IEEE P802.11
Wireless LANs

|  |
| --- |
| 11be D2.0 CR for Beacon Protection |
| Date: 2022-09-02 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

11039, 13533, 11038, 11055

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the offline discussion with Thomas and Gabor.
* Rev 2: Add CID number in abstract
* Rev 3: Update title document number and revision at the top of word 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 TGbe D2.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D2.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 11039 | Po-Kai Huang | 35.16.1 | 531.06 | It is arguable whether the following sentence located in 35.16.1 is the best location in the specificatioin. "An EHT AP shall have dot11BeaconProtectionEnabled set to 1." A better position will be 11.52 Beacon frame protection procedures. | Consider moving the sentence "An EHT AP shall have dot11BeaconProtectionEnabled set to 1." to 11.52 Beacon frame protection procedures. | Revised – We move the corresponding description to a new clause in clause 12 similar to what has been done in 11ax.TGbe editor to make the changes shown in 11-22/1460r3 under all headings that include CID 11039 |
| 13533 | Mark Hamilton | 35.16.1 | 531.06 | "An EHT AP shall have dot11BeaconProtectionEnabled set to 1."  What if the AP is configured so that it does not do a key handshake (Open, etc.)? | Qualify this statement that other underlying security methods have to be enabled, also. | Revised – We move the corresponding description to a new clause in clause 12 and add “when using RSN” to mimic the following existing sentence in baseline.*The STA shall use management frame protection (MFPR=1) when using RSN.*TGbe editor to make the changes shown in 11-22/1460r3 under all headings that include CID 13533 |
| 11038 | Po-Kai Huang | 35.16.1 | 531.06 | Beacon protection is mandated by 11be for EHT AP as shown below. "An EHT AP shall have dot11BeaconProtectionEnabled set to 1." This implies that dot11RSNAProtectedManagementFramesActivated is true due to the following sentence. "If dot11RSNAProtectedManagementFramesActivated is false, dot11BeaconProtectionEnabled shall be set to false." Suggest to specifically add that "An EHT AP shall have dot11RSNAProtectedManagementFramesActivated set to 1." | Add "An EHT AP shall have dot11RSNAProtectedManagementFramesActivated set to 1." An alternative location for this sentence is 12.6.19 Protection of robust Management frames. | Revised – We move the corresponding description to a new clause in clause 12.TGbe editor to make the changes shown in 11-22/1460r3 under all headings that include CID 11038 |
| 11055 | Po-Kai Huang | 35.16.1 | 531.06 | Beacon protection is mandated by 11be for EHT AP as shown below. "An EHT AP shall have dot11BeaconProtectionEnabled set to 1." Clarify the operation of MLD in 11.52. | Add the following in 11.52. "For MLO, if OCVC capability is not present in a non-AP MLD or if the current AP MLD does not advertise OCVC capability, i.e., all affiliated APs does not advertise OCVC capability, but beacon protection is enabled, the non-AP MLD shall verify that the operating channel information for each setup link in the first received Beacon frame that has been validated using BIP matches the current operating channel parameters of each setup link. If there is a mismatch, the non-AP MLD shall disassociate from the AP MLD. NOTE - All AP MLD advertise the same RSNE and RSNXE if included with the exception of the AKM Suite List field and the MFPR subfield of the RSN Capabilities field see (12.6.2 (RSNA selection)).NOTE - For non-AP MLD, there is only one RSNE and RSNXE inserted into the (Re)Association Request frame initiated by the non-AP MLD (see 12.6.3 (RSNA policy selection in an infrastructure BSS))." | Revised – We add the texts to 11.52. We also clarify how to enable beacon protection for non-AP STA based on the description in dot11BeaconProtectionEnabled.*dot11BeaconProtectionEnabled OBJECT-TYPESYNTAX TruthValueMAX-ACCESS read-writeSTATUS currentDESCRIPTION"This is a control variable.It is written by an external management entity.Changes take effect as soon as practical in the implementation.This variable indicates whether beacon protection is enabled. If dot11BeaconProtectionEnabled is true for an AP, beacon protection is enabled ontransmission. If dot11BeaconProtectionEnabled is true for a non-AP STA andthe STA receives a BIGTK from the AP with which it is associated, beaconprotection is enabled on reception. Otherwise, beacon protection is disabled."DEFVAL {false}::= { dot11StationConfigEntry 195 }*TGbe editor to make the changes shown in 11-22/1460r3 under all headings that include CID 11055 |

