IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Misc text clarification | | | | |
| Date: 2021-01-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom |  |  | nehru.bhandaru@broadcom.com |
| Jonathan Segev | Intel |  |  | Jonathan.segev@intel.com |
| Dibakar Das | Intel |  |  | Dibakar.das@intel.com |
| Ali Raissinia | Qualcomm |  |  |  |
| Christian Berger | NXP |  |  |  |
| Ido Ouzieli | Intel |  |  |  |

Abstract

This text proposes some minor bug fixes to draft 2.6.

Revisions:

* Rev 0: Initial version of the document.

**Discussion:**

1. The usage of the Protection of Range Negotiation and Measurement Management Frames Required field in the case of FTM session between two associated STAs is unclear. The corresponding MIB variable “dot11RSTARequiresPMFActivated” is defined only for pre-associated case. However, elsewhere the spec seems to imply this field also applies for the associated STAs:

“If an RSTA has set the Protection of Range Negotiation and Measurement Management Frames Required field in the RSNXE to 1, in the cases listed above, an ISTA shall establish a security”.

Note that since LMR and FTM frames are classified as Robust Action frames an associated STA capable of MFP will protect them per baseline 802.11 standard. No additional control required for that behaviour. This is also clarified in current spec:

“If the ISTA and the RSTA are associated, the security context is established as defined in 12.6.19 (Protection of Robust Management Frames), and 12.6.20 (Robust management frame selection procedure).”

To clarify the usage of the Protection of Range Negotiation and Measurement Management Frames Required field only for the unassociated case we propose the following:

* Rename this field to “Protection of Range Negotiation and Measurement Management Frames Required Unassociated (RNM-UMFP)” to reaffirm its usage only for the unassociated case.
* If this bit is set to 1 by an RSTA, then RSTA also sets the MFPC bit in RSN Capabilities to 1.
* Modify the text describing every usage of it so that it is limited only to unassociated case.

1. There is some ambiguity regarding whether an existing FTM session continues or is terminated when the ISTA becomes associated or disassociated from the RSTA. In particular, consider the case where an associated ISTA has an FTM session that’s protected by baseline PMF. However, once the ISTA becomes disassociated its not clear whether the FTM session should still be protected or not. As such we believe the simplest approach is to terminate an existing FTM session and renegotiate a new one at all such transition events.

**3.4 Abbreviations and acronyms**

TGaz Editor: Add the following entry into 3.4 in alphabetic order:

RNM-UMFP: Protection of Range Negotiation and Measurement Management Frames Required Unassociated

**9.4.2.241 RSN Extension element (RSNXE)**

TGaz Editor: Modify the third row in Table 9-321 on page 68 (line 22) as follows

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 10 | Protection of Range Negotiation and Measurement Management Frames Required Unassociated | A STA sets the Protection of Range Measurement Management Frames Required field to 1 if dot11RSTARequiresPMFActivated is true. Otherwise the STA sets the Protection of Range Measurement Management Frames Required field to 0. See 11.21.6.3.1 (General) |

**11.21.6.3 Fine Timing Measurement procedure negotiation**

**11.21.6.3.1 General**

TGaz Editor: Modify the paragraph starting on page 123 (line 8) as follows

NOTE—The MFPC and MFPR capabilities define if the security context between an RSTA and an associated ISTA is established or not.

TGaz Editor: Modify the paragraph starting on page 123 (line 29) as follows

An RSTA shall set the RNM-UMFP field in the RSNXE to 1 only if it has set the MFPC bit to 1 in the RSN Capabilities field in the RSN element.

Protection of Management frames for ranging negotiation and measurement while associated is possible only if both RSTA and ISTA are MFP capable.

An RSTA that requires protection of Management frames for ranging negotiation and measurement

for associated ISTAs can either set the MFPR bit to 1 in the RSN Capabilities field in the RSN element or reject FTM session setup attempts that use an unprotected IFTMR.

If an RSTA has set the RNM-UMFP field in the RSNXE to 1, in the cases listed above, an ISTA that is not associated to the RSTA shall establish a security context with that RSTA prior to initiating a Fine Timing Measurement Procedure Negotiation with that RSTA. (#3236)

Furthermore, an RSTA shall reject a request in the cases listed above, if it has set the RNM-UMFP field of the RSNXE to 1, and an ISTA that is not associated to it and has not successfully set up a security context to protect FTMR, FTM and LMR frames exchanged between the RSTA and the ISTA. The RSTA may accept the request in the cases not listed above. (#3940, #3236)

TGaz Editor: Modify the paragraph starting on page 131 (line 9) as follows

An RSTA shall reject a request from an unassociated ISTA, unless the request is for Passive TB Ranging, if it has set the RNM-UMFP field of the RSNXE (#3940) to 1, and the ISTA has not successfully set up a security context to protect IFTMR,  
IFTM and LMR frames exchanged between the RSTA and the ISTA.

TGaz Editor: Replace all instances elsewhere of the word “ Protection of Range Negotiation and

Measurement Management Frames Required” with “RNM-UMFP”

**11.21.6.6.2 TB Ranging and Non-TB Ranging session termination**

TGaz Editor: Add the following paragraph starting on page 187 (line 23) as follows:

When negotiation or measurements for a secure or non-secure FTM session are in progress, the FTM session shall automatically terminate if an association is initiated or terminated (See procedures in 11.3.5 (Association, reassociation, and disassociation)).

[place document body text here]

**References:**