IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Replay Counter and MFPC Cleanup | | | | |
| Date: 2024-05-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Henry Ptasinski | Element78 Communications LLC |  |  | henry@e78com.com |

Abstract

This submission address some issues with the replay counter text in 802.11REVme\_D5.0.

R0: Initial version.

R1: Adjust text for replay counter rule (i)

R2: Add some discussion details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| - | 12.5.2.4.4 | 3029 | 47 | The MFPC bit must be set in the RSNIE during negotiation in order for management frame protection to be negotiated, so setting the MFPC bit after the negotiation and as a condition of the negotiation result doesn't make any sense.  Also at p3030 l19, p3043 l28, and p3043 l57. | Delete "shall set the MFPC bit on a given link to 1, it" in both locations. |

## Discussion

The setting of MFPC and MFPR are covered in clause 12.6.3 (for infra and tdls) starting at p3054 l39:

An AP and a non-AP STA shall use Table 12-5 (Robust management frame selection in an infrastructureBSS(#587)) and the values of the MFPC and MFPR subfields(#211) advertised in the RSNEs to determine if they may associate, and if so whether management frame protection is enabled.

Similar text for IBSS is contained in clause 12.6.4.

Clause 12.6.5 has more limited text covering MBSS:

All mesh STAs in an MBSS use the same group data cipher suite and the group management cipher suite (if management frame protection is enabled).

A note in 12.6.17 provides an definition of MFP negotiation:

NOTE 1—Management frame protection is negotiated for a link if both STAs set the MFPC bit to 1 (see 12.6.3 (RSNA policy selection in an infrastructure BSS), 12.6.4 (RSNA policy selection in an IBSS), 12.6.5 (RSNA policy selection in an MBSS), and 12.6.6 (RSNA policy selection in a PBSS)).

## Proposed resolution:

***Request the TGme editor to apply the changes below:***

***At P3029, L47:***

c) If (#4166)management frame protection is negotiated, the (#4212)receiver ~~shall set the MFPC bit on a given link to 1, it~~(#199) shall maintain a single replay counter for received individually addressed robust (#3573)PV0 Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))) that are received with the To DS subfield equal to 0, and (#3573)(S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))).

***At P3030, L19:***

f) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA(#3573), RA (individual or group address; not if TDLS) and priority value of the received MPDU. The receiver shall discard (#3573)fragmented MSDUs, A-MSDUs(#3089) and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. (#4166)(#199)If management frame protection is negotiated, the receiver ~~shall set the MFPC bit on a given link to 1, it~~ shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA(#3573), (QMF receiver of an individually addressed robust PV0 Management frame with the To DS subfield equal to 1 only) ACI, and (S1G STA only) Protocol Version subfield of that individually addressed Management frame.

***At P3043, L28:***

c) (#199)If (#4166)management frame protection is negotiated, the (#4212)receiver ~~shall set the MFPC bit on a given link to 1, it~~ shall maintain a single replay counter for received individually addressed robust Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))) that are received with the To DS subfield equal to 0(#3573), and a single replay counter for received individually addressed robust PV1 Management frames except PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))(11az).

***At P3043, L57:***

f) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA(#3573), RA (individual or group address; not if TDLS) and priority value of the received MPDU. The receiver shall discard (#3573)fragmented MSDUs, A-MSDUs(#3089) and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. (#4166)If management frame protection is negotiated, the receiver ~~shall set the MFPC bit on a given link to 1, it~~(#199) shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA (#3573)and (QMF receiver of an individually addressed robust Management frame with the To DS subfield equal to 1 only) ACI of that individually addressed Management

frame.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| - | 12.5.2.4.4 | 3029 | 49 | The "that are received ..." applies to the PV0 Management frames not the Fine Timing frames. | Change:  "a single replay counter 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 0,"  to:  "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))," |
| - | 12.5.2.4.4 | 3029 | 57 | The "that are received ..." applies to the PV0 Management frames not the Fine Timing frames. | Change:  "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."  to:  "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))" |
| - | 12.5.4.4.4 | 3043 | 30 | The "that are received ..." applies to the PV0 Management frames not the Fine Timing frames. | Change:  "a single replay counter for received individually addressed robust Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))) that are received with the To DS subfield equal to 0,  to:  "a single replay counter for received individually addressed robust 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))," |
| - | 12.5.4.4.4 | 3043 | 39 | The "that are received with the To DS subfield equal to 1" applies to the PV0 Management frames, not the Fine Timing frames or the PV1 frames. | Move “ that are received with the To DS subfield equal to 1” to apply to the PV0 Management frames. |
| - | 12.5.4.4.4 | 3043 | 32 | PV1 frames are not supported with GCMP. | Delete:  ",and a single replay counter for received individually addressed robust PV1 Management frames except PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details))" |
| - | 12.5.4.4.4 | 3043 | 39 | PV1 frames are not supported with GCMP. | Delete:  “ and robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))) that are received with the To DS subfield equal to 1.” |

