IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for Location |
| Date: 2019-10-16 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Electronic City, Bangalore India |  | Girish.madpuwar@broadcom.com  |
| Nehru Bhandaru | Broadcom | San JoseCA, USA |  | Nehru.bhandaru@broadcom.com |
| Mengchang Doong  | Broadcom | San Jose, CA USA |  |  |

**Abstract**

This submission proposes resolutions of comments received from LB240.

* CIDs: 2148, 1090

The comments are based on TGaz Draft 1.0 and the proposed changes are relative to TGaz Draft 1.5

Revision 0: initial draft

Revision 1 and 2: Based on Draft 1.5 – address 2148

Revision 3/4: Update to address CID 1090 deficiencies

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 2148 | 11.22.6.4.1 | 53 | [Re-raising this comment from the comment collection, as it is not possible to determine from 18/1544r8 whether/how it was addressed. References are to the CC draft and hence may be wrong against D1.0.]"RSTA centric EDCA based" is confusing -- is there any EDCA-based mode that is not RSTA-centric? |  | Revise.Most of the references to RSTA centric.. are removed and revised. They are not present in TGaz Draft 1.5.TGaz Editor: Replace in Draft 1.5 the single instance (p89.37) of “11.22.6.4.2 RSTA Centric EDCA based scheduling Measurement” with “11.22.6.4.2 EDCA based ranging measurement exchange” |
| 1090 | Alecsander Eitan | 1 | 1.01 | Missing test vectors for all the Secure operations | Revised.TGaz Editor: CID 1090 was partially addressed in 11-19-718r3 whose resolutions are already adopted into Draft 1.5. Incorporate the changes in this document relative to Draft 1.5 to fix some inaccuracies in the test vectors. |

CID 1090 Discussion:

This CID was partially addressed in 11-19-718r3 whose resolutions are already adopted into Draft 1.5.

The endian order used for counter in computing the secure LTF bits was incorrect.

The following test vector received a secondary verification

**TGaz editor: Modify the following in J.14.1 p232 as follows**

Downlink Secure LTF bits are derived as follows, 176 bits that comprise of 156 bits for 80 MHz

Bandwidth, two symbols for repetition and two repetitions, plus 16 bits for SAC rounded to

nearest multiple of 8 bits. 3

SAC || Secure-LTF-DL-bits = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF 4 Expansion”, Secure-LTF-Counter)

Hash: SHA-256

Length: 176 (bits)

Secure-LTF-Key-Seed:

07606f7b0d98ca03ec2d61e17c6bdfd3

0e2f2030e3470222551a05ec55d135b9

Secure-LTF-Counter: ~~0x000000000005~~  **0x000000000100**

SAC: ~~19 a0~~ **e5 b9**

Secure-LTF-DL-Bits:

~~3f28725c316c5e9d12a68f06a9577645 17~~

~~8f2d2833~~

**88 12 d5 b7 75 8e cf c6 4b 03 34 93 70 a1**

**31 57 12 b5 d6 20**

**…**

Secure-LTF-Counter: ~~0x000000000005~~**0x000000000100**

SAC: ~~83 1f~~ **e5 b9**

Secure-LTF-UL-Bits:

~~928e0a8d7a999f8756241ea7c7e652f6 9~~

~~73cc9fc6~~

**da ac 92 58 02 f1 d7 d4 1e 62 3f 5d a0 a8 3e 7a**

**10 5a d4 71**