Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh teleconference Minutes, May 28, 2024Randomized and Changing MAC addresses (RCM) |
| Date: 2024-06-07 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jay Yang | ZTE |  |  | Yang.zhijie@zte.com.cn |
| Peter Yee | NSA-CSD/AKAYLA |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh teleconference of May 28, 2024.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting May 28th, 2024, 9:30 a.m. to 11:30 a.m. ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Jay Yang(ZTE), Peter Yee**

**Editor: Carol Ansley (Cox Communications)**

**The teleconference meeting was called to order by the Chair at 9:33 a.m. ET.**

Agenda slide deck [11-24/0962r01](https://mentor.ieee.org/802.11/dcn/24/11-24-0962-01-00bh-agenda-tgbh-2024-may-28.pptx)

1. **Policies and procedures were presented by Chair Mark Hamilton. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ Timeline reminder (slide 16)
	+ Motions record: 11-22/0651r45
	+ Reminder: Ad hoc (F2F/Hybrid), June 18-20: 11-24/0929r1
* **Comment Resolution, Initial SA ballot**
	+ Comment resolution document: [11-24/0883r4](https://mentor.ieee.org/802.11/dcn/24/11-24-0883-04-00bh-p802-11bh-initial-sa-comments.xlsx)
		- Updated; Color coding
	+ CID 3021: Withdrawn by commenter
	+ Editorial CIDs update: 11-24/0952r0 (Ansley)
	+ Comment review and resolution (slide 17)
1. **Comment Resolution queue**

<https://mentor.ieee.org/802.11/dcn/24/11-24-0789-03-00bh-cr-for-pasn-id.docm> (Li)

[https://mentor.ieee.org/802.11/dcn/24/](https://mentor.ieee.org/802.11/dcn/24/11-24-0916-02-00bh-cids-on-irm.docx)[11-24-0916-02-00bh-cids-on-irm.docx](https://mentor.ieee.org/802.11/dcn/24/11-24-0916-02-00bh-cids-on-irm.docx) (Smith)

<https://mentor.ieee.org/802.11/dcn/24/11-24-0893-00-00bh-cr-for-sa-comments-in-9-4-2.docx> (Yang)

<https://mentor.ieee.org/802.11/dcn/24/11-24-0895-00-00bh-cr-for-sa-comments-in-11-10-9.docx> (Yang)

<https://mentor.ieee.org/802.11/dcn/24/11-24-0884-00-00bh-p802-11bh-initial-sa-comments-personal-comments.xlsx> (Hamilton)

<https://mentor.ieee.org/802.11/dcn/24/11-24-0931-00-00bh-cids-3121-and-3122.docx> (de la Oliva)

<https://mentor.ieee.org/802.11/dcn/23/11-23-2148-01-00bh-probability-of-irm-duplicates.pptx> (Smith)

Bring back/for further discussion:

<https://mentor.ieee.org/802.11/dcn/24/11-24-0919-03-00bh-cr-on-activated-vs-supported.docx> (Stacey)

<https://mentor.ieee.org/802.11/dcn/24/11-24-0898-01-00bh-sa-cr-for-cid3131.docx> (Mutgan)

1. **SA Comments resolution in details**

Q: 24/904 including the resolution for CID3120--ready for motion

Q:CID3021 is withdrawn by the commenter ---ready for motion

1. **Yan Li (ZTE) presented [11-24-0789-03-00bh-cr-for-pasn-id.docm](https://mentor.ieee.org/802.11/dcn/24/11-24-0789-03-00bh-cr-for-pasn-id.docm)**

This includes the resolutions for CID3003, CID3015, and CID3194

C: My main comments are on the exact requirement for protection of device ID and PASN ID. You delete the note about device ID being opaque. In my opinion, the device ID being opaque is still valid. If you try to change the rule on device ID, I would like to have a clear understanding why the change should be done. I don’t think any change on PASN ID has impact on what we have on device ID. So, I disagree with that change. Regarding the propose of using opaque for PASN ID, I do like the last change you describe for the CID. That paragraph seems to imply the solution is that the access point does it completely than the station does. As the first PASN frame in the air includes a plain PASN ID, if the STA fails to compete the PASN authentication, the same PASN ID in plain text will be used multiple times. The document implies the procedure in annex AF is mandatory for PASN ID. I think that’s a valid question. I propose to delete the change for device ID. I’m not sure whether the group has a clear requirement for PASN ID.

