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 a way to resolve 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 resolve CIDs 2252, 2253, 2329, 2330, also from LB178.

***Instruct the editor to incorporate the following changes from section 8.4.2.27.2 into the draft:***

### 8.4.2.27.2 Cipher suites

The cipher suite selector 00-0F-AC:4 (CCMP) is the default cipher suite value.

The cipher suite selectors 00-0F-AC:1 (WEP-40) and 00-0F-AC:5 (WEP-104) are only valid as a group cipher suite in a transition security network (TSN) and allow pre-RSNA devices to join the BSS.

Use of any group cipher suite other than TKIP, WEP-104, or WEP-40 with TKIP as the pairwise cipher suite is not supported.

Use of GCMP as a group cipher suite with a pairwise cipher suite other than GCMP is not supported.

The cipher suite selector 00-0F-AC:0 (Use group cipher suite) is only valid as the pairwise cipher suite. An AP may specify the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites. If an AP specifies 00-0F-AC:0 (Use group cipher suite) as the pairwise cipher selection, this is the only pairwise cipher selection the AP advertises.

If any cipher suite other than TKIP, WEP-104, or WEP-40 is enabled, then the AP supports pairwise keys, and thus the cipher suite selector 00-0F-AC:0 (Use group cipher suite) is not a valid option.

***Instruct the editor to remove all modifications made to section 11 from the draft:***

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