IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment resolution for Misc security comments | | | | |
| Date: 2023-03-23 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Chaoming Luo | OPPO |  |  | luochaoming@oppo.com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission resolves security related comments under ‘Misc’ topic. The following 4 CIDs are resolved: 1478, 1479, 2263, 2265.

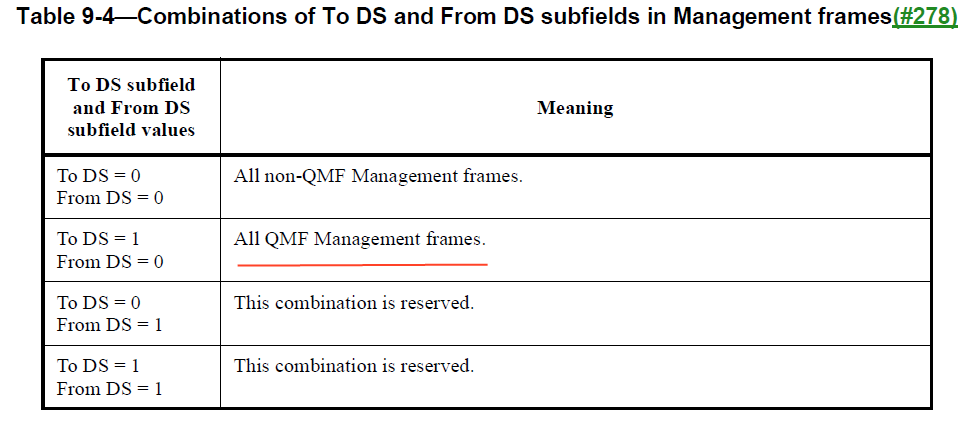
Revisions:

* Rev 0: Initial version of the document.
* Rev 1:
* Reassign 2262 and 2264 to Claudio.
* Remove the incorrect text since we do not have PV1 sensing frames (11bf PAR does not cover S1G).
* Refine the restructured text to make sure the ‘legacy’ behaviour is maintianed.
* Adding back the missing text of ‘The QMF receiver shall…’ to item d) of 12.5.3.4.4 (PN and replay detection).

# PN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1478 | Henry Ptasinski | 221.18 | Protected sensing frames do not need a separate PN space. The timing and usage of these frames is comparable to other protected management frames, and replay detection can operate the same way. Using a separate PN for replay detection, without changes on the transmitter side, undermines replay detection for ALL protected management frames. | Use the same PN as other protected management frames. If a separate PN space were actually needed (which doesn't appear to be the case), then a new key would have to be defined for these frames. | ***Rejected***    *The group has discussed why a separate PN space is needed in* [*https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx*](https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx) *and has additional discussion in* [*https://mentor.ieee.org/802.11/dcn/22/11-22-0891-03-00bf-cc40-cr-for-pn-sn-and-ac.docx*](https://mentor.ieee.org/802.11/dcn/22/11-22-0891-03-00bf-cc40-cr-for-pn-sn-and-ac.docx) *.* |
| 1479 | Henry Ptasinski | 221.60 | Protected sensing frames do not need a separate PN space. The timing and usage of these frames is comparable to other protected management frames, and replay detection can operate the same way. Using a separate PN for replay detection, without changes on the transmitter side, undermines replay detection for ALL protected management frames. | Use the same PN as other protected management frames. If a separate PN space were actually needed (which doesn't appear to be the case), then a new key would have to be defined for these frames. | ***Rejected***    *The group has discussed why a separate PN space is needed in* [*https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx*](https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx) *and has additional discussion in* [*https://mentor.ieee.org/802.11/dcn/22/11-22-0891-03-00bf-cc40-cr-for-pn-sn-and-ac.docx*](https://mentor.ieee.org/802.11/dcn/22/11-22-0891-03-00bf-cc40-cr-for-pn-sn-and-ac.docx) *.* |
| 2263 | Joseph Levy | 221.30 | The change made in has changed the legacy behavior. It is now requiring replay counters for PV1 protected Fine Timing frames that are received with the To DS subfield equal to 1. These frames were previously excluded. | Update to the current baseline and then insert the desired changes, while maintaining "legacy" behavior. | ***Revised***  According to ‘*Table 9-4—Combinations of To DS and From DS subfields in Management frames*’ in 11me, ‘To DS’ here is used to indicate whether the management frame is a QMF.  To make sure the legacy behaviour is maintained, the text is revised to reflect the actual intention.  And, there does missing the sentence ‘The QMF receiver shall use …’ in item d) of the text, so it should be added back.  *TGbf editor to add the changes shown in IEEE 802.11-23/0508r1 under all headings that include CID 2263.* |
| 2265 | Joseph Levy | 222.05 | The change made in has changed the legacy behavior. It is now requiring replay counters for PV1 protected Fine Timing frames that are received with the To DS subfield equal to 1. These frames were previously excluded. | Update to the current baseline and then insert the desired changes, while maintaining "legacy" behavior. | ***Revised***  According to ‘*Table 9-4—Combinations of To DS and From DS subfields in Management frames*’ in 11me, ‘To DS’ here is used to indicate whether the management frame is a QMF.  To make sure the legacy behaviour is maintained, the text is revised to reflect the actual intention.  And, there does missing the sentence ‘The QMF receiver shall use …’ in item d) of the text, so it should be added back.  *TGbf editor to add the changes shown in IEEE 802.11-23/0508r1 under all headings that include CID 2265.* |

