IEEE P802.11
Wireless LANs

|  |
| --- |
| Cleanup of more comment resolutions for LB201 |
| Date: 2014-09-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Ping FANG | Huawei Technologies | Vision Business Park, Nanshan, Shenzhen, China | 0086 755 36835832 | Ping.fang@huawei.com |

Abstract

When apply the change from database, editors found more editorial comment resolutions need to be cleaned up.

This submission suggest actions to sovle the issues with 4374, 4337, 4302, 4383, 4269, 4261, 4263, 4183, 4187, 5201, 4938, 4940, 4946, 4603, 4696, 5138, 4075, 4022, and 4275.

R1 includes resolution to open CID4274 and updates based on offline discussion with Mark Rison.

R2 keeps track of the changes from R1 in tracking mode as edited on screen.

R3 is a clean version of R2 with all the changes accepted.

*Note:*

*Action line proposes the cleanup solution to the corresponding CID resolution.*

*CIDs in red are considered to be non editorial.*

CID **4374**

Comment is:

There are some grammar errors in sentence "In Beacon and Probe Response and FD frames, a FILS indication element is included by an AP with dot11FILSActivated value of true. FILS indication element indicates properties of the FILS authentication protocol used and also indicates if concurrent IP address assignment is performed by the AP. The IP address type is also indicated." For example, the first "and" should be "," and "a FILS indication element" should be "a FILS Indication element".

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for CID 4374 to:

Revised ,

change the paragraph to “When dot11FILSActivated is true, an AP shall include a FILS Indication element in Beacon and Probe Response frames, and may include a FILS Indication element in FILS Discovery frames. The FILS Indication element indicates properties of the FILS authentication protocol used, whether AP performs IP address assignment, and the IP address type.”

CID **4337**

CID : AES-CCM-128 and AES-CCM-256 are not defined

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4337 to

Revised, add to the end of “AES-CCM-128 is used if the AKM is 00:0F-AC-<ANA-1> and AES-CCM-256 is used if the AKM is 00-0F-AC-<ANA-2>.” a new sentence “ AES-GCM-X (in Table 8-113) is GCM with X-bit AES key”. Note to Editor, the sentence “AES-CCM-128 is used if the AKM is 00:0F-AC-<ANA-1> and AES-CCM-256 is used if the AKM is 00-0F-AC-<ANA-2>.” was replaced earlier to “AES-GCM-128 is used if the AKM is 00:0F-AC-<ANA-1> and AES-GCM-256 is used if the AKM is 00-0F-AC-<ANA-2>.”

CID **4302**

CID: Move sentence "The STA shall respond to ..." to before line 29 of page 78 as it applies to all STAs.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4302 to

Revised, the whole paragraph has been rewritten by 14/0765r7.

CID **4383**

CID: There are grammar errors in sentence "If the STA chooses to initiate FILS shared key authentication, the STA first chooses a random 16 octet nonce. It then determines whether to attempt PMKSA caching. If so, it generates a list of one or more PMKSA identifiers, otherwise it constructs an EAP-Initiate/Re-auth packet as specified in IETF RFC6696, with the following additional clarification:" For example, "the STA" shall be "a STA". please correct.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4383 to

Revised, change the text to “If a STA chooses to initiate FILS shared key authentication, it shall first choose a random 16 octet nonce and then determine whether to attempt PMKSA caching. If PMKSA caching is attempted, it shall generate a list of PMKSA identifiers. Otherwise, it shall construct an EAP-Initiate/Re-auth packet as specified in IETF RFC6696, with the following additional clarification:”

CID **4269**

CID: Incorrect reference to TLV

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4269 to

Revised, change “IP Address Request TLV” to “FILS IP Address Assignment element”.

CID **4261**

CID: Incorrect section reference

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4261to

Revised, remove “in 8.5.8.35”.

CID **4263**

CID: Incorrect section reference

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4263 to

Revised, change “Table 8-43 (Category values)” to “Table 8-54(Category values)”.

