IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Comments – LB288-4.5.10 | | | | |
| Date: 2025-04-07 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Carol Ansley | Cox Communications |  |  | carol@ansley.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document covers comments: 11, 104, 297, 303, 304, 382, 383, 384, 385, 387, 388, 389, 390, 771, 787, 788, 789, 880,881, 882, 904, 937, 993

Similarly,

The Measurement ID subelement is optionally included in a Beacon request to request that the responding STA to include a Measurement ID element in the Probe Request frames it transmits.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number(C)** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 297 | Hiroyuki Motozuka | 4 | 24.56 | "may" is used in normative texts and should not be used in Clause 4 | Please replace "may" with "might" or "can", depending on context, at eight occurrences in subclause 4.5.4.10a and 4.10.2. | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #297. |
| 881 | stephane baron | 4.5.10.4.a | 24.61 | text indicate :"An non-AP MLD supporting CPE frame anonymization may change the(#1046) MAC address(es) of its affiliated STAs". But frame anonymization is not limited to the MAC address. | Indicate that frame anonymization also obfuscate other frame fields transmitted in clear OTA | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #881. |
| 882 | stephane baron | 4.5.10.4.a | 25.06 | BPE MAC address change is not clear. Text indicate "A BPE EDP AP MLD and its associated non-AP MLDs may change their OTA MAC addresses". Do you mean " A BPE AP MLD and its affiliated APs may change their OTA MAC addresses"? In addition, you do not mention frame anonymization performed by both AP and non-AP STAs. | Please clearly indicatge that the AP MLD and its affiliated APs may change their MAC address, that is one of the core differences between CPE and BPE. In Addition, mention the frame anonymization as a mechanim used by bot AP MLD and its associated non AP MLDs. | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #882. |
| 11 | Graham Smith | 4.5.4.10 | 24.18 | "If a fixed MAC address identifying the STA is observable in these transactions, then it is trivial to track the STA." I can see that the intention is to refer to the previous sentence and the "transactions" but it reads awkward. | Replace cited text with "If a STA uses a fixed MAC address in these transactions, then it is trivial to track that STA." | Accept. |
| 303 | Antonio DeLaOlivaDelgado | 4.5.4.10 | 24.31 | Description of what EDP does should be better in the paragraph. Right now it looks like a minor thing the writer does not want to talk about. | I think we should have a better description for EDP features, I suggest replacing current "Additional mitigation can be provided by EDP features." with "Additional mechanisms to increase the privacy of associated STAs and MLDs can be provided by EDP features. For MLD, EDP provides frame anonymization mechanisms able to hide identificable information in the header of frames by periodically changing the MAC address, AIDs, and other header parameters for groups of stations." Probably we also need to explain more some other features, this text is just a starting point. | Revised.  Editor, please update section 4.5.4.10 as shown in document 25/626r0 marked with tag #303. |
| 880 | stephane baron | 4.5.4.10 | 24.32 | text indicate "Additional mitigation can be provided by EDP features.(#1202)", but do not clarify that those enhancements are available after association while associated with an AP | give more details on when those enhancements are applicable | Revised.  Editor, please update section 4.5.4.10 as shown in document 25/626r0 marked with tag #880. |
| 993 | Philip Hawkes | 4.5.4.10 | 24.32 | Since EDP features are a subset of enhncements with an overview in a separate section, it would be helpful to have a cross reference to 4.5.4.10a | Add a cross reference to 4.5.4.10a | Revised.  Editor, please update section 4.5.4.10 as shown in document 25/626r0 marked with tag #993. |
| 937 | Srinivas Kandala | 4.5.4.10a | 23.56 | There does not appear to be not much difference between client privacy enancement (CPE)" and and "Enhancemed Data Privacy (EDP). The phrase :"Using EDP client privacy enhancements (CPE)" does not mean much unless each of the terms are clarified | Clarify the differences. If they mean the same thing,consider dropping one of them | Rejected.  Enhanced Data Privacy is the name of the amendment, and client privacy enhancement is the name for a group of features that are part of EDP. The other large grouping of features is BSS privacy enhancement or BPE. |
| 771 | Massinissa Lalam | 4.5.4.10a | 24.53 | This sentence "An non-AP MLD [...] change the MAC address(es) of its affiliated STAs during an association either at its own request or at the direction of the AP MLD with which it is associated" is not clear. The "own request" seems OK, but what does "at the direction of the AP MLD" means? Is this when instructed by the AP (so "under the direction of")? Clarification is needed. | Clarify the sentence, as is it is difficult to get the intent of the end of this sentence | Revised.  Editor, please update section 4.5.4.10 as shown in document 25/626r0 marked with tag #771. |
| 787 | John Wullert | 4.5.4.10a | 24.56 | The word "may" is used in specifications to reflect a permissible action. The usage of the word "may" in this paragraph does not align with that usage. | Revise paragraph to remove the word "may". Suggested revised text "Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can reduce the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a STA or MLD can reduce the content of preassociation and association messages to lower the opportunity to fingerprint the STA or MLD through its messages outside of a secured connection. An non-AP MLD supporting CPE frame anonymization can change the MAC address(es) of its affiliated STAs during an association either at its own request or at the direction of the AP MLD with which it is associated'" | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #787.. |