C: The text implies the access point can send any plaintext in PASN frame one. I don’t think that’s a good idea. I would like to know why opaque ID is not used for PASN ID?

A: Device ID is only used in FILS authentication and 4-way HS, and it will always be encrypted.

C: Two completely independent questions, one is whether Device ID be opaque is erased in the text. The PASN ID should be opaque. Why does the proposal in the text not require PASN ID beopaque in? Or am I miss something?

 A: I think PASN ID being opaque or not is a big discussion.

C: With PASN ID always being opaque, it can change in PASN authentication every time. There is no problem if the first authentication is 4-way HS, then the STA can use opaque in the following PASN authentication. The problem is with the AP always sending PASN ID and device ID to every STA; what should the STA do if the STA never uses PASN ID? Should we force it to provide that one? Could we have a specified a status to say do not use the ID for PASN, which will keep it simple? PASN ID doesn’t have to be opaque, as it's changed every time.

C: I agree with the general idea. Define the PASN ID mapping to device ID. You propose another information element. I believe PASN ID uses the same element as Device ID, so there is no need to define a new element for PASN ID. *E.g.*, only one or the other of the PASN ID or Device ID field is to be used in different scenario.

A: I don’t have a strong preference to have a separate element or not.

C: PASN ID is just to map to or relevant to Device ID, so, just use one information element is efficient.

A: Generating PASN ID from Device ID is complicated. Add a new format is simpler.

C: Focus on Figure12-0b, for 4-way HS, i understand you follow the figure above. The non-AP STA should do an Authentication request before starting the 4-way HS.

C: There is no PASN ID2 and ID3 coming back from the third message of the 4-way HS in the figure. I’m confused by the figure and not sure of the intention. Is the Deauth there in each FTM session or not? There’s an FTM session with AP1, and then an association with AP2 for another FTM session.

A: Authentciation and association are ignored. And I will add it offline.

C: How do you illustrate the usage of PASN ID2?

A: The example of the usage of PASN ID2 is in the Figure12-0a.

C: I would clarify whether the first 4-way HS belongs to the first FTM session or not.

A: I need more consideration on this part.

C: I do know the Deauth is needed there, but I’m concerned on the timing of Deauth compared with the action with AP2. Maybe the Deauth can wait for the FTM session going on, so that the PASN1 is used in the same FTM session.

C: I’m struggling on the comments that the PASN ID is opaque.

C: I’m also struggling on the comments that if PASN fails, the PASN ID will be used many times. Even if it is opaque, the same block will still be used for many times. How to make it help in this scenario if it’s opaque? I’m not sure on the value of PASN ID being the opaque.

A: It was proposed that PASN is mandatory opaque, is it right? Maybe being opaque is not the only way to keep the PASN ID encrypted in some implementation. In the SPEC, Annex AF is optional, and non-normative.

A: Maybe PASN ID is just random, it doesn't matter whether it is encrypted.

C: The main concern on the requirement that the PASN ID is just random, is fine. It’s not mandatory to use the Annex AF design. I like it if it's random, but not opaque. Random is fine. Nowhere does it say the PASN ID generated is different.

C: I wonder why we are working on this as the current draft already has an RCM solution? We need to understand how the PASN ID is generated as it’s plain text over the air. The proposal may cause the implementation not to use RCM.

C: In Figure 12-0b, it's fine because PASN ID2 is never used. No need to generate PASN ID3 in the second 4-way HS. The AP shall provide a new PASN ID if the previous one is used.

 C: I'm not against if the AP provides a PASN ID3.

C: There are many comments. Either the PASN ID is opaque or random is fine.

A: The current draft says the AP provides a new PASN ID in each PASN authentication.

C: Where is that? I can’t find it. What’s the context, is it in the PASN procedure?

C: Random or opaque, both of them are based on requirements. Let’s see other comments on whether the PASN ID is mandatorily to random. I like changing to random. Let’s see if we agree on this.

C: How about the PASN ID in the 4-way HS? Is that covered with the same language?

