IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Some Security Comments from LB193 |
| Date: 2013-04-22 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This document proposes resolutions to CIDs 1075 and 1552

***Instruct the editor to modify section 11.10.2 as indicated:***

### 11.10.2 AP PeerKey protocol

The PMK shall be derived using the key derivation function (KDF) from 11.6.1.7.2 (Key derivation function (KDF)) using Equation (11-4):

PMK = KDF-256(*keyseed*, “AP Peerkey Protocol”,

 0x00 || Max(LOCAL-MAC, PEER-MAC) || Min (LOCAL-MAC, PEER-MAC)) (11-4)

where

0x00 is a single octet with a value of zero

LOCAL-MAC is the AP’s BSSID

PEER-MAC is the peer AP’s BSSID

The Max and Min operations for IEEE 802 addresses are with the address converted to a positive integer treating the first octet as the most significant octet of the integer. Keyseed shall be irretrievabley destroyed after the PMK is generated.

***Instruct the editor to modify figures 11-42, 11-44, 11-46, 12-14, and 12-17 as indicated:***

***In figure 11-42 change EAPOL() to EAPOL-Key() in the following boxes: SMKNEGOTIATING1, SMKNEGOTIATING2, STKSTART, STKCALCNEGOTIATING2, STKCALCNEGOTIATING3, and STKCALCNEGOTIATING4.***

***In figure 11-44 change EAPOL() to EAPOL-Key() in the following boxes: PTKSTART, and PTKINITNEGOTIATING.***

***In figure 11-46 change EAPOL() to EAPOL-Key() in the following box: REKENEGOTIATING.***

***In figure 12-14 change EAPOL() to EAPOL-Key() in the following boxes: FT-PTK-START, and FT-PTK-CALC-NEGOTIATING3.***

***In figure 12-17 change EAPOL() to EAPOL-Key() in the following boxes: FT-PTK-START and FT-PTK-CALC-NEGOTIATING3.***

**References:**