| 904 | Robert Stacey | 4.5.4.10a | 24.56 | Avoid "may" in this sentence -- it has a special meaning in IEEE standards. "Might" is the appropriate word here. Also, we are ultimately concerned about individual privacy and only proximally concerned with device privacy. | Change to "Third parties might seek to track a person's location and activities by observing wireless communications. It is frequently the case that a specific wireless communications device is used only by a specific person and that by tracking the device a third party can track the individual." | Revised.  Editor, please update section 4.5.4.10a as shown below in document 25/626r0 marked with tag #904.. |
| 382 | Mark RISON | 4.5.4.10a | 24.57 | "a STA or MLD may reduce the amount of information disclosed" is not normative | Change "may" to "might" in the first occurrence in this subclause, and to "can" in all other occurrences in this subclause | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #382. |
| 385 | Mark RISON | 4.5.4.10a | 24.57 | "STA or MLD" should be "STA or non-AP MLD" | Change throughout subclause | Revised.  the first instance of STA or MLD is correct, since an AP MLD or a non-AP MLD can use EDP features. The other instances are changed.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #385. |
| 788 | John Wullert | 4.5.4.10a | 24.57 | The text here says that either a STA or an MLD can use the EDP features. While there are parts of the text that specifically desribe MLO and non-MLO behavior, in other sections the draft only refers to the use of EDP features by MLDs. It may be preferable to do that, rather than having separate MLO/non-MLO descriptions in every instance even when the behavior is the same. However, if that approach is being used the text should state so explicitly. | Add a note to indicate that EDP features are described using MLO terminology and those descriptions apply to non-MLO devices as well. In cases where the behavoir of MLO and non-MLO devices differ, separate descriptions are provided. | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #788. |
| 383 | Mark RISON | 4.5.4.10a | 24.58 | "preassociation" -- is this defined? In any case it's confusing given the "preassociation" security feature | Change to "content of messages sent before and during association" | Accept.  there are several other uses of preassociation in 4.5.4.10 from the baseline. |
| 384 | Mark RISON | 4.5.4.10a | 24.58 | It is not clear what it means to reduce the content of messages | Change "reduce" to "modify" | Accept. |
| 304 | Antonio DeLaOlivaDelgado | 4.5.4.10a | 24.61 | The phrase "An non-AP MLD supporting CPE frame anonymization may change the MAC address(es) of its affiliated STAs during an association either at its own request or at the direction of the AP MLD with which it is associated." indicates the non-AP MLD may request to change the MAC address whenever it wants, this is not correct in current specification | Either remove that part from the phrase or include the funcitonality in the specifciation. | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #304.. |
| 104 | Chaoming Luo | 4.5.4.10a | 25.01 | As dicussed in the requirement, mobile AP MLD may support BPE EDP features, non-mobile AP MLD does not have the stated privacy issue, so BPE EDP features should apply only to mobile MP MLD. Otherwise some of the current design decisions do not make sense, e.g., "A Privacy Beacon frame shall not contain a Multiple BSSID element". | Change to: A mobile 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. A mobile AP MLD that is a BPE AP MLD may protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are preconfigured to recognize the BPE AP MLD. | Rejected.  While a non-mobile AP may not have the exact privacy concerns that a mobile AP has, there is no need to restrict the implementation of BPE features to only mobile APs. An AP may still seek to obfuscate its presence and information about its ESS. |
| 390 | Mark RISON | 4.5.4.10a | 25.01 | "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." -- this is weird, because by definition APs in the same ESS know about each other | Delete "such as the ESS to which it belongs" | Rejected.  While other APs in the same ESS do share that information, third party observers may not be participants in the ESS. The obfuscation of the ESS is a part of the goals of BPE. |
| 789 | John Wullert | 4.5.4.10a | 25.01 | The word "may" is used in specifications to reflect a permissible action. The usage of the word "may" in this paragraph does not align with that usage. Also, order of phrasing in one sentence is confusing. | Revise the paragraph to remove the word "may". Suggested revision: "An AP MLD supporting BPE EDP features can reduce the amount of information about itself, such as the ESS to which it belongs, that is revealed to third party observers. A BPE AP MLD can protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are preconfigured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs can change their OTA MAC addresses together with associated values for both unicast and group transmissions." | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #789. |
| 389 | Mark RISON | 4.5.4.10a | 25.03 | It's not clear what "preconfigured" means | Change to "configured" (also in the para at 95.6) | Revised.  Who has section 10.71.8.2? There is a paragraph that uses “preconfigured” multiple times. I have added it below here as well.  Also, the baseline uses “preconfigured”. Should this be a reject?  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #387. |
| 387 | Mark RISON | 4.5.4.10a | 25.04 | "A BPE EDP AP MLD and its associated non-AP MLDs may change their OTA MAC addresses together with associated values for both unicast and group transmissions. " -- it is not clear whether the "together" pertains to "change" or to "with" | Change to "A BPE EDP AP MLD and its associated non-AP MLDs may change their OTA MAC addresses and associated values for both unicast and group transmissions. " | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #387. |
| 388 | Mark RISON | 4.5.4.10a | 25.06 | It is not clear what "associated values" refers to | Change to "SN and stuff" | Revised.  Editor, please update section 4.5.4.10a as shown in document 25/626r0 marked with tag #388. |

