IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB249-Clause-11-24-6-4-2-CID-Resolution | | | | |
| Date: 2020-01-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | akasher@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions to LB249 comments 3905. The base is TGaz D2.0.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3905 | 128.00 | 11.22.6.4.2 | "When a Secure Fine Timing Measurement Session is established as described in 11.22.6.3.1, the 31 Fine Timing Measurement frames transmitted during the execution of Measurement Exchange 32 shall be Protected Dual of Public Action frames (See Cl. 9.6.10 Protected Dual of Public Action 33 frames)." What is a "secure Fine Timing Measurement session" precisely? Using PMF to protect the negotiation frames without employing secure LTF also provides some level of security, is it considered a secure Fine Timing Measurement session? Or, does the highlighted text mean "a FTM session using secure LTF"? | Please clarify the meaning of a secure Fine Timing Measurement session, and modify the text accordingly throughout the 11az spec wherever appropriate. |  |

Discussion:

The draft defines two levels of “Secure FTM”. One level is a based on MAC security using PMF. This is controlled by the “Protection of Range Negotiation and Measurement Management Frames Required” field in the extended capability element. The second level is a base on PHY level security using secure LTF. This is controlled by the Secure LTF Support field in the extended capability element and the Secure LTF Required subfield in the Ranging Parameters element in TB and non-TB ranging and the Securet ToF Supported field in the Beamforming Capability subelement of the EDMG capabilities element, and the Secure ToF Measurement subfield in the Measurement Parameters field of the IFTMR and the initial FTM frame. The term “Secure Fine Timing Measurement” is meant to describe the MAC level security. It may be good to clarify in the names of the subclauses that deal with the PHY level security, that Secure LTFs and Secure TRNs are used.

***TGaz Editor: Modify the title of subclause 11.22.6.4.6 in P153L22 as follows:***

**11.22.6.4.6 Secure LTF based Non-TB and TB Ranging Measurement Exchange Protocol**

***TGaz Editor: Modify the title of subclause 11.22.6.4.6.1 in P153L23 as follows:***

**11.22.6.4.6.1 Secure LTF Non-TB ranging mode**

***TGaz Editor: Modify the title of subclause 11.22.6.4.2.1.6 in P133L30 as follows:***

**11.22.6.4.2.1.6 Secure EDMG TRNs based measurement exchange for EDMG STAs**

***TGaz Editor: Modify figure 9-10000 in P61L24 as follows:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 | B3 | B4 B7 |
|  | Fine Timing  Measurement  Responder | Fine Timing  Measurement  Initiator | PDMG/PEDMG supporting APs in the area | Protection of Range Negotiation and Measurement Management Frames Required | Reserved |
| Bits: | 1 | 1 | 1 |  | 5 |

***TGaz Editor: Insert the following text after P61L35:***

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 11.22.6.3.1 (Range Measurement Negotiation)

***TGaz Editor: Modify the text in P116L6-15 as follows:***

Prior to initiating a Fine Timing Measurement Procedure Negotiation for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the Extended Capabilities element or the DMG Fine Timing and Range Measurement Capability Information field to 1, an ISTA shall establish a security context with the RSTA.

An ISTA initiating a Fine Timing Measurement Procedure Negotiation for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the Extended Capabilities element or the DMG Fine Timing and Range Measurement Capability Information field to 0 may establish a security context with the RSTA based on its operating policy setting.

**References:**

**P802.11az D2.0**