IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of (most of) the GCMP Comments | | | | |
| Date: 2010-07-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission also proposes two ways to address CIDs 2012, 2101, 2102, 2111, 2112, 2113, 2250, 2251, 2298, 2327, 2328, 2294, 2295, 2296, 2633, 2634, 2635, 2636, 3048, 3049, 3117, 3118, 3120, 3302, 3538 from LB178.

It does not propose a way to address CIDs 2252, 2253, 2329, 2330, also from LB178.

***Option 1: eliminate the section in its entirety. TKIP is deprecated already so there’s no need to mention it. GCMP is not explicitly prohibited, which is OK since it is technically superior to CCMP and cannot be prohibited.***

***Option 2, explain why TKIP is not suitable for VHT and since GCMP is technically superior to CCMP, do not mention it (therefore, it is not explicitly prohibited).***

### 11. Security

### 11.4 RSNA security association management

### 11.4.3 RSNA policy selection in an ESS

*Insert the following text at the end of the 3rd paragraph of section 11.4.3:*

Within an ESS, a VHT STA shall eliminate TKIP as a choice for the pairwise cipher. TKIP is inappropriate for a VHT STA because the security assumption of its authentication component (Michael) is too low (2-20 for TKIP versus 2-64 for CCMP).

### 11.4.4 RSNA policy selection in an IBSS and for DLS

*Insert the following text after the 3rd paragraph of section 11.4.4:*

A VHT STA that is in an IBSS or that is transmitting frames through a direct link shall eliminate TKIP as a choice for the pairwise cipher suite. TKIP is inappropriate for a VHT STA because the security assumption of its authentication component (Michael) is too low (2-20 for TKIP versus 2-64 for CCMP).

**References: 11-11-0964-00-000ac-prohibiting-technology**