transmitted by an AP MLD with BPE enabled, the over the air value in the Address 2 field is matched to a temporary random MAC address for the affiliated AP of the AP MLD on the link on which the frame is transmitted, and the the over the air value in the Address 1 field is transformed back to the original group address assigned by the AP MLD. | **Rev** | **Revised**P75 line 4: I Insert new sub item after change in CID 1036: - The over-the-air value in Address 1 field of a group addressed frame is transformed back to the original group MAC address assigned by the transmitting MLD.Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1037 |
| 797 | John Wullert | 76.05 | 514 | When used as a single adjective, "over the air" should be hyphenated | Change "over the air" to "over-the-air" | **Dup** | DUPLICATE |
| 1038 | Philip Hawkes | 76.07 |   | There is no text about Timestamp anonymization when BPE is enabled | Append the following bullet to the list:- If the AP MLD has BPE enabled, then the over the air values for the sequence Timestamp in Privacy Beacon frames are transformed back t the original timestamp assigned by the AP MLD. | **Rev** | **Revised**P75 line 7: Insert a new item“- If BPE is enabled, then: - The over-the-air Timestamp in the Privacy Beacon is transformed back to the original Timestamp assigned by the AP MLD. “Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1038 |
| 336 | Carol Ansley | 76.11 |   | "Mitigating against" is poor wording | Remove "against", "mitigating" already means reducing the impact of. | **Acc** | **Accept**Document 25/0951r00 accounts for resolution of this CID. . Instruction to the editor: apply changes referenced with tag: #336 |
| 1039 | Philip Hawkes | 76.15 |   | "mitigate using traffic analysis using" sounds awkward with two occurences of the word "using". | Replace with "mitigate traffic analysis using" | **Acc** | **Accept**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1039 |
| 798 | John Wullert | 76.19 | 517 | Requirements indicate that MSDUs should/shall be transmitted in A-MSDUs. It is not totally clear whether these requirements hold when a STA has only a single MSDU to transmit. | Revise requirements on CPE STAs and BPE STAs to clarify handling of single MSDUs. (Could be added as a note.) | **Dup** | DUPLICATE |
| 957 | Robert Stacey | 76.19 |   | When writing a requirement, it is better to use the singular. The plural is not implementable or testable (an implementor has design control over one implementation not all implementations). Also, if you define one way of doing something it applies in all instances. Finally, introduce the requirements with the statement in the note -- it help understanding. | Replace the two sentences at 76.19 and 76.21 as well as the NOTE with the following:"In order to provide confidentiality for the SA and DA, the following apply:- A CPE STA should transmit an MSDU in an A-MSDU.- A BPE STA shall transmit an MSDU in an A-MSDU." | **Acc** | **Accept**Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #957 |
| 225 | Jarkko Kneckt | 76.19 |   | Introduction should describe how SA and DA can be used for STA tracking. | Please add justifications for SA and DA protection to the introduction. | **Rev** | **Revised***[Phil] I think we should consider rejecting this CID, since we don’t provide such details for other fields. I have proposed some text below, but I am also fine with rejecting this CID*Add the following text at p75 line 25 after NOTE 1 added by CID 938.“ NOTE 2— When present, SA (or DA respectively) provides the MAC address of the source (or destination respectively) of the frame when the source is distinct from the transmitter (or the destination is distinct from the receiver respectively). These MAC addresses can remain unchanged for a relatively long time; in many cases these MAC addresses never change. If SA and/or DA are not encrypted, then a non-AP MLD in a BSS or ESS might be profiled according to the frequencies of SA and/or DA in frames transmitted or received by those non-AP MLDs. This might be exploited to detect a person’s presence.“Instruction to the editor: apply changes referenced with tag: #225 |
| 517 | Mark RISON | 76.23 |   | But it could be an A-MSDU with just one MSDU | Add to the NOTE: "An A-MSDU can contain a single MSDU." | **Rev** | **Revised**Delete the note at p76 line 23.Add the following text at p76 line 7 after the text added by CID 1032.“FA uses transmission of MSDUs in A-MSDUs to provide confidentiality of SA and DA, noting that an A-MSDU can contain a single MSDU – see 10.71.1a (General).“Document 25/0951r00 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #517 |

**Background**

Clause 10.71.1 was written before text for BPE was stable, so some changes are needed to account for BPE.

Clause 10.71.1 included some normative text, while an “Introduction” is informative. A new section 10.71.1a (General) is proposed, where normative text is moved.

The description of the threat (currently “presence monitoring”) is improved, along with some description of the objective of Frame Anonymization.

