IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Resolution for some LB249 CRs | | | | |
| Date: March 09, 2020 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |

Abstract

This document contains proposed resolutions for following CIDs against TGaz Draft 2.0 from LB249:

3517, 3514, 3515, 3522, 3406, 3519, 3407, 3408, ~~3524~~, ~~3525~~, ~~3526~~, 3536, 3409, 3414, 3833, 3448, 3521, ~~3880~~

The baseline documents for changes in this document are TGaz Draft 2.0 and Draft P802.11REVmd D3.0. The text in red are the instructions to the editor.

| CID | Page | Clause | Comment | Proposed Change | Resolution |
| --- | --- | --- | --- | --- | --- |
| 3517 | 103.12 | 11.3.2 | There are references to "Robust Unicast Class 2 Frames" but these are not defined. Ditto "protected Class 2 frames" in 11.3.4 | As it says in the comment | Revise  Add definition of protected Class 2 frames and replace text in figure.  TGaz Editor: Make changes as specified in this document – 11-20/0255r1 |
| 3514 | 104.27 | 11.3.3 | "If STA A in an infrastructure BSS receives a Class 2 or Class 3 frame from STA B when in State 27 1 that is not authenticated with STA A" makes no sense: a state is not authenticated with a STA | Revert the changes to this para | Revise.  This change was made to allow for protected Class 2 frames in State 1a. Perhaps it can be clearer.  TGaz Editor: Make changes as specified in this document – 11-20/0255r1 |
| 3515 | 104.33 | 11.3.3 | "PASN Authenticated State 1a" -- no such state | Delete "PASN Authenticated " | Accept.  TGaz Editor: Make change as indicated in the comment – 104.33 – shown below  when in ~~PASN Authenticated~~ State 1a, STA A shall discard the frame |
| 3522 | 104.7 | 11.3.3 | "A STA shall not transmit Class 2 frames unless in State 1a or State 2 or State 3 or State 4. " -- in State 1a only "Robust Unicast Class 2 Frames" / "protected Class 2 frames" are allowed, per other text | As it says in the comment | Revise.  This could be clarified in the text.  TGaz Editor: make changes to 11.3.3 p104.7 as below  A STA shall not transmit Class 2 frames unless in ~~State 1a or~~ State 2 or State 3 or State 4. In State 1a, A STA shall not transmit Class 2 frames other than Unicast Protected Dual of Public Action frames. |
| 3406 | 105.25 | 11.3.4.3 | The modification made to Authentication - destination STA, are confusing. It would be simpler to leave the exiting text as is and add a paragraph which provides what happens when the MLME-AUTHENTICATE.response primitive with a ResultCode of Success received. | Modify the paragraph as follows: "g) If the Authentication frame was constructed using the procedures in 12.3.3.2 18 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5 (FT protocol), or 13.6 19 (FT resource request protocol), upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is SUCCESS, the MLME shall transmit an Authentication frame that is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5 (FT protocol) or 13.6 (FT resource request protocol), with a status code of SUCCESS, and the state for the originating STA shall be set to State 2 if it was in State 1(#1403); the state shall remain unchanged if it was other than State 1. Else if the Authentication frame was constructed using the procedures in 12.13 (Preassociation Security Negotiation), upon receipt of a MLME-AUTHENTICATE.response primitive, if the ResultCode is SUCCESS, the MLME shall transmit an Authentication frame that is constructed using the procedure in 12.13 (Pre-association Security Negotiation) with a status code of SUCCESS. The state for the originating STA shall be set to State 1a if it was in State 1; the state shall remain unchanged if it was other than State 1. Note: PASN authentication is disallowed in states other than State 1. | Revise.  The current text is concise and accurate. Don’t see a need to separate out PASN from other protocols. However 11az D2.0 seems to have an error that may have caused the confusion - see below  TGaz Editor: make change to 11.3.4.3 p105.27  The state for the originating STA shall be set to State 2 if it was in State 1 (#**1403**) ~~or State 1a~~ when PASN authentication procedure was not used. The state for the originating STA shall be set to State 1a if it was in State 1 and PASN authentication procedure was used~~;~~ . Note: PASN authentication is disallowed in states other than State 1. |
| 3519 | 105.3 | 11.3.4.2 | "PASN authentication is disallowed in states other than State 1" is vague | Change to "the state shall remain unchanged if it was other than State 1". In 11.3.4.3 change "PASN authentication is disallowed in states other than State 1" to "the state shall remain unchanged if it was other than State 1" | Revise.  The current text is more useful in that it states PASN authentication is disallowed in states other than State 1. Replacement as suggested by the commentor seems to imply that PASN is allowed in other states and they will remain unchanged after PASN procedure. A different semantics.  It might be clearer to have a shall statement as opposed to the current test.  TGaz Editor: Change the sentence to the following  “PASN authentication shall be disallowed in states other than State 1.” |
| 3407 | 106.26 | 11.3.5 | Changing the specification so that disassociation is not allowed in State 1 is a change to the base line specification, and should not be made. Disassociation should be allowed independent of what the State of the STA is. | Delete: "Disassociation is not allowed in State 1 or State 1a." Do not delete: "when not in State 1" in two places. Add a statement as to what the behavior of a STA in State 1a would be if it received a disassociation request. | Revise.  Agree with the commentor. Not sure how this got into the draft, but we are not changing the baseline behavior in State 1.  TGaz Editor replace 106.26 text as follows  “  Disassociation is not allowed in State 1 or State 1a.  Disassociation notification ~~when not in State 1~~ sets a non-FILS(11ai) STA’s state to State 2. Disassociation notification ~~when not in State 1~~ sets a FILS STA’s state to State 1(11ai).”  with  “Disassociation is not allowed in State 1a. Disassociation notification when not in State 1 or State 1a sets a non-FILS(11ai) STA’s state to State 2. Disassociation  notification when not in State 1 or State 1a sets a FILS STA’s state to State 1(11ai).” |
