IEEE P802.11
Wireless LANs

|  |
| --- |
| CID 7551, 7552 and 7606 |
| Date: 2016-02-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 1322 Crossman avenue, Sunnyvale, California, United States of America | 408 555 1212 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission proposes a resolution to CID 7551, 7552 and 7606

CID 7551 has a comment “What is an ‘MTKSA’? The term appears in Subclause 12.6 twice, but not in Clause 3, nor is it defined/described in Subclause 12.5.1.1” with a proposed resolution of “Change both instances to ‘mesh TKSA’ or ‘mesh PTKSA’ (depending on resolution to other comment), with the right case. Also delete "pairwise" before the second.”

CID 7552 has a comment “What is an ‘MTKSA’? The term appears in Subclause 12.8 twice but not in Clause 3, nor is it defined/described in Subclause 12.5.1.1” with a proposed resolution of “Change both instances to ‘mesh TKSA’ or ‘mesh PTKSA’ (depending on resolution to other comment), with the right case. Also delete ‘pairwise’ before the second.”

CID 7606 has a comment “What is an ‘MGTKSA’? The term in not in Clause 3, nor is it defined/described in Subclause 12.5.1.1” with a proposed resolution of “Change to ‘mesh GTKSA’, with the right case.”

Discussion: “other comment” is undefined. Change to “mesh TKSA” and “MGTKSA” to “mesh GTKSA”. Nothing wrong with “pairwise”.

Resolution: incorporate changes to document 11-16/0281

***Instruct the editor to modify section 12.6.1.1.9 as indicated:***

**12.6.1.1.9 IGTKSA**

When management frame protection is enabled, a non-AP STA’s SME creates an IGTKSA when it receives a valid Message 3 of the 4-way handshake or FT 4-way handshake, the Reassociation Response message of the fast BSS transition protocol with a status code indicating success, a Mesh Peering Open Message of the Authenticated Mesh Peering Exchange (AMPE) protocol, or a valid Message 1 of the group key handshake. The Authenticator’s SME creates an IGTKSA when it establishes or changes the IGTK with all STAs to which it has a valid PTKSA or mesh TKSA.

***Instruct the editor to modify section 12.6.7 as indicated:***

**12.6.7 RSNA policy selection in an MBSS**

All mesh STAs in an MBSS use the same group cipher suite. Mesh STAs establish authenticated peerings with each other using the AMPE protocol (see 14.5 (Authenticated mesh peering exchange (AMPE))). In AMPE, mesh STAs negotiate a pairwise cipher suite, and establish a pairwise mesh TKSA, to protect individually addressed frames and state a group cipher suite and establish a mesh GTKSA to process incoming group addressed frames from a peer.

**References:**