CID **4183**

CID: This text needs proofreading: "including FILS", "request IP address", "by sending FILS IP", "Assignementelement",

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4183 to

Accepted

CID **4187**

CID: "when using" is vague about what is the subject doing the using.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4187 to

Accepted

CID **5201**

CID: Incorrect reference.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 5201 to

Revised, “Change " Figure 8-399(Access Network Options field format)." to " Figure 8-435 (Access Network Options field format)”

CID **4938**

CID: Line 35 - the purposes of 4-way handshake are as follows... - that would be better as the purpose of key confirmation are as follows... where FILS authentication/association and 4-way handshakes both confirm the keys. It might also be worth calling out that the confirmation validates the identitity of peer. This is done by validating the PMK when a TTP is present, but via a digital signature - used in FILS non-TTP case.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4938 to

Rejected, the text commented on is from the baseline document. The commented text addresses non-FILS 4 way handshake and is therefore not changed by 11ai.

CID **4940**

CID: 11ac/11mcD2.6 adds KEK bits column to table 11-8. This should be updated to include FILS additions.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4940 to

Revised, update the Table 11-8—Integrity and key-wrap algorithms as in Revmc D3.0, and fill the two new columns “KCK bits” and “KEK bits” with 256 and 128 for row 1, 384and 256 for row 2.

CID **4946**

CID: line 9 - ...with whom it shares a cached PMKSA. Perhaps this should state that this is a PMKSA established via FILS (i.e. AKM in PKMSA is a FILS AKM). Also on line 19, page 107.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4946 to

Rejected, the task group doesn’t wish to limit PMKSA caching functionality in this manner.

CID **4603**

CID: Very long sentence.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4603 to

Rejected, the comment doesn’t provide specific change that can be applied in order to satisfy the comment

CID **4696**

CID: "If dot11FILSActivated equal".

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 4696 to

Revised, accept in principle, change "If dot11FILSActivated equal" to "If dot11FILSActivated is equal"

CID **5138**

CID: Why the sentence related to FILS Action frame is put in "higher layer setup during association procedure"? Suggest to move to somewhere else.

Issues: Resolution says “revised” but no change is provided.

Action: Change the resolution for 5138 to

Revised, move the sentence “FILS Action frame is protected as robust Action frame. (See 4.5.4.9 (Robust management frame protection)) and Table 8-43 (Category values)” to the end of line 60 page 69 of D2.0.

CID **4075**

CID: Overview and Step 1 and Step 2 are gratuitous and unhelpful. Make subclauses if necessary.

Issues: Resolution says “revised” but no change is provided.

Discussion: the level of subclause is 5, and no room to add new subclauses. We can make the title starting with “step…” bold

Action: Change the resolution for 4075 to

Revised, the level of subclause is 5 and no room to add new subclauses. Change the step title starting with “step…” bold.

CID **4022**

CID: "FD frames" -- no no no no no! We have 1) FD frame; 2) FD Discovery frame; 3) FILS Discovery frame.

Refering to the same structure using different terminology will inevitably result in torsional dislocation of foundation garments.

Action: Change the resolution for 4022 to

Revised, instruct editor to go through the draft and replace “FD frame” and “FD Discovery frame” with “FILS Discovery frame”.

CID **4275**

CID: Incorrect reference to section

Action: Change the resolution for 4275 to

Rejected, the reference is correct. D2.0 is based on Revmc D2.0, IEEE 802.11ac-2013, and IEEE 802.11af-2013, not based on 802.11-2012. The editor will continuously update reference to reflect the baseline changes.

CID **4274 (open CID)**

CID: Incorrect reference and missing table

Action: Accept the resolution for 4274 as

Revised, the type of IP address is provided in Table 8-221i in D2.1. Delete the sentence “For each domain, the type of IP address available is also indicated in 8.4.2.181 (FILS IP Address Assignment element).”

**References:**

14/0565r18 (D2.0 comments spreadsheet post-San Diego)