A: The AP should provide a new PASN ID in the 4-way HS in my contribution.

C: OK, I believe the two places are consistent in saying the PASN ID is random or randomly changing.

C: In Figure 12-0b, the non-AP associates with AP1 and gets PASN ID1, and then uses PASN ID1 in the first FTM session on the right. Maybe add AP-3 to illustrate how to use PASN ID2 in Figure 12-0b?

A: The usage of PASN ID2 is enough in Figure 12-0a.

C: The example looks like the non-AP should associate with the ESS first. I believe PASN does not rely on the 4-way HS, so I hope the text clearly illustrates that PASN authentication may be ahead of association.

C: You want to add a new figure with PASN authentication first, and then a 4-way HS?

A: No, no need to add a new figure, but it should be clearly in the text.

C: There is a highlighted initial connection. Explain the initial connection, *e.g.*, may be PASN or 4-way HS to complete the initial connection, to address the concern.

A: I don’t want to add such sentence into the draft.

C: PASN ID should not be predictable. It could be opaque, but the opaque process output is too big. PASN ID could be very short, so just random is OK. The basic idea that it is just not predictiable

C: Random but not including PII, or both requirements. Define PASN ID better. The length is not less than 6 octets.

C: Maybe there is no need opaque ID at all.

C: From the editor’s perspective, please don’t do it here (subclause 9); it belongs to subclause 12. I would propose multiple ways to do it. PASN ID should be defined as a random value in subclause 12. If you imply a new PASN ID, it will apply such rules. That will be a simple way.

C: I don't think we should remove opaque from the draft. It's optional. I also don't think it's mandatory.

C: It's an open question. It's AP vendor-specific to adopt the opaque mechanism or not.

C: I don’t think PASN ID is restricted to the same ESS.

C: FTM can be done across ESSes, but PASN ID can't be shared among ESSes, so let’s be very carefully.

C: APs in the different ESSes sharing the PASN ID, may cause security concerns.

C: Add a statement somewhere that says that "Device ID, IRM, PASN ID, and measurement shall not be shared across ESSes".

C: Device ID and IRM are definitely in the same ESS, saved in the same local profile.

C: For quality location measurement and other support of FTM, I understand the privacy concern.

C: A given AP is only in one ESS; this is an IEEE group.

C: Using PASN ID in the same ESS not much of a constraint. We do this in the same ESS.

C: PASN use in an ESS is different. The PMK generated in the PASN is absolutely not the PMK shared across the ESS.

C: The PASN ID is limited to the single ESS. If someone strongly feels it should be shared like the PMK, we should understand the use case.

C: Joe Levy, if you want to try to get use case ideas, you may consult to 11bk group via the reflector.

1. **Graham Smith (SRT Wireless) presented [11-24-0916-02-00bh-cids-on-irm.docx](https://mentor.ieee.org/802.11/dcn/24/11-24-0916-02-00bh-cids-on-irm.docx)**

CID3197 is covered in this presentation.

C: The commenter proposes to change "may" to "shall".

C: Could you show the context again? I’m not sure how “may” or “shall” fits in here.

A: I like the idea; also, change "may proceed" to "proceeds"

C: 36.10, take it out.

C: 39.12, using "may", it looks good to me.

C: It's OK to use "may" (in 39.12).

C: For 39.17, shall we change "AP may set" to "AP sets"? we could say “AP sets”,

C: We should keep consistency with the first two sentences.

C: We should look at the first sentence.

C: You should be OK to do this?

A: Yes, I’m OK on this.

C: Could I see the change proposed in, CID3197? I think that one is fine.

C: In the first sentence, change "is set to" to "shall be set to "

C: How about the second sentence?

A: The second is OK for me.

C: I wonder whether the second one and last sentence are duplicated.

C: Give me the direction to change that.

A: Make the first two sentences to be normative and merge the duplicated sentence. I see the second and last sentence may slightly different. Please double check that when you delete the last sentence.

A: I will do it offline.

------------------CID deferred----------

CID3057

C: I suggest replacing the “throughout” to "to" in the proposed change.

A: OK, I will change it to "distribute IRMs to the APs in the ESS" in the resolution.

------------------no objection ----------

**Meeting adjourned at 11:30 a.m. ET.**