IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Comments – LB290-Misc. | | | | |
| Date: 2025-10-15 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Carol Ansley | Cox Communications |  |  | carol@ansley.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document covers comments: 2005, 2011, 2012, 2013, 2015, 2046, 2051, 2106, 2107, 2108, 2289, 2466.

R0 – initial draft

R1 – with changes from discussion 10/14/2025

R2 – small cleanup 10/15/2025

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Page | Comment | Proposed Change | Resolution |
| 2005 | 1.35 | The amendment title reads "Enhanced Service with Privacy Protection", but the project title of the amendment in the PAR reads "Enhanced Service with Data Privacy Protection". The amendment in D2.0 should be the same title as in the PAR. | Please change the amendment title to the amendment title given in the PAR "Enhanced Service with Data Privacy Protection". | Rejected. The PAR title is in the process of being changed to the title shown on the face of the Draft. |
| 2011 | 29.29 | "...used by a third-party observer to determine the long-term presence of a person at a location, even if the identity of the person cannot be determined." It is only a privacy concern IF the device can be attributed to a person. As written it makes no sense. | ...used by a third-party observer to determine the long-term presence of a non-AP STA or non-AP MLD at a location, in the case that the user can be determined." | Revised.  Agree in principle with the comment.  Editor to make the changes associated with tag #2011 in this document. |
| 2012 | 29.38 | "...the third-party observer can determine that the corresponding 802.11 device continues to be present at that location. In some cases, the location could be fixed (relative to the ground) while in other cases the location could be in motion, e.g. the device is moving, or the AP is installed in a vehicle and both the AP and the device are moving". in motion, e.g., the device is moving?? Really, good job that was explained. In a vehicle, but somehow the observer is running along side, or following in another vehicle. In either case, why bother with the device, not many people in a vehicle. This does not make much sense. Get rid of it. | delete "at that location. In some cases, the location could be fixed (relative to the ground) while in other cases the location could be in motion, e.g. the device is moving, or the AP is installed in a vehicle and both the AP and the device are moving" | Revised.  Agreed in principle.  The group agreed to remove the text because of a lack of clarity in the text. The group disagrees that the potential use case is invalid. For example, the vehicle may be a bus or train with many riders. |
| 2013 | 29.45 | "Frame anonymization, available when MLO is enabled, improves user privacy by restricting the periods 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. The periods, called EPP epochs, can be relatively short in duration when compared to the typical lifetime of an association." In fact, assuming a user has been identified with a device, it only needs one change of parameters to hide it. There is no need to make short epochs. Also, what is a typical lifetime of an association? I know this is clause 4 but this text seems to be trying to justify why to use FA with debatable facts. | Replace cited text as follows:."Frame anonymization, available when MLO is enabled, restricts the periods within which unencrypted fields and elements remain static or predictable. These periods are called EPP epochs. | Revised.  Agree in principle with some of the suggested text changes for simplification.  Editor to make the changes associated with tag #2013 in this document. |
| 2015 | 30.14 | "FA transmits MSDUs in A-MSDUs (which encrypt SA and DA) to mitigate such profiling." No it doesn't, this should be for a device following EPP . This should be a general EPP statement.nothing to do with FA. | Replace cited text with "An AP MLD or non-AP MLD implementing EPP features transmits MSDUs in A-MSDUs (which encrypt SA and DA) to mitigate such profiling." | Revised.  Editor to make the changes associated with tag #2015 in this document. |
| 2046 | 25.36 | With regarding to CID 148, the given resolution is not accurate, as the project name was not EDP. However, moving on; what is an "EPP feature"? It doesn't appear to be defined anywhere. | Add a new definition in clause 3.2: "enhanced privacy protection: [EPP] enhancements for the protection of privacy". Easy; that's all you need. | Rejected.  An acronym for EPP has been added to Clause 3.4 in lieu of a definition. This is in line with other amendments in the baseline.  Subclause 4.5.4.10a has a more complete description of EPP. |
| 2051 | 29.64 | "An AP MLD or non-AP MLD implementing EPP features can support CPE features, BPE features or both." But 3.2 says that BFE includes CPE features. | remove "or both" | Revised.  Agree in principle with the comment.  Editor to make the changes associated with tag #2051 in this document. |
| 2106 | 29.26 | Reword sentence for clarity | Change "When values are (a) assigned to an 802.11 device, (b) static or predictable and (c) transmitted in unencrypted fields and elements" to "When an 802.11 device transmits static or predictable values associated or assigned to that device in unencrypted fields or elements," | Revised.  Agree in principle with the comment.  Editor to make the changes associated with tag #2106 in this document. |
| 2107 | 29.30 | Sentence is duplicative of previous sentence: "Without appropriate mitigations, the values transmitted in these unencrypted fields and elements remain static or predictable until a new association is performed, even when other EPP features are enabled." | Delete sentence. | Accepted. |
| 2108 | 29.29 | Use FA acronym consistently. | Add acronym: "Frame anonymization (FA), available when MLO is enabled,...". Also change line 51: "The CPE FA mechanisms..." and line 55" The BPE FA mechanisms...". | Accepted. |
| 2289 | 30.01 | Not sure what does the text mean exactly. May an AP MLD or non-AP MLD operating solely with BPE support CPE ? Does "without multi-group management" mean "with single group management" ? | Make it clearer | Revised.  Agree in principle with the comment.  Editor to make the changes associated with tag #2289 in this document. |
| 2466 | 29.08 | What does it mean by "network acquisition steering and selection" here? This description is too generic. Please clarify which functions are being referred here (e.g. AP discovery, STA steering etc.). | As in comment | Reject.  The text the comment refers to is from the baseline. This comment should be brought to REVmf. |

