IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MPDU Anonymization / De-anonymization for 11bi | | | | |
| Date: 2023-09-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Jouni Malinen |  |  |  |
| Duncan Ho |  |  |  |
| George Cherian |  |  |  |

Abstract

We propose the draft specification for the following requirements in contribution “11-23-0892-03-00bi-requirements-and-issues-tracking” for TGbi draft D0.1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Requirement** | **Issue** | **Status** | **Information** |
| 7 | 11bi shall define a mechanism for a CPE Client to initiate changing its own OTA MAC Address used with a CPE AP in Associate STA State 4 without any loss of connection. | MAC address change while associated | Discussions underway |  |
| 9 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted SN and the scrambler seed on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway |  |
| 10 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted PN on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway |  |

Revisions:

* Rev 0: Initial version of the document.

**High level summary of the changes:**

Includes MPDU Anonymization / De-anonymization in figures and text of clause 5.1.5.1 (General) introducing the MAC data-plane architecture.

**Proposed spec text:**

The baseline for this text is 802.11be D4.0.

***TGbi editor: Apply the following changes in clause 5.1.5.1 (General):***

***TGbi editor: CHANGE 1. Replace Fig 5-2a (MAC data plane architecture (MLO) for unicast data frames) as with the following (new blocks have orange fill):***



***TGbi editor: CHANGE 2. Replace Fig 5-2b (MAC data plane architecture for AP MLD and affiliated APs) as with the following (new blocks have orange fill):***



***TGbi editor: CHANGE 3 Apply the following change:***

The MLD upper MAC sublayer functions include:

* Authentication, association, and reassociation (between an AP MLD and a non-AP MLD)
* Security association (e.g., PMKSA, PTKSA) and distribution of GTK/IGTK/BIGTK
* MPDU Anonymization / De-anonymization parameter establishment (between an AP MLD and a non-AP MLD)
* SN/PN assignment for frames to be encrypted by PTK for unicast frames

***TGbi editor: CHANGE4 Apply the following change:***

The MLD lower MAC sublayer functions include:

* MPDU Anonymization / De-anonymization of MPDU header fields
* Link specific control information exchange/indication (e.g., RTS/CTS, acknowledgements, NDP, etc.)

***TGbi editor: CHANGE 5 Insert the following after NOTE 4 and before text on the “Block Ack Scoreboarding” block:***

When MLO is being used, the “MPDU Anonymization / De-anonymization” block are applied to the Affiliated STA MAC address, SN and PN to maintain anonymity of the non-AP MLD. The “Anonymization / De-anonymization” block transforms between “internal” values (which remain secret to maintain anonymity) and “over-the-air” values (which can be safely transmitted in the clear while maintaining anonymity, and then transformed back to the “internal” values by the intended receiver).