IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment resolution for Misc security comments | | | | |
| Date: 2023-03-17 | | | | |
| 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 6 CIDs are resolved: 1478, 1479, 2263, 2265, 2262, 2264.

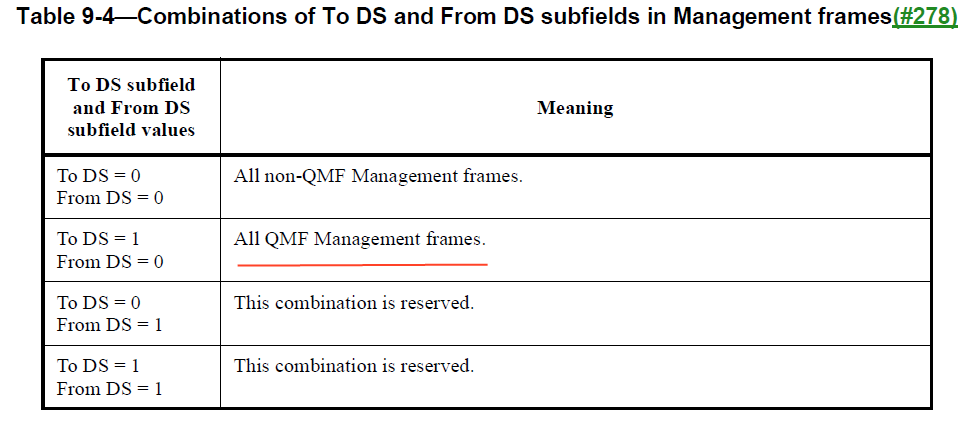
Revisions:

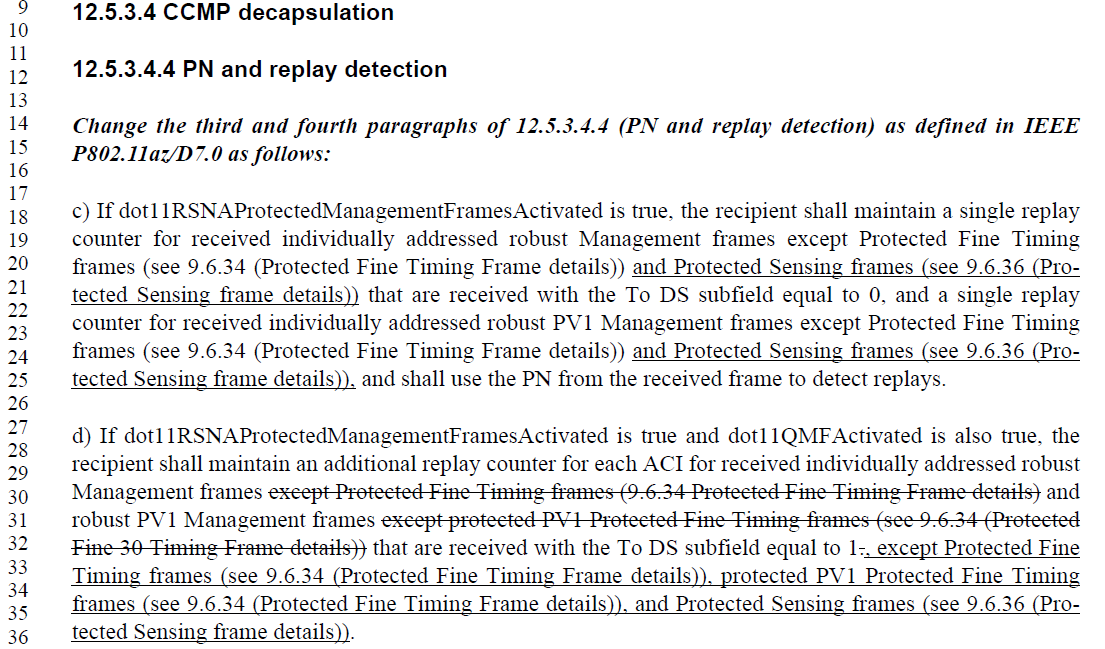
* Rev 0: Initial version of the document.

# 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. | ***Rejected***  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.  *Both the 11az text and 11bf text for Item d) are precluding PV1 protected Fine Timing frames to use the existing per ACI replay counters.* |
| 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. | ***Rejected***  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.  *Both the 11az text and 11bf text for Item d) are precluding PV1 protected Fine Timing frames to use the existing per ACI replay counters.* |

**For reference**:



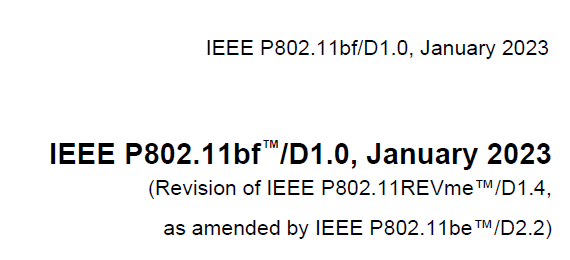


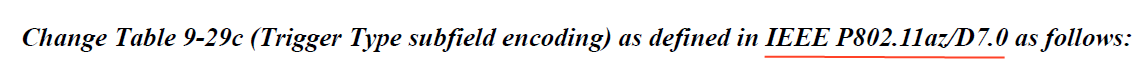
# Baseline

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 2262 | Joseph Levy | 221.30 | This clause has changed in the 802.11REVme D2.0 - this clause seems to be from the 802.11az amendment, but .11az is not listed as an amendment. Please correct and align the base line text. | Fix the base line. | ***Accepted***  *As stated in the PAR, 11az is the baseline of 11bf.*  *TGbf editor: please list 80211az-2022 as an amendment and change all appearances of ‘IEEE P802.11az/D7.0’ in the editor’s notes to ‘IEEE 80211az-2022’.* |
| 2264 | Joseph Levy | 221.49 | This clause has changed in the 802.11REVme D2.0 - this clause seems to be from the 802.11az amendment, but .11az is not listed as an amendment. Please correct and align the base line text. | Fix the base line. | ***Accepted***  *As stated in the PAR, 11az is the baseline of 11bf.*  *TGbf editor: please list 80211az-2022 as an amendment and change all appearances of ‘IEEE P802.11az/D7.0’ in the editor’s notes to ‘IEEE 80211az-2022’.* |

**For reference**:

*Draft P802.11bf\_D1.0, Page 1:*



****

# SP

Do you support resolutions to the following 6 CIDs and incorporate the text changes into the latest TGbf draft: 1478, 1479, 2263, 2265, 2262, 2264, in 11-23/0508r0.

Y/N/A