IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bf D5.0 CR for Replay Counter CIDs |
| Date: 2024-10-25 |
| 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:

13, 14, 16, 17, 18

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on feedback from Henry.

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 TGbf D5.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbf D5.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbf Editor: Editing instructions preceded by “TGbf Editor” are instructions to the TGbf editor to modify existing material in the TGbf draft. As a result of adopting the changes, the TGbf editor will execute the instructions rather than copy them to the TGbf Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| R1-13 | Henry Ptasinski | 12.5.4.4.4 | 206.10 | Normative requirements should not be in parenthesis (and in addition, a closing parenthesis is missing). Text is inconsistent with 12.5.2.4.4. ToDS subfield value applies to all individually addressed robust Management frames in this paragraph but that requirement is not clear from the sentence construction. PV1 frames are not supported with GCMP. | Change to: If management frame protection is negotiated, the receiver shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 0, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)). | Revised – Agree in principle with the commenter. Follow the suggested change to adjust the location of the except. Also, agree on the comments of GCMP due to the following baseline spec texts.*An S1G STA shall not use PV1 frames when using GCMP encapsulation.*Texts of note are revised correspondingly. TGbf editor to make the changes shown in 11-24/1716r1 under all headings that include CID 13 |
| R1-14 | Henry Ptasinski | 12.5.2.4.4 | 204.14 | The condition on To DS subfield applies to all PV0 frames in this paragraph, not just Protected Sensing frames. Text is inconsistent with item d below. | Change to: If management frame protection is negotiated, the receiver shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 0, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)), and (S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames. | Revised – Agree in principle with the commenter. Follow the suggested change to adjust the location of the except. Texts of note are revised to better clarify. TGbf editor to make the changes shown in 11-24/1716r1 under all headings that include CID 14 |
| R1-16 | Henry Ptasinski | 12.5.4.4.4 | 206.22 | Exception for Protected FTM frames is included twice. | Change to: If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the receiver shall maintain an additional replay counter for each ACI for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)). | Accepted -  |
| R1-17 | Henry Ptasinski | 12.5.2.2 | 203.35 | Replay counter index bits should be protected by the AAD. | Add protection for replay counter bits. | Rejected – The solution follows principle of 11az, which does not include replay counter indication in AAD and just does post decryption validation.  |
| R1-18 | Henry Ptasinski | 12.5.4.2 | 205.29 | Replay counter index bits should be protected by the AAD. | Add protection for the replay counter index bits. | Rejected – The solution follows principle of 11az, which does not include replay counter indication in AAD and just does post decryption validation.  |

**Discussion:**

None

**Proposal:**

**12.5.2.4 CCMP decapsulation**

**12.5.2.4.4 PN and replay detection**

***Change items c) and d) as follows:***

c) If management frame protection is negotiated, the receiver shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to

0, , and (S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames ~~except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details)).~~(#14)

NOTE 4—For Protected Fine Timing frames and Protected Sensing frames, PV1 Management frames are not applicable.(#14)

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the

receiver shall maintain an additional replay counter for each ACI for received individually addressed robust

PV0 Management frames ~~except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame~~

~~details))~~ that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (see

9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing

frame details)).

**12.5.4.4 GCMP decapsulation**

**12.5.4.4.4 PN and replay detection**

***Change items c) and d) as follows:***

c) If management frame protection is negotiated, the receiver shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 0, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing frame details))~~PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details))~~.(#13)

 (#13)

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the receiver shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames ~~and robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details))~~ that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)).(#16)

NOTE ~~3~~3—PV1 frames are not supported with GCMP (see 12.5.4.1 (GCMP overview)).(#13)