**Discussion: None**

***TGbe editor: Add new subclause 12.12.3 Security constraints for EHT as follows (track change on):***

**12.12 Constraints on allowed security parameters**

**12.12.3 Security constraints for EHT(#11039)**

An EHT AP shall have dot11BeaconProtectionEnabled set to 1 when using RSN. (#13533, #11039)

NOTE - An EHT AP has dot11RSNAProtectedManagementFramesActivated set to 1 when using RSN due to the requirement that if dot11RSNAProtectedManagementFramesActivated is false, dot11BeaconProtectionEnabled needs to be set to false (see 11.52 Beacon frame protection procedures).(#11038)

***TGbe editor: Modify 11be spec as follows***

**35.16 EHT BSS operation
35.16.1 Basic EHT BSS operation**

(…existing texts…)

(#11039)

(…existing texts…)

* **Beacon frame protection procedures**

In an infrastructure BSS, when beacon protection is enabled, the MLME shall provide an encapsulation service for Beacon frames. All Beacon frames shall be submitted to this service for protection processing.

If dot11BeaconProtectionEnabled is true, the AP shall enable beacon protection and set the Beacon Protection Enabled field of the Extended Capabilities element to 1 to indicate that beacon protection is enabled on the transmission of Beacon frames. Otherwise, the field shall be set to 0.

If dot11BeaconProtectionEnabled for a non-AP STA is true and the non-AP STA receives a BIGTK from the AP with which it is associated, the non-AP STA shall enable beacon protection. (#11055)

NOTE—In a multiple BSSID set, a non-AP STA receives BIGTK from its associated AP (which can correspond to either the transmitted BSSID or nontransmitted BSSID) and uses it for validating the contents of the Beacon frame transmitted by the AP corresponding to the transmitted BSSID.(#10)

The beacon protection service shall take the following actions:

* Beacon frame protection shall be set using the MLME-SETPROTECTION.request primitive with the Protectlist including a Key Type value of BIGTK. A non-AP STA shall also set the Protect Type value to Rx. An AP shall set the Protect Type value to Tx.
* The BIGTK shall be installed using the MLME-SETKEYS.request primitive with the value BIGTK for the Key Type parameter.
* The Beacon frames shall be encapsulated and protected using BIP (see 12.5.4 (Broadcast/multicast integrity protocol (BIP))).
* The protected Beacon frames shall be decapsulated and validated using BIP (see 12.5.4 (Broadcast/multicast integrity protocol (BIP))).

If dot11RSNAProtectedManagementFramesActivated is false, dot11BeaconProtectionEnabled shall be set to false.

For non-MLO, if OCVC capability is not present in a non-AP STA or if the current AP does not advertise OCVC capability, but beacon protection is enabled, the non-AP STA shall verify that the operating channel information in the first received Beacon frame that has been validated using BIP matches the current operating channel parameters. If there is a mismatch, the non-AP STA shall disassociate from the AP.(#11055)

For MLO, if OCVC capability is not present in a non-AP MLD or if all AP(s) affiliated with the current AP MLD do not advertise OCVC capability, but beacon protection is enabled, the non-AP MLD shall verify that the operating channel information for each setup link in the first received Beacon frame that has been validated using BIP matches the current operating channel parameters of each setup link. If there is a mismatch, the non-AP MLD shall disassociate from the AP MLD. (#11055)

NOTE – All APs affiliated with an AP MLD advertise the same RSNE and RSNXE if included with the exception of the AKM Suite List field and the MFPR subfield of the RSN Capabilities field (see 12.6.2 (RSNA selection)). (#11055)

NOTE – For non-AP MLD, there is only one RSNE and RSNXE inserted into the (Re)Association Request frame initiated by the non-AP MLD (see 12.6.3 (RSNA policy selection in an infrastructure BSS)). (#11055)