IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution for some LB 255 CRs |
| Date: September 10 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | nehru.bhandaru@broadcom.com |

Abstract

This document contains proposed resolutions for following CID 6028 against TGaz Draft 4.0 from LB 255

The baseline documents for changes in this document are TGaz Draft 4.0 and Draft P802.11REVme D0.2 The text in red are the instructions to the editor.

| CID | PageClause | Comment | Proposed Change | Resolution |
| --- | --- | --- | --- | --- |
| 6028 | 113.3111.3.4  | Follow-up to CID 5361. The draft now states "PASN authentication is disallowed in states other than State 1." However, a DMG STA that does not perform IEEE Std 802.11 authentication will initiate in State 2 (and thus, will never be in State 1). So, such a STA can never do PASN authentication. | Correct the statement at the cited location. Add transition(s) for a DMG STA that does not perform IEEE 802.11 authentication to transition from State 2 to a PASN Authenticated state, and then directly to State 3 through (Re)Association. (And, add text in 12.12 to describe the PBSS/PCP case.) Or, clarify in the text that a DMG STA that does not perform IEEE 802.11 authentication also shall not perform PASN authentication. | Resolution: Reject It is already stated in TGaz D4.0 § 4.5.4.2 that PASN is one of the six IEEE 802.11 std authentication methods, and thus, clearly, DMG STAs that do not perform IEEE 802.11 authentication \*cannot\* perform PASN authentication. |

**CID 6028**

**Comment:**

Follow-up to CID 5361. The draft now states "PASN authentication is disallowed in states other than State 1." However, a DMG STA that does not perform IEEE Std 802.11 authentication will initiate in State 2 (and thus, will never be in State 1). So, such a STA can never do PASN authentication.

**Discussion:**

In 11az D4.0, PASN was never intended to be used by DMG STAs that did not perform IEEE Std 802.11 authentication. It was this way since the introduction of PASN in TGaz D1.1.

Change to support PASN from State 2 for DMG STAs that did not perform Std 802.11 authentication would be a new feature.

If PASN is desired, DMG STAs should perform PASN from State 1.

The changes are probably not going to be simple to support this feature.

Best course of action seems to be not to add the new feature.

As to clarifying in the text that “a DMG STA that does not perform IEEE 802.11 authentication also shall not perform PASN authentication”, it is already stated in TGaz 4.0 draft that PASN is one of the six IEEE 802.11 std authentication methods, and thus, clearly, DMG STAs that do not perform IEEE 802.11 authentication \*cannot\* perform PASN authentication.

Note also that the commentor, in the comment, states that ..such STAs cannot perform PASN and seems to express a desire to support it – implying that the commentor understood that they cannot perform… and thus no further clarification seems needed.

It is already stated in TGaz D4.0 that

 “

**4.5.4.2 Authentication**

Change the following paragraphs as shown:

IEEE Std 802.11-2020 defines six IEEE 802.11 authentication methods: Open System authentication, Shared Key authentication, FT authentication, (IEEE Std 802.11-2020) simultaneous authentication of equals (SAE), FILS authentication (IEEE Std 802.11-2020) and preassociation security negotiation (PASN) authentication.

“

Additional clarity does not seem to be needed and thus I recommend rejecting this comment.