4.5.4.10 MAC privacy enhancements

***Change the first paragraph as follows:***

When a non-AP STA searches for, and connects to, an infrastructure BSS, IBSS, or PBSS or attempts to discover services on a network before association, it selects a MAC address for the particular connection.If a STA uses a fixed MAC address in these transactions, then it is trivial to track that STA.(#11, 383) An MSDU transmitted by a STA is assigned a sequence number that, if never reset, can also be used to track a device irrespective of the MAC address. If OFDM is used, the PHY DATA scrambler used can enable tracking of a device irrespective of the MAC address if it is not reseeded. The dynamic nature of BSS membership combined with this tracking information allows for construction of a network of connections, locations, and behavior. This network can be used to glean private and sensitive information regarding the individual behind the device.

***Change the third paragraph as follows:***

To mitigate traffic analysis and tracking, a non-AP STA or a non-AP MLD can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association Additional mechanisms to increase the privacy of associated STAs and non-AP MLDs can be provided by EDP features. For example, EDP provides MLDs with frame anonymization mechanisms hiding identifiable information in the frame headers by periodically changing the MAC addresses, AIDs, and other header parameters for groups of affiliated STAs while associated.(#303, 880) (see 4.5.4.10a) (#993) A non-AP MLD can also change the MAC addresses of its affiliated STAs prior to an association. Such a non-AP STA or a non-AP MLD using the device ID mechanism, upon reconnecting to a network, can provide either a device ID or a PASN ID previously provided by the network. Such a non-AP STA using the identifiable random MAC address (IRM) mechanism, upon reconnecting to the network can provide the IRM that the STA or the non-AP MLD previously provided to the network. Such a non-AP STA can use both device ID and IRM mechanisms concurrently. Such a STA or the non-AP MLD can also use a measurement ID, previously provided by the network, to assist while performing beacon report measurement procedures. These mechanisms allow the network to recognize the STA or the non-AP MLD while providing protection against third party tracking or traffic analysis. When the network can recognize the STA, it can map already established shared identity state (see 12.2.13 (Identifying a non-AP STA or a non-AP MLD with changing MAC address)) to this STA, which can allow the network to provide network acquisition steering and selection, or allow the network to connect transactional information obtained preassociation or in a prior association to the device that is associating. While discovering networks, a non-AP STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

***Insert the following new subclause after 4.5.4.10 (MAC privacy enhancements):***

**4.5.4.10a Enhanced Data Privacy (EDP) enhancements**

Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can reduce the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the STA or non-AP MLD through its messages outside of a secured connection.(#383, 384) A non-AP MLD supporting CPE frame anonymization can change the MAC address(es) and other fields used in communications of its affiliated STAs during an association.(#881, 304, 771)

An AP MLD supporting BPE EDP features can reduce the amount of information about itself, such as the MAC addresses of its affiliated APs and the ESS to which it belongs, that is revealed to third party observers.(#789, 882) A BPE AP MLD can protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are configured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs can change their OTA MAC addresses and other trackable fields for both unicast and group transmissions.(#11, 382, 385, 387, 388, 389, 787, 789, 904)

NOTE – EDP features might be generally described with MLO terminology, but separate descriptions are provided for individual features to explain when the behaviour of MLO and non-MLO devices will differ.(#788)

10.71.8.2 BPE AP MLD beaconing

***Modify fourth paragraph as shown:***

A BPE non-AP MLD shall use the Equation (28) to determine whether it is configured with the transmitter of the received Privacy Beacon frame. A BPE AP MLD is discovered if the Identity Hash field of the Privacy Beacon frame matches with a secure hash calculated with the Address 2 of the Privacy Beacon frame and a previously shared Identity Key. (#389)