IEEE P802.11
Wireless LANs

|  |
| --- |
| Some TGaz SA Ballot 1 CRs |
| Date: December 07 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | nehru.bhandaru@broadcom.com |

Abstract

This document contains discussion and proposed resolutions for some of the comments from SA Ballot 1 on P802.11az/D4.0. Considered comments are: 288269, 288243, 288055, 288054, 287873, 287834, 287669, and 287648.

Proposed changes are relative to IEEE P802.11-REVme™/D0.4.

Revision Notes

R0 – initial version

References

[1] IEEE P802.11-REVme™/D0.4, October 2021

[2] P802.11az/D4.0, August 2021

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | ClausePage/Line | Comment | Proposed Change | Resolution |
| 288269 | 11.21.6.3.4137.17 | "When Management Frame Protection is negotiated for TB and non-TB ranging" - shouldn't this be in a more gnereral section, not restricted to secure LTF (+ bullett points) | move to subclause 11.21.6.3.1, page 127, line 20 | ReviseAgree in principle with the commentor. However 11.21.6.3.1 applies to EDCA ranging also. Propose to move to 11.21.6.3.3 the section specific to TB and NTB ranging (to which MFP applies although there is no secure LTF)TGaz Editor: Move the paragraph p137.17-20 to the more general section before 11.21.6.3.3 p135.37 |
| 288243 | 11.21.6.3.3135.37 | "An RSTA shall reject a request, unless the request is for passive TB ranging, if it has set the URNM-MFPR field of the RSNXE (#3940) to 1, and the ISTA has not successfully set up a PTKSA to protect IFTMR, IFTM and LMR frames exchanged between the RSTA and the ISTA." - create an exception for 20 MHz only STAs | Change to "An RSTA shall reject a request, if it has set the URNM-MFPR field of the RSNXE (#3940) to 1, and the ISTA has not successfully set up a PTKSA to protect IFTMR, IFTM and LMR frames exchanged between the RSTA and the ISTA, with the following exceptions: i) the request is for passive TB ranging, or ii) the request has has a Format and Bandwdith value indicating 20 MHz bandwidth." | ReviseAgree in principle with the commentor. Currently implementations are certified that have the requested behavior. This is related to CID 287669. See discussion later in the document.TGaz Editor: Make changes for the CID described in <https://mentor.ieee.org/802.11/dcn/21/11-21-1979-00-00az-sa1-nb-crs-a.docx> |
| 288055 | 4.5.4.223.41 | The term "preassociation security negotiation authentication" is clumsy. Isn't the "security negotiation" == "authentication" or at least authentication is part of the "security negotiation". | Change the term so that it aligns better with the other terms (open system authentication, shared key authentication, etc.). In each case it is "<some characteristic> authentication". Perhaps, in this case, it should simply be "preassociation authentication" | RejectNegotiation does not mean authentication. PASN sets up security context – e.g., PTKSA. Security negotiation may not include authentication, in general e.g., PSK modes. Open system authentication does not do any authentication (security wise) – and the authentication refers to 802.11 authentication (frame use)Also note that FILS authentication is similar – Fast Initial Link Setup Authentication. I agree we could rename PASN w/ PASS (pre-association security setup), but I think there is enough contextual text that makes the intended semantics clear.TGaz Editor: No change to the draft. |
| 288054 | 4.5.4.224.6 | Is it really "prior to association", i.e., association will necessarily happen? Or is it without association? Also, some unnecessary capitalization. | Change to "PASN authentication allows for the protection of Management frames without association." | AcceptTGaz Editor: Change as suggested i.e.,PASN authentication allows ~~Management Frame Protection prior to~~ protection of Management frames without association by establishing a PTKSA using authentication frames. |
| 287873 | 11.21.6.4.5.3174.19 | In the text "Or the ista-ltf-key and ltf-iv for generating secure HE-LTF based on (#1830, #1832) the values of the Secure LTF Counter (#2289) and the corresponding Validation SAC subfields in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame, received from the RSTA; see 11.21.6.4.5.4 (Secure LTF octet stream generation)."  the Validation SAC is no longer needed as we changed derivation, see equation in P280L18-19 | Change it to "Or the ista-ltf-key and ltf-iv for generating secure HE-LTF based on (#1830, #1832) the values of the Secure LTF Counter (#2289) subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame, received from the RSTA; see 11.21.6.4.5.4 (Secure LTF octet stream generation)." | AcceptAgree with the commentor. Validation SAC is no longer used to derive LTF keysTGaz Editor: Change as suggested, except in addition replace values by value (editorial change) |
| 287834 | 9.3.1.1944.1 | Multi-bit field values should be specified as an integer. | In table 9-23d, merge the two columns for B0 and B1 into one column.And specify the NDPA Announcement Type subfield as an integer value.I.e.0 | VHT NDP Announcement frame1 | Ranging NDP Announcement frame2 | HE NDP Announcement frame3 | Reserved | Revise.Agree with the commentor. It seems to be the style in base TGm draft.TGaz Editor: Please change as suggested by <https://mentor.ieee.org/802.11/dcn/21/11-21-1979-00-00az-sa1-nb-crs-a.docx> |
| 287669 | 9.4.2.24171.20 | Bit 10 of the RSN Extension Element "URNM-MFPR" - we do not have enough flexibility in the defintion of this bit for AP policies | Amend meaning of this bit to carve out an exeption of other use cases, e.g., IoT, and/or create a second bit to support more differentiated policies | ReviseThis is related to CID 288243; the currently specified bit in RSNXE is for this behavior, but it has been used w/ an exemption for 20 MHz devices.TGaz Editor: Please change as suggested by <https://mentor.ieee.org/802.11/dcn/21/11-21-1979-00-00az-sa1-nb-crs-a.docx> |
| 287648 | 3.221.4 | The definition of PASN Authentication frame is "An Authentication frame used in PASN" | Remove or actually include information in the defition that is not given in the name | RevisePerhaps PASN could be expanded in the definition. This definition was added in response to an earlier comment that wanted the definition of that seemingly obvious definition…TGaz Editor: Replace the definition with “Authentication frame used in Preassociation security negotiation” |