| 3408 | 106.40 | 11.3.5.3 | Why is State 1a include in the AP or PCP SME refusal of a not-authenticated STA. Isn't a State 1a STA authenticated? | Either remove the State 1a STA from this response, or provide an explanation. | Revise.  Agree with the commentor. In State 1a, a STA is authenticated. Propose to reject association in State 1a with a REFUSED reason code.  TGaz Editor: Replace text in az Draft as follows  “b) If the state for the STA is State 1 or State 1a and the STA is a non-DMG STA, the SME shall refuse the association request by issuing an MLME-ASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.”  With  “  b) If the state for the STA is State 1 and the STA is a non-DMG STA, the SME shall refuse the association request by issuing an MLME-ASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.  If the state for the STA is State 1a and the STA is a non-DMG STA, the SME shall refuse the association request by issuing an MLME-ASSOCIATE.response primitive with ResultCode REFUSED.” |
| 3524 | 106.7 | 11.3.5 | "In order to associate or reassociate, a 7 STA in State 1a must perform a IEEE Standard 802.11 non-PASN authentication or FILS 8 authentication and transition to State 2." is already covered by the previous sentence | Delete the cited text | Take this offline and bring it back  The section is about association/reassociation which is allowed only in state 2. There is no need to talk about what happens in State 1a – like other states are not talked about in this section. |
| 3525 | 106.7 | 11.3.5 | "Association and reassociation are allowed only in State 2." -- not true. You can reassociate to the same AP, in which case you'll be in State 3 or 4 | Delete the cited text | Take this offline and revisit  TGaz Editor – Change p106.7 in az Draft as follows.  ~~Association and reassociation are allowed only in State 2.~~ In order to associate or reassociate, a STA in State 1a must perform a IEEE Standard 802.11 non-PASN authentication or FILS authentication and transition to State 2. |
| 3526 | 106.27 | 11.3.5 | "Disassociation notification \*when not in State 1\* sets a non-FILS(11ai) STA's state to State 2. " -- the stuff between asterisks should not be deleted, because if for whatever reason (e.g. confusion by peer as to the current state) a STA is sent a Disassociate frame in State 1 it should not consider itself promoted to State 2 | Do not delete the stuff between asterisks | Take this offline  Addressed by resolution to comment 3407.  No additional changes needed. |
| 3536 | 108.14 | 11.13 | I'm not sure this is correct (though SA queries always get me extremely confused). This means an SA query will be sent if a PTKSA was established with PASN, but per earlier 11.3 text any association should have gone via non-PASN authentication, so there is no situation where we could be associated but have a PASN-based PTKSA (which is when SA queries are used, per 11.3.5.3/5) | Revert the changes to this para | Revise.  SA query is used to determine if there is a PTKSA security association. The intent is to have this be available in State 1a. Since SA Query is a robust management frame (Table 9-53), we need to declare it as a class 2 frame in 11.3.3 (Frame filtering based on STA state)  TGaz Editor: Change the modification p104.16 as follows  iv) Unicast SA Query (11.13) and Protected Dual of Public Action frames (9.6.10) when PTKSA from PASN authentication exists. |
| 3409 | 176.34 | 12.2.4 | The wording of the paragraph g) seems to be inconsistent with the rest of 12.2.4. Suggest, aligning the phrasing to be more consistent. | Replace: "g) If an RSNA uses PASN authentication, an RSNA capable STA's SME establishes an RSNA as described in 12.13 (Pre-Association Security Negotiation)" With: "g) When an RSNA capable STA uses PASN authentication, the STA's SME establishes an RSNA as described in 12.13 (Pre-Association Security Negotiation)" | Accept.  TGaz Editor: Please make the suggesged change. |
| 3414 | 177.2 | 12.2.4 | P802.11az seems to claim that SAE and FILS cannot be used within an RSNA. That is incorrect. | Remove the change to the last paragraph, i.e., delete this added text from the draft: "Only Authentication frames with the authentication algorithm equal to Open System authentication, FT authentication, or PASN authentication may be used within an RSNA." | Revise.  Agree with the commentor. Perhaps it needs to say something useful about just PASN instead.  TGaz Editor change p177.2 as follows  “Only Authentication frames with the authentication algorithm equal to Open System authentication, FT authentication, or PASN authentication may be used within an RSNA. An RSNA STA shall not associate if Shared Key authentication was invoked prior to RSN association.”  Replace with  “An RSNA STA shall not associate if Shared Key authentication was invoked prior to RSN association. PASN Authentication may be used within an RSNA. However, an RSNA STA shall only allow association if authentication other than PASN was invoked prior to RSN association” |
| 3833 | 191.14 | 12.13.5 | "The AP sets the Wrapped Data in the second PASN frame, as shown in the figure below, to be the 14 concatenation of " -- this is self-referential duplication! | Change "The AP sets the Wrapped Data in the second PASN frame, as shown in the figure below, to be the 14 concatenation of [...] Second Authentication frame body with a Confirm message. " to just "The AP sets the Wrapped Data in the second PASN frame, as shown in Figure 12-54b." | Reject.  The text provides some additional information about the contents of the authentication frame body that can be used to correlate with the SAE protocol – Commit/Confirm… |
| 3448 | 24.11 | 6.3.5.2.2 | There is no PASN authentication frame. There are only Authentication frames that are carrying PASN parameters or element(s). REVmd has a comment to address the similar issues with FILS and SAE. (Their CID is #4787.) Follow the direction of REVmd, and do the same thing for the phraseology "PASN authentication frame" throughout the TGaz draft. | As in comment, follow the direction of REVmd. | Reject.  In 11md D3.0, there are other names ‘Content of FILS Authentication… , Content of SAE…” etc. Content of PASN authentication frame name is explained in the table below the primitive just like the others. So it seems consistent. |
| 3521 | 24.3 | 6.3.5 | The AuthenticationType parameter of the MLME-AUTHENTICATE primitives needs to be extended to allow for PASN authentication | As it says in the comment | Revise.  Agree. In addition to the content row, Authentication Type needs to be extended with PASN in MLME-Authentication tables  TGaz Editor change the Valid range column, Authentication Type row in tables for the authentication primitives as specified in 11-20/0255r1 |
| 3880 |  | 12.7.1.3 | Tgba Draft 5.0 - also extends the key hierarchies - Pairwise (12.7.1.3), FT (12.7.1.6), FILS (12.12.2) to derive key material for use as WTK (WUR Transient Key). Tgaz 2.0 draft also extends the same key hierachies and must reconcile with changes forthcming in TGba. | Either Tgba uses HLTK based derivation for WUR key or Tgaz needs to modify the derivation to take into account the bits, if any, required for WUR operation. | TBD |