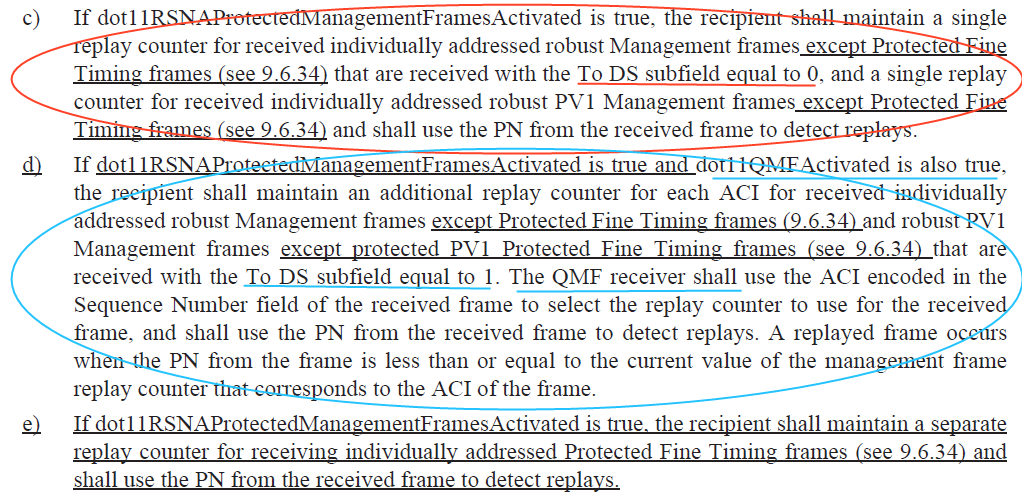
**For reference**:



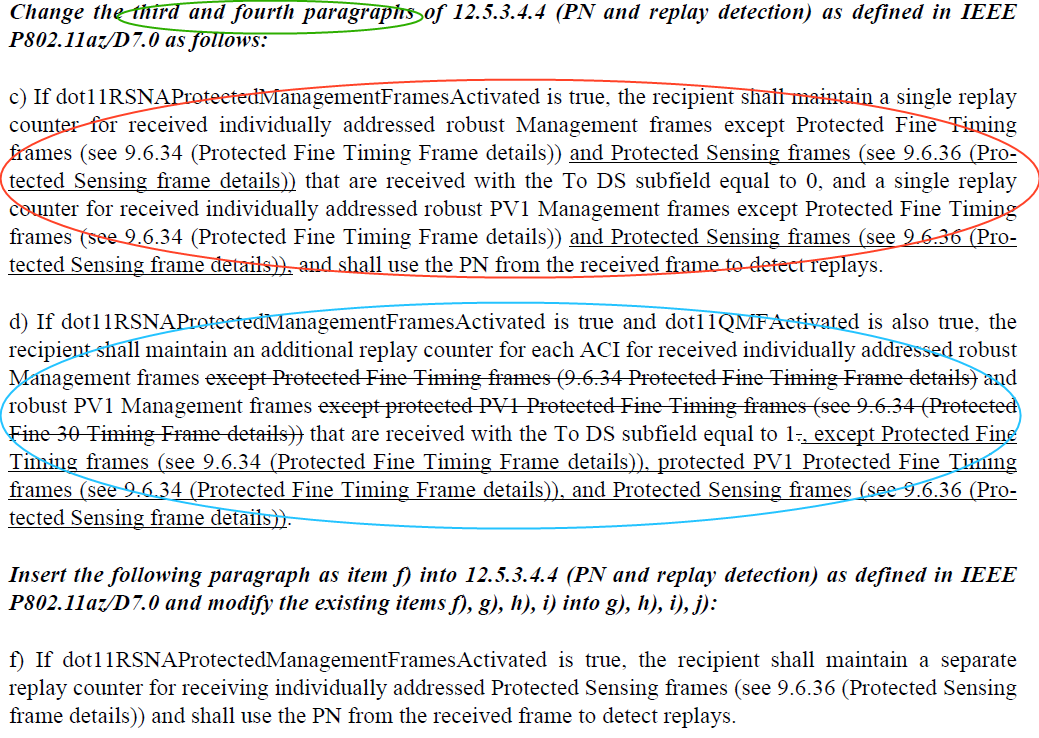
**12.5.2.4.4 PN and replay detection** in 11me:



**12.5.3.4.4 PN and replay detection** in 11az-2022:



**12.5.3.4.4 PN and replay detection** in 11bf D1.0:



# Resolution

**12.5.3.4.4 PN and replay detection**

*TGbf Editor: Please modify the text of 12.5.3.4.4 (PN and replay detection) as follows:*

*Change the third and fourth paragraphs of 12.5.3.4.4 (PN and replay detection) as defined in IEEE P802.11az/D7.0 as follows:*

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0, and 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)) ~~and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)),~~ and shall use the PN from the received frame to detect replays. (#2263)

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management ~~frames except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details )~~ and robust PV1 Management frames ~~except protected PV1 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 (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 1. The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame.(#2263)

**12.5.5.4.4 PN and replay detection**

*TGbf Editor: Please modify the text of 12.5.3.4.4 (PN and replay detection) as follows:*

*Change the third and fourth paragraphs of 12.5.5.4.4 (PN and replay detection) as defined in IEEE P802.11az/D7.0 as follows:*

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0, and 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)) ~~and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)),~~ and shall use the PN from the received frame to detect replays. (#2265)

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames ~~except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details )~~ and robust PV1 Management frames ~~except protected PV1 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 (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 1. The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame. (#2265)

# SP

Do you support resolutions to the following 4 CIDs and incorporate the text changes into the latest TGbf draft: 1478, 1479, 2263, 2265, in 11-23/0508r1.

Y/N/A