**CID 287834**

**Discussion**

Table 9-23d style needs to change to specify values for integral subfields, rather than bit values.

**Proposed Changes**

TGaz Editor: Replace Table 9-28d - NDP Announcement frame variant encoding with the following table

|  |  |
| --- | --- |
| **NDP Announcement Type subfield** | **NDP Announcement frame variant** |
| 0 | VHT NDP Announcement frame  |
| 1 | Ranging NDP Announcement frame  |
| 2 | HE NDP Announcement frame  |
| 3 | Reserved |

**CID 287669 and 288243**

Bit 10 of the RSN Extension Element "URNM-MFPR" - we do not have enough flexibility in the defintion of this bit for AP policies

**Discussion**

Agree in principle with the commentor.

Some IoT etc., use cases exist that need to allow PASN without security w/ 20 MHz.

WFA is using the current RSNXE capability bit as described by the proposed change for CID 288243 by the commentor i.e., exempt 20 MHz BW STAs to allow certain use cases.

A new bit can be defined in RSNXE to disallow the exemption, for completeness and other environments that need to be more secure.

The corresponding RSNXE capability bit and MIB variables should be renamed or extended – as one might need another policy bit to disallow the exemption in the future for certain other deployments.

**Proposed Changes**

TGaz Editor: Add the following definition to § 3.3 p21.31

**Unassociated Range Negotiation and Measurement Management Frame Protection Required Exempt 20MHz (URNM-MFPR-X20)**: A security policy that specifies whether ranging frames are required to be protected without association if bandwidth greater than 20 MHz is used.

TGaz Editor: Rename the row for the current definition for URNM-MFPR in table 9-321 (RSNXE)



with the following

|  |  |  |
| --- | --- | --- |
| 10 | URNM-MFPR-X20 | A STA sets the URNM-MFPR-X20 field to 1 if dot11RSTARequiresPMFActivated is set to 1. Otherwise, it sets the field to 0. See 11.21.6.3.1. (General), C.3 MIB detail. |

TGaz Editor: Add additional ANA row for the current definition for URNM-MFPR in table 9-321 (RSNXE)

|  |  |  |
| --- | --- | --- |
| <ANA-<URNM-MFPR>> | URNM-MFPR | A STA sets the URNM-MFPR field to 1 if dot11RSTARequiresPMFActivated is set to 2. Otherwise, it sets the field to 0. See 11.21.6.3.1. (General) |

TGaz Editor: Change the type for the MIB variable dot11RSTARequiresPMFActivated to INTEGER that takes a defined set of values for the feature P269.18

dot11RSTARequiresPMFActivated ~~TruthValue~~ INTEGER,

TGaz Editor: Replace the MIB definition for dot11RSTARequiresPMFActivated by the following p271.7

dot11RSTARequiresPMFActivated OBJECT-TYPE

SYNTAX INTEGER {Inactive (0), Required-X20M (1), Required (2)}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity or the SME.

Changes take effect at the next occurrence of an MLME-START.request or MLME-JOIN.request primitive.

The attribute applies only to preassociation ranging behavior.

When set to Required (2), indicates that the station requires Management Frame Protection for all management frames exchanged during the negotiation and measurement reporting.

When set to Required-X20M (1), indicates that the station Management Frame Protection for all management frames exchanged during the negotiation and measurement reporting except those using a 20 MHz bandwidth for measurements.

Otherwise, when set to Inactive (0), indicates that Management Frame Protection is not required for ranging.

see 11.21.6.3.1 (General), and range measurement procedure; see 11.21.6.4.3 (TB ranging measurement exchange), 11.21.6.4.4 (Non-TB ranging measurement exchange); and 11.21.6.4.5 (Secure LTF in the TB and non-TB ranging measurement exchange protocol) to successfully negotiate a range measurement session; see 11.21.6.3.1(General)."

DEFVAL { Inactive }

::= { dot11WirelessMgmtOptionsEntry 57 }

TGaz Editor: Replace the paragraph at p125.24 about how URNM-MFPR is set in RXNE

A STA in which dot11RSTARequiresPMFActivated is true shall set the URNM-MFPR field of the 24 RSNXE (#**3940**) to 1. Otherwise, it shall set the URNM-MFPR field to 0. (#**5372E**)

with the following

A STA in which dot11RSTARequiresPMFActivated has the value Required (2) shall set the URNM-MFPR field of the RSNXE to 1. Otherwise, it shall set the URNM-MFPR field to 0.

A STA in which dot11RSTARequiresPMFActivated has the value Required-X20M (1) shall set the URNM-MFPR-X20M field of the RSNXE to 1. Otherwise, it shall set the URNM-MFPR-X20M field to 0.