IEEE P802.11
Wireless LANs

|  |
| --- |
| CIDs 1046, 1187, 1188, 1190 and 1191 |
| Date: 2024-10-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |

Abstract

Abstract

This submission addresses CIDs 1046, 1187, 1188, 1190, 1191 against 3.2 (Definitions).

We propose draft specification text for TGbi draft D0.7.

Revisions:

* Rev 0: Initial version of the document.

| **CID** | **Commenter** | **Clause**  | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| 1046 | Antonio DeLaOlivaDelgado | 3.2 | 19.62 | We have over the air sequence number and over the air packet number, should not we have an over the air MAC address definition? | Add a definition of over-the-air MAC address | **Revised**The term “over-the-air MAC address” is not clear, and not used very often. Suggest using the term “used to MAC addresses used to identify the [client] as the transmitter or receiver of a frame”. Updates to 4.5.4.10 (MAC privacy enhancements), 12.14.5.1 (Non-MLO), 12.14.5.2 (MLO)Document 1xxxr0 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1046 |
| 1187 | Mark RISON | 3.2 | 19.35 | If "frame anonymization" can only be used with MLO, then it should be called "MLO frame anonymization". Similarly "group enhanced data privacy (EDP) epoch" and "individual enhanced data privacy (EDP) epoch" and "presence monitoring" | As it says in the comment | **Rejected**There is no need to prefix terms to clarify their scope. The existing terms are sufficient.  |
| 1188 | Mark RISON | 3.2 | 19.39 | "in frame anonymization mechanisms" should be just "in frame anonymization" (see previous definition) | As it says in the comment | **Accepted**Document 1xxxr0 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1188 |
| 1190 | Mark RISON | 3.2 | 19.52 | "Counter Mode (CTR) with cipher-block chaining message authentication code (CBC-MAC)" -- capitalisation inconsistent | As it says in the comment | **Revised**Propose replacing with the text for the expansion of CCMP acronym “CTR with CBC-MAC protocol”.Document 1xxxr0 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1190 |
| 1191 | Mark RISON | 3.2 | 19.63 | Definitions start with an uppercase | Change ": determining" to ": Determining" | **Accepted**Document 1xxxr0 accounts for resolution of this CID. Instruction to the editor: apply changes referenced with tag: #1191 |

**Proposed spec text:**

***TGbi editor: Add or update the following definitions in 3.2 (Definitions). The baseline for this text is Draft P802.11bi\_D0.6.***

**client privacy enhancements**: A set of enhanced data privacy (EDP) features whose primary purpose is improving the privacy of a single non-AP STA or non-AP MLD.

**BSS privacy enhancements**: A set of enhanced data privacy (EDP) features whose primary purpose is improving the privacy of all 802.11 devices in a BSS, including the AP or AP MLD.

**over-the-air packet number**: [OPN] The value transmitted in an individually addressed CTR with CBC-MAC (#1190) protocol (CCMP) header or Galois/Counter Mode (GCM) protocol (GCMP) header in the place of the packet number as part of frame anonymization.

**over-the-air sequence number**: [OSN] The value transmitted in an individually addressed medium access control (MAC) protocol data unit (MPDU) header in the place of the sequence number as part of multi-link operation (#1187)frame anonymization.

**presence monitoring**: D(#1191)etermining the ongoing presence of non-access point (non-AP) multi-link devices (MLDs) associated to an AP MLD.

***TGbi editor: Apply the following changes to 4.5.4.10 (MAC privacy enhancements. The baseline for this text is Draft P802.11bi\_D0.5.***

When a non-AP STA searches for, and connects to, an infrastructure BSS, IBSS, or PBSS or attempts to discover services on a network preassociation, it defines the addressing of its MAC layer for the particular connection. If a fixed MAC address is used to identify a STA as the transmitter or receiver of a frame, then(#1046) it is trivial to track the STA. 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.

***TGbi editor: Apply the following changes to 12.14.5.1 (Non-MLO). The baseline for this text is Draft P802.11bi\_D0.6.***

During(#1046) BSS transition, if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element, then an EDP non-AP STA shall randomize the MAC address used to identify the EDP non-AP STA as the transmitter or receiver of a frame(#1046).

***TGbi editor: Apply the following changes to 12.14.5.2 (MLO). The baseline for this text is Draft P802.11bi\_D0.6.***

During(#1046) BSS transition, if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element, then an EDP non-AP MLD shall randomize the MAC addresses used to identify the EDP non-AP MLD as the transmitter or receiver of a frame (including STA MAC address(es) and MLD MAC address) (#1046).