IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed resolution to CID2199 | | | | |
| Date: 2014-02-15 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Carlos Cordeiro | Intel |  |  | [Carlos.Cordeiro@intel.com](mailto:Carlos.Cordeiro@intel.com) |

Abstract

This submission proposes a resolution to CID2199 submitted on 11ad text.

The discussion is in reference to Draft P802.11REVmc\_D2.0.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2199 | 1411.32 | 10.3.4.1 | Section 10.3.4.1 states that DMG STAs do not support authentication and deauthentication. This appears to be an optimisation that should only apply to cases where the Open Authentication algorithm is used, otherwise 11ad STAs cannot make use of other authentication algorithms such as SAE, Fast BSS Transition and those in 11ai. Even when Open Authentication is in use I'm not sure how multi-band operation is affected by this restriction. | Restrict this optimisation to cases where the Open Authentication algorithm is in use. This will require also changes in other parts of the draft, such as Figure 10-12 which shows authentication and association states. |

**Discussion:** TGm held a discussion on possible resolutions to this CID back at the Jan/14 meeting. See <https://mentor.ieee.org/802.11/dcn/14/11-14-0030-02-000m-discussion-on-cid2199.pptx>. The preferred resolution was resolution 1, which allows the use of Authentication frames when the Open System Authentication algorithm is not in use.

**Proposed resolution**: Revised

**10.3.1 State variables**

*Change the fourth and fifth paragraphs as follows*

For nonmesh STAs, this state variable expresses the relationship between the local STA and the remote STA. It takes on the following values:

— State 1: Initial start state for non-DMG STAs and for DMG STAs performing 802.11 Authentication. Unauthenticated, unassociated. ~~State 1 is not used by DMG STAs.~~

— State 2: Initial start state for DMG STAs that do not perform 802.11 Authentication. Authenticated (DMG STAs that performed 802.11 Authentication and non-DMG STAs ~~only~~), not associated.

— State 3: Authenticated (DMG STAs that performed 802.11 Authentication and non-DMG STAs ~~only~~) and associated (Pending RSN Authentication).

— State 4: For Infrastructure BSS and PBSS only, RSNA Established or Not Required.

~~State 1 is not used by DMG STAs, and the state machine starts in State 2.~~

**10.3.2 State transition diagram for nonmesh STAs**

*Replace Figure 10-12 with the following*



**10.3.4.1 General**

*Change the last paragraph as follows*

Authentication is optional in a non-DMG IBSS. In a non-DMG infrastructure BSS, authentication is required. APs do not initiate authentication. A DMG STA performs authentication when the authentication algorithm used by the STA is not Open System authentication and does not perform authentication otherwise (see 11.2.3.1). ~~Authentication and deauthentication are not supported by DMG STAs~~.

**11.2.3.1 Overview**

*Change the first paragraph as follows*

In an ESS, a non-DMG STA and a~~n~~ non-DMG AP both complete an IEEE Std 802.11 authentication exchange prior to association. Such an exchange is optional in an independent BSS network. In DMG, a STA shall complete an IEEE Std 802.11 authentication exchange with an AP prior to association if the authentication algorithm used by the STA is not Open System authentication; otherwise, the STA shall not perform an IEEE Std 802.11 authentication exchange.

**11.2.3.2 Open System authentication**

**11.2.3.2.1 General**

*Change the first paragraph as follows*

Open System authentication is a null authentication algorithm. Any non-DMG STA requesting Open System authentication may be authenticated if dot11AuthenticationAlgorithm at the recipient non-DMG STA is Open System authentication. A STA may decline to authenticate with another requesting STA. Open System authentication is the default authentication algorithm for pre-RSNA equipment.