IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution to CID 5058 |
| Date: 2019-08-16 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Solomon Trainin | Qualcomm |  |  | strainin@qti.qualcomm.com |
| Yunsong Yang | Self |   |  | yunsongyang1@gmail.com |

Abstract

This document proposes text changes to resolve LB242 comment CID 5058.

**Background**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed change** | **Resolution** |
| 5058 | 9.4.2.127 | 120.16 | It is better that the new Protected DMG Dual Support subfield be verified in the security context during 4-way handshake and Re(Association) procedures to prevent downgrade attack. TGm defined a new RSN Extension element, which can be used for such purpose (see REVmd D2.3 or doc. 11-19-114r5). | Add the cited bit to the Extended RSN Capabilities field in the RSN Extension element. | Revised. |

**Discussions**

* Agree with the commemter that the cited subfield should be verified in the security context. The proposal is to remove the cited subfield from the DMG Capabilities element and add the subfield in the RSNXE, which can be sent by AP in Beacons, Probe Response frames, 4-way handshake message 3, FILS (Re)association Response, and FT authentication sequence messages 3 and 4, can be sent by non-AP STA in (Re)association Request frames and 4-way handshake message 2, and is verified during 4-way handshake, FT reassociation, and FILS (re)association. The RSNXE is already defined in REVmd D2.3.
* In addition, the subfield should be set based on a MIB variable, not based on if the Management Frame Protection Capable field in the RSNE is set to 1, as the text in 12.6.20 implies. The use of the relevant protected DMG Action frames in the non-DMG STA is based on both conditions are met. Therefore, it is proposed that dot11ProtectedAnnounceImplemented be added to dot11DMGSTAConfigEntry.

**Proposed text changes:**

*Change the Protected DMG Dual Support subfield (B52) in Figure 9-547 back to “Reserved” and delete the inserted paragraph of “The Protected DMG Dual Support subfield is set to 1 to indicate that the STA supports Protected Dual of Unprotected DMG Action frames as described in 12.6.20. Otherwise, it is set to 0.”*

*Insert the following changes to subclause 9.4.2.241 in P802.11 REVmd D2.3, as highlighted.*

9.4.2.241 RSN Extension element (RSNXE)

…

|  |
| --- |
| Table 9-322 Extended RSN Capabilities field  |
| Bit | Information | Notes |
| 0-3 | Field Length  | The length of the Extended RSN Capabilities field, in octets, minus 1, i.e., *n*-1. |
| 4 | Protected TWT Operations Support | The STA sets the Protected TWT Operations Support field to 1 when dot11ProtectedTWTOperationsImplemented is true, and sets it to 0 otherwise. See 10.48.1 (TWT overview). |
| 5 | Protected Announce Support | The non-EDMG STA sets the Protected Announce Support field to 1 when dot11ProtectedAnnounceImplemented is true, and sets it to 0 otherwise. See 12.6.20 (Robust management frame selection procedure). |
| 6 – (8×n – 1) | Reserved |  |

***Change 12.6.20 in P802.11ay D4.0 as highlighted:***

**12.6.20 Robust management frame selection procedure**

*Insert the following at the end of the section*

If a Protected Announce Action frame exists to allow robust STA-STA communications of the same information that is conveyed in the corresponding Announce Action frame, the protected variant shall be transmitted when the dot11ProtectedAnnounceImplemented equals true by each communicating DMG STA.

Otherwise, Protected Announce Action frame of the category DMG Action shall not be used.

An DMG STA shall not set the dot11ProtectedAnnounceImplemented equals true if the dot11RSNAProtectedManagementFramesActivated equals false.

An non-EDMG STA shall transmit the RSNXE with the the Protected Announce Support field to 1 when the dot11ProtectedAnnounceImplemented equals true. (9.4.2.241 RSN Extension element (RSNXE)).

An EDMG STA shall set the dot11ProtectedAnnounceImplemented to true if the dot11RSNAProtectedManagementFramesActivated equals true. The Protected Announce Support filed is set to 0 in the EDMG STA.

The Unprotected DMG Action frames are listed in 9.6.21.1 and the DMG Action frames are listed in 9.6.19.

***Change table (“dot11DMGSTAConfigEntry”) as follows:***

Dot11DMGSTAConfigEntry ::=

SEQUENCE {

dot11DMGOptionImplemented TruthValue,

dot11RelayActivated TruthValue,

dot11REDSActivated TruthValue,

dot11RDSActivated TruthValue,

dot11MultipleMACActivated TruthValue,

dot11ClusteringActivated TruthValue,

dot11DiscoveryAssistanceActivated TruthValue,

dot11DMGTDDLocalClockModeActivated TruthValue,

dot11DMGTimeAdvertisementBeaconInterval Unsigned32,

dot11ExtendedTPCActivated INTEGER,

dot11TDDOptionImplemented TruthValue,

dot11SAROptionImplemented TruthValue,

dot11UnsolicitedBAActivated TruthValue,

dot11ProtectedAnnounceImplemented TruthValue

}

***Insert the following MIB variables to the end of dot11DMGSTAConfigTable:***

dot11ProtectedAnnounceImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute, when true indicates the station supports the use of Protected Announce Action frame. The attribute is set to true only if the dot11RSNAProtectedManagementFramesActivated is true. "

DEFVAL { false }

::= { dot11DMGStationConfigEntry 14}