**CID 3517**

Comment:

“There are references to "Robust Unicast Class 2 Frames" but these are not defined. Ditto "protected Class 2 frames" in 11.3.4”

Discussion:

These are currently only unicast protected dual of public action frames – as defined in 11.3.3 frame filtering based on STA state. Agree - it might be better to clarify this terminology.

TGaz Editor: Change Figure 11-16 (note: this is a replacement figure for 11-17 in rev md 3.0) state 1A descrption as follows:

Change “Robust Unicast Class 2 Frames” to “protected Class 2 frames”

Replace p104.17 definition in Class 2 frames iv) as follows

iv) Protected Class 2 frames comprising Unicast Protected Dual of Public Action frames (9.6.10) when PTKSA from PASN authentication exists.

**CID 3514**

Comment: p104.27

"If STA A in an infrastructure BSS receives a Class 2 or Class 3 frame from STA B when in State

1 that is not authenticated with STA A" makes no sense: a state is not authenticated with a STA”

Discussion:

TGaz Editor: Update the change to 11md D3.0 as follows (replacing the corresponding change in 11az)

If STA A in an infrastructure BSS receives a Class 2 or Class 3 frame from STA B that is not authenticated with STA A (i.e., the state for STA B is State 1), STA A shall discard the frame.

If STA A in an infrastructure BSS receives an unprotected Class 2 frame or a Class 3 frame from STA B when the state for STA B is State 1a, STA A shall discard the frame.

**CID 3521**

TGaz Editor, add in TGaz Draft before each of the the current ‘Insert a new row in the following unnumbered table:’ instructions in sections 6.3.5.3.2, 6.3.5.4.2, 6.3.5.5.2 the following

Change the ‘Valid range’ column for the ‘Authentication Type’ row in the following unnumbered table by appending PASN as follows

OPEN\_SYSTEM,

SHARED\_KEY,

FAST\_BSS\_TRANSITION,

SAE, FILS\_SHARED\_KEY

WITHOUT\_PFS,

FILS\_SHARED

KEY\_WITH\_PFS,

FILS\_PUBLIC\_KEY,

PASN