**Proposed spec text:**

***TGbi editor: Apply the following changes to 10.71.1 (Introduction). The baseline for this text is Draft P802.11bi\_D0.5.***

* **Introduction**

Frame anonymization (FA) is an EDP(#1024) feature available when MLO is enabled(#TBD) (#156). The objective of FA is that, for the set of values assigned to an MLD that are transmitted in unencrypted fields and elements, those values remain static or predictable only within configurable time windows called EDP Epochs. (#959)

NOTE 1—When values assigned to an 802.11 device are (a) static or predictable and (b) transmitted in unencrypted fields and elements, then those values can be used by a third party determining the long-term presence of a person at a location, even if the identity of the person cannot be determined (#959). Without frame anonymization enabled, the values transmitted in these unencrypted fields and elements remain static or predictable until a new association is performed (#66), even when other EDP features are enabled. Examples of unencrypted fields and elements that contain static or predictable values assigned to an 802.11 device include: Address fields, including transmitter address (TA), receiver address (TA), source address (SA) and receiver address (SA); Sequence Number (SN); Packet Number (PN); Timestamp; Association Identifier (AID) and fields and elements derived from the AID. (#1029, #1030) A third party can monitor the values transmitted in these fields and, as long as the values remain static or predictable, the third party can determine that the 802.11 device continues to be present at that location. In some cases, the location could be fixed (relative to earth) while in other cases the location could be a vehicle in motion. FA improves user privacy by restricting the time windows within which unencrypted fields and elements remain static or predictable, thereby increasing the effort required for a third party to determine the long-term presence of the person. (#67, #938, #959)

NOTE 2—When present, SA (or DA respectively) provides the MAC address of the source (or destination respectively) of the frame when the source is distinct from the transmitter (or the destination is distinct from the receiver respectively). These MAC addresses can remain unchanged for a relatively long time; in many cases these MAC addresses never change. If SA and/or DA are not encrypted, then a non-AP MLD in a BSS or ESS might be profiled according to the frequencies of SA and/or DA in frames transmitted or received by those non-AP MLDs. This might be exploited a third party to determine the long-term presence of the person. (#225)

3

* (#336) third parties determining the presence of a person(#959)
* (#336) third parties determining the presence of a person (#959)
* (#1039) third parties determining the presence of a person (#959) across multiple FA epochs via (#938)

(#938)(#66, #938) (#66, #938) (#938).(#938) In each EDP epoch, a new frame anonymization parameter set (FA parameter set) is used. EDP epoch operation is described in 10.71.2 (EDP epoch operation). The establishment of the new FA parameter set is described in 10.71.3 (Establishing frame anonymization parameter sets).(#67)

FA mechanisms are partitioned into Client Privacy Enhancement (CPE) frame anonymization that mitigates detection of a non-AP MLD, and BSS Privacy Enhancement (BPE) frame anonymization that mitigates detection of a BSS (the BPE AP MLD and its associated non-AP MLDs). CPE FA is “baseline” FA; that is, CPE FA mechanisms are enabled whenever FA is enabled. BPE FA is optional for FA; that is, BPE FA can only be enabled when CPE FA is additional enabled.(#223)

The transmitting MLD applies the processing in 10.71.5 (MAC header anonymization and transmitting functions) to the identified MAC header fields.

* The sequence number and packet number (assigned by the transmitting MLD) are transformed into over-the-air(#514) values that can be(#515) transmitted in the clear while maintaining anonymity.
* The Address 1 field of an individually addressed frame(#1030) (on the downlink) or the Address 2 field (on the uplink), then the value is set to a temporary (that is, per EDP-Epoch) random MAC address for the affiliated STA of the non-AP MLD. on the link on which the frame is transmitted.
* If BPE is enabled, then:
* The Address 2 field (on the downlink), or the Address 1 field (on the uplink), is set to the temporary random MAC address of the affiliated AP of the AP MLD. (#224, #1033)
* The value in the Address 1 field of a group addressed frame is transformed into an over-the-air value. (#224, (#1034)
* The Timestamp (assigned by the AP MLD) in the Privacy Beacon is transformed into an over-the-air value that can be transmitted in the clear while maintaining anonymity of the AP MLD. (#224, #1035)

The(#516) receiving MLD applies the processing described in 10.71.6 (MAC header anonymization and receiving functions) to the over-the-air(#514) MAC header field values.

* During address filtering,
* The over-the-air(#514) value in Address 1 of an individually addressed frame (#1036) (on the downlink) or Address 2 (on the uplink) is matched to the temporary random MAC address for the affiliated STA of the non-AP MLD on the link on which the frame is transmitted.
* If BPE is enabled, then:
* The over-the-air value in Address 2 field (on the downlink), or the Address 1 field (on the uplink), is matched to the temporary random MAC address of the affiliated AP of the AP MLD. (#224, #1036)
* The over-the-air value in Address 1 field of a group addressed frame is transformed back to the original group MAC address assigned by the transmitting MLD. (#224, #1037)
* The over-the-air(#514) values for the sequence number and packet number are transformed back to the original sequence number and packet number assigned by the transmitting MLD.
* If BPE is enabled, then:
* The over-the-air Timestamp in the Privacy Beacon is transformed back to the original Timestamp assigned by the AP MLD. (#224, #1038)

The AID of a non-APMLD, and fields and elements derived from the AID, are anonymized using temporary, random AIDs assigned by the AP MLD. (#1032)

FA uses transmission of MSDUs in A-MSDUs to provide confidentiality of SA and DA, noting that A-MSDU can contain a single MSDU – see 10.71.1a (General). (#517)

.

**10.71.1a General**

The FA feature may be enabled if only if MLO is enabled.

The FA feature shall be enabled if and only if dot11EDPGroupEpochActivated is true. #958)

The FA feature may be enabled if and only if dot11DSMACAddressActivated is true. (#156)

 (#TBD)

A CPE STAs should transmit an MSDU in an A-MSDU.(#957)

A BPE STAs shall transmit an MSDU in an A-MSDU.(#957)

 (#517)