IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D0.4 CR for CID 1146 | | | | |
| Date: 2024-10-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions for the following CIDs:

1146

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.6 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.6 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1146 | Po-Kai Huang | 12.2.10 | 0.00 | Several statements in 12.2.10 needs to be tweaked to allow MAC address change during reassociation. Suggested change as proposed in 11-23-1664r1 | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1727r0 under all headings that include CID 1146 |

**Discussion:**

None

**Proposal: (#1146)**

**TGbi Editor: *Instruction: Modify 12.2.11 as shown below***

* + 1. **Requirements for support of MAC privacy enhancements**

MAC privacy enhancements are enabled on a non-AP STA when dot11MACPrivacyActivated is(M118) true. The STA shall periodically change its MAC address to a random value while not associated to a BSS. The STA shall construct the randomized MAC address from the locally administered address space as defined in IEEE Std 802-2014 and IEEE Std 802c™-2017. However, the non-AP STA shall not change its MAC address during a transactional exchange, for example, transmitting Public Action frames for preassociation discovery, or during the creation of state on an AP using preassociation capabilities, for example, RSN preauthentication or FT over-the-DS. The smaller the period of MAC address change, down to a single transmitted frame per MAC address, the greater the privacy these enhancements afford. The actual period used when changing a MAC address is implementation dependent and outside the scope of this standard.

If such a non-AP STA starts any transaction that establishes state bound to a MAC address and might elect to establish an association or establish transaction state with a discovered BSS, it shall check the value of dot11LocallyAdministeredMACConfig and shall configure its MAC address according to the rules of the local address space prior to the start of the transaction. State created with an AP using a prior MAC address, for instance, RSN preauthentication state or FT state established over-the-DS, is bound to the MAC address used when that state was created. Prior to establishing an association to the AP, the non-AP STA shall change its MAC address to the MAC address used when the state was created unless client privacy enhancement is used (see 12.14.5 ((Re)Association Request/Response Frame Encryption)).

The SME of the non-AP STA may change the MAC address by generating an MLME-UPDATEMACADDRESS.request primitive containing the new MAC address. On receipt of an MLME‑UPDATEMACADDRESS.request primitive, the MLME shall attempt to update the MAC address that is to be used by the MAC entity and shall generate an MLME-UPDATEMACADDRESS.confirm primitive to notify the SME whether the MAC address has been changed to the new value.

Every time a MAC address is changed to a new random value, counters in (#270)all sequence number spaces used to identify each MSDU, A-MSDU or MMPDU shall be reset (see 10.3.2.14.2 (Transmitter requirements)) and the STA shall set the TXVECTOR parameter SCRAMBLER\_RESET to RESET\_SCRAMBLER on the next transmitted PPDU.

The non-AP STA connecting to an infrastructure BSS shall retain a single MAC address for the duration of its connection across an ESS unless client privacy enhancement is used (see 12.14.5 ((Re)Association Request/Response Frame Encryption)). A PMKSA created as part of an RSNA contains the MAC address used to create the PMKSA. The non-AP STA that supports PMKSA caching shall, if necessary, change its MAC address back to that value when attempting a subsequent association to the ESS using PMKSA caching unless client privacy enhancement is used (see 12.14.5 ((Re)Association Request/Response Frame Encryption) and 12.14.6 (PMKSA caching privacy)).

To construct a random MAC address, the STA shall select a randomized MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017.

To avoid leakage of possibly sensitive network identifying information, STAs should refrain from transmitting Probe Request frames containing preferred SSID values and, instead, use passive scanning or transmit Probe Request frames containing the wildcard SSID.

When dot11MACAddressPolicyActiviated is true, an AP shall set the MAC Address Policy field in the Extended Capabilities field to 1, indicating the existence of a MAC address policy. When dot11MACAddressPolicyActivated is false, an AP STA shall set the MAC Address Policy field in the Extended Capabilities field to 0, indicating that local MAC addresses are not restricted.

A non-AP STA that receives from an AP an Extended Capabilities field with the Local MAC Address Policy subfield set to 1 should, unless it has previously stored the MAC address policy for the ESS, discover that policy, using the MAC Address Policy ANQP-element, before sending any Association Request frame to that AP using a local MAC address as the TA.

MAC privacy enhancements are enabled on a non-AP MLD when dot11MACPrivacyActivated is set to true. When enabled, the non-AP MLD shall adhere to the above requirements for a non-AP STA (that is not affiliated with an AP MLD) in selecting a MLD MAC address, including sequence number space and scrambler requirements. The above requirements defined for a non-AP STA in managing its MAC address during association or establishing transaction state with an AP shall apply to the non-AP MLD in managing its MLD MAC address during association or establishing transaction state with an AP MLD.

When a non-AP MLD with MAC privacy enhancements enabled becomes a non-AP STA for the purpose of BSS transition to an AP, the non-AP STA shall adhere to the requirements above and 35.3.1 (General) for managing and selecting the MLD MAC address. Similarly, when a non-AP STA becomes a non-AP MLD for the purpose of BSS transition to an AP MLD, the non-AP MLD shall adhere to the requirements above and 35.3.1 (General) for managing the MLD MAC address.

NOTE—The non-AP STA MAC address is the MLD MAC address when a non-AP MLD transitions to an AP. See

35.3.1 (General).

When MAC privacy enhancements are enabled on a non-AP MLD, the SME of the non-AP MLD manages the MAC addresses for each of the affiliated non-AP STAs. The randomized MAC address for an affiliated non-AP STA shall be selected according to IEEE Std 802-2014 and IEEE Std 802c-2017. Every time an affiliated STA MAC address is changed to a new random value, counters in all sequence number spaces used to identify each MMPDU shall be reset (see 10.3.2.14.2 (Transmitter requirements)) and the STA shall set