4.5.4.10a Enhanced Privacy Protection (EPP) enhancements

Third parties observing the wireless medium might seek to track device locations and device activity. Using EPP features, a STA or MLD can modify the amount of information disclosed in several ways. Using EPP client privacy enhancements (CPE), a non-AP STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the non-AP STA or non-AP MLD through its messages outside of a secured connection.

Additional threats exist while a secured connection is established. When ~~values are (a) assigned to~~ an 802.11 device~~, (b)~~ transmits static or predictable values associated with or assigned to that device ~~and (c) transmitted~~ in unencrypted fields and elements, ~~then~~ those values can be used by a third-party observer to determine the long-term presence of that ~~a person~~ non-AP STA or non-AP MLD at a location, even if the identity of the person related to that device cannot be determined[#2011,#2106]. ~~Without appropriate mitigations, the values transmitted in these unencrypted fields and elements remain static or predictable until a new association is performed, even when other EPP features are enabled.~~ [#2107]

Examples of unencrypted fields and elements that contain static or predictable values assigned to the transmitter or receiver include: transmitter address (TA), receiver address (RA); sequence number (SN); packet number (PN); timestamp; association identifier (AID) and fields and elements derived from the AID. A third-party observer can monitor these values and, as long as the values remain static or predictable, the third-party observer can determine that the corresponding 802.11 device continues to be present ~~at that location. In some cases, the location could be fixed (relative to the ground) while in other cases the location could be in motion, e.g. the device is moving, or the AP is installed in a vehicle and both the AP and the device are moving~~. [#2012]

Frame anonymization (FA), available when MLO is enabled, restricts the periods within which unencrypted fields and elements remain static or predictable ~~improves user privacy by restricting the periods 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~~. [#2013, #2108] The periods, called EPP epochs, can be relatively short in duration when compared to the typical lifetime of an association.

The CPE FA ~~frame anonymization~~ mechanisms anonymize fields that identify a non-AP MLD (such as the MAC address(es) of its affiliated STAs) during an association.[#2108]

The BPE FA ~~frame anonymization~~ mechanisms anonymize fields that identify an AP MLD and its set of associated non-AP MLDs (such as the MAC address(es) of its affiliated APs, the ESS to which it belongs, and its group addresses). [#2108] 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 AP MLD and its associated non-AP MLDs can change their OTA MAC addresses and other trackable fields for both individually addressed and group addressed transmissions.

An AP MLD or non-AP MLD implementing EPP features can support CPE FA mechanisms ~~features,~~ or ~~both CPE and~~ BPE FA mechanisms ~~features~~ ~~or both~~.[#2051, #2289] While a CPE AP MLD implements one or more EPP groups, a BPE AP MLD implements a single EPP group. As such, an AP MLD or non-AP MLD implementing ~~operating solely with~~ BPE FA mechanisms implements CPE FA mechanisms ~~features~~ within a single EPP group~~, but~~ without multi-group management.[#2289]

A third party can also determine the long-term presence of an MLD by exploiting other unencrypted fields and elements that contain static or predictable values that are not assigned to the transmitter or receiver. For example, the SA (or DA respectively), when present, provides the MAC address of the source (or destination respectively) of the frame. These MAC addresses can remain unchanged for a relatively long time or might never change. If SA and/or DA are not encrypted, these values might be used to profile the transmitter and/or receiver. ~~FA~~ An AP MLD or non-AP MLD implementing FA features can transmit~~s~~ MSDUs in A-MSDUs (which encrypt SA and DA) to mitigate such profiling. [#2015]