## Discussion:

Prior to addtion of protected fine timing frames, the replay counter text for robust Management frames was:

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames that are received with the To DS subfield equal to 0, …

The Protected Fine Timing text was inserted in the middle of the phrase, so the “To DS” condition now looks like it applies to the Protected Fine Timing frames instead:

c) If (#4166)management frame protection is negotiated, the (#4212)receiver shall set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust (#3573)PV0 Management frames (11az) except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))) that are received with the To DS subfield equal to 0, and (#3573)(S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))).

## Proposed resolution:

***Request the TGme editor to apply the changes below:***

***Option 1:***

***At P3029:***

c) If (#4166)management frame protection is negotiated, the (#4212)receiver shall set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust (#3573)PV0 Management frames (11az)~~except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))))~~ 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(11az)))), and (#3573)(S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))).

d) (11az)If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the (#4212)receiver shall maintain an additional replay counter for each ACI for received individually addressed robust (#3573)PV0 Management frames (11az)~~except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))))~~ 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(11az)))).

***At P3043:***

c) (#199)If (#4166)management frame protection is negotiated, the (#4212)receiver shall set the MFPC bit on a given link to 1, it shall maintain a single replay counter for received individually addressed robust Management frames (11az)~~except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))~~ that are received with the To DS subfield equal to 0(#3573) except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))~~, and a single replay counter for received individually addressed robust PV1 Management frames except PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))(11az)~~.

d) (11az)If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the (#4212)receiver shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames (11az)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(11az))) ~~and robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))) that are received with the To DS subfield equal to 1~~.

***Option 2:***

***At P3029:***

c) If (#4166)management frame protection is negotiated, the (#4212)receiver shall set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust (#3573)PV0 Management frames (11az), except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))), that are received with the To DS subfield equal to 0, and (#3573)(S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames (11az)except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))).

d) (11az)If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the (#4212)receiver shall maintain an additional replay counter for each ACI for received individually addressed robust (#3573)PV0 Management frames (11az), except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))), that are received with the To DS subfield equal to 1.

***At P3043:***

c) (#199)If (#4166)management frame protection is negotiated, the (#4212)receiver shall set the MFPC bit on a given link to 1, it shall maintain a single replay counter for received individually addressed robust Management frames (11az), except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))), that are received with the To DS subfield equal to 0(#3573)~~, and a single replay counter for received individually addressed robust PV1 Management frames except PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))(11az).~~

d) (11az)If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the (#4212)receiver shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames (11az), except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))), ~~and robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az)))~~ that are received with the To DS subfield equal to 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Line | Comment | Proposed Change |
| - | 12.5.2.4.4 | 3030 | 32 | The phrase "check that  the replay counter used to detect replays is correct" does not clearly specify the required behavior. | Change:  "If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect."  to:  "If the receiver performs replay detection prior to decryption, then the receiver shall check that the PN of the received frame is greater than the appropriate replay counter, and discard the frame if incorrect." |
| - | 12.5.2.4.4 | 3030 | 34 | The sentence regarding the separate FTM replay counter is unnecessary. The requirement is already covered in item (f). Similar text is not present in Clause 12.5.4.4.4. The standard does not call out any of the other (many) replay counters in this way. | Delete:  "In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-15 (Expanded CCMP MPDU(#3525)(11az))) signals that the management PDU is a Protected Fine Timing frame." |

## Proposed resolution:

***Request the TGme editor to apply the changes below:***

***At P3030 L32:***

i) (11az)If the receiver performs replay detection prior to decryption, then the receiver shall ~~check that~~

~~the replay counter used to detect replays is correct and discard the frame if incorrec~~discard the frame if the PN of the received frame is less than or equal to the corresponding replay counter specified in rule (f). ~~In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-15 (Expanded CCMP MPDU(#3525)(11az))) signals that the management PDU is a Protected Fine Timing frame.~~ The replay counter shall not be updated unless the decryption is successful and the frame is accepted.

**References:**

[**Draft P802.11REVme\_D5.0.pdf**](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11me/Draft%20P802.11REVme_D5.0.pdf)