Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, April 18, 2023Randomized and Changing MAC addresses (RCM) |
| Date: 2023-04-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of April 18, 2023.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting April 11, 2023 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: Peter Yee**

**Editor: Carol Ansley (Cox)**

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

Agenda slide deck [11-23/0653r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0653-01-00bh-agenda-tgbh-2023-april-18.pptx)

1. **Policies and procedures were presented by the chair. (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 reminders**
* **Policies, duty to inform, participation rules**
* **Organization topics (see Backup slides)**
	+ Timeline reminder (slide 20)
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r23**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-23-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record:** [**11-22/0651r16**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-16-00bh-tgbh-motions-list.pptx)
* **Motion 16 (slide 28 of motions record deck)**
	+ Consider: [11-23/0129r6](https://mentor.ieee.org/802.11/dcn/23/11-23-0129-06-00bh-irm-proposed-text.docx)
* **Discuss timing for D0.3**
* **Review D0.2 CC comments and status, plan for between now and May**
* **Discuss Contributions (next slide)**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Timing**

We are targeting a WG letter ballot coming out of the May meeting and all efforts are directed to achieving that. We don’t currently have a either D0.3 or a D1.0, so we need to converge quickly if the letter ballot is going to happen following the May meeting. The motion we will run today will have a major impact on how close we get. If the motion passes, there will be only 3 CIDs remaining to resolve.

1. **Proposed Text for IRM**

Based on mailing list discussion, Graham Smith has updated his proposed text for IRM in [11-23/0129r06](https://mentor.ieee.org/802.11/dcn/23/11-23-0129-06-00bh-irm-proposed-text.docx). A note has been added that indicates when the IRM MAC address is to be used and when it is to be changed.

Q: What’s the meaning of a zero-length device ID? Can we add clarification a note of when/how it is used? [in new subclause 12.2.11.1]

A: Maybe it indicates that the same device ID is in use.

C: We need to indicate that it is the current ID that is being maintained.

Smith reposted the document with the changes as [11-23/0129r07](https://mentor.ieee.org/802.11/dcn/23/11-23-0129-07-00bh-irm-proposed-text.docx). Hamilton posted the updated [11-22/0973r24](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-23-00bh-cc41-comments-against-d0-2.xlsx) (comment collection resolutions) to match.

1. **Motion 16 (from** [**11-22/0651r16**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-16-00bh-tgbh-motions-list.pptx)**)**

The motion reads: ‘Move to approve the resolutions of CC41 comments, and incorporate the text changes into the P802.11bh draft, as indicated in [11-22/0973r24](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-24-00bh-cc41-comments-against-d0-2.xlsx) for CIDs marked “Ready for motion”:

CIDs 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 17, 24, 25, 26, 27, 30, 31, 32, 33, 36, 40, 41, 42, 45, 47, 49, 50, 51, 52, 53, 58, 61, 62, 63, 64, 65’

Moved: Kurt Lumbatis

Seconded: Joseph Levy

Result: Approved by unanimous consent

Q: This leaves 3 CIDs remaining to resolve. Should we work on those or ask the editor to create a new draft. There have been comments from some people that it would be good to see an updated draft so they can understand what the state of the document is.

A: I think we should go for an D0.3, but it would be helpful to continue work too.

C: Let’s discuss the remaining CIDs and ask Carol to produce a new draft based on where we end up.

1. **Review D0.2 CC comments and status, plan for between now and May**

Hamilton showed that CIDs 19, 20, and 35 remain outstanding. An updated contribution on the first two will be discussed. CID 35 needs a little more discussion as well. We will either proceed without updates for those CIDs or reach consensus for them prior to the May meeting so that we can have a Draft 1.0 coming out of that meeting.

1. **Contributions on CIDs 19 and 20 [related to PASN]**

Okan Mutgan (Nokia) presented [11-22/1732r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-02-00bh-resolution-for-cid19-and-cid20.pptx), clarifying the discussions from last week. It has two proposals. Device ID is either exchanged in PASN Authentication message 2 and Authentication message 3 or it is exchanged in PASN Authentication message 1 and Authentication message 2. The second option allows for a suboption of using an opaque ID instead of a plaintext device ID. The opaque ID is to be changed with each FTM session. In all cases, a new device ID is generated for each FTM session.

C: We need to decide whether opaque ID is required in each option. I see 4 options (1 or 2 and with or without opaque ID).

C: I think both cases are for implementation purposes. A vendor can make the choice. The options remain the same.

C: I have a lot of trouble with option 1. The AP has no idea who the STA is. Option 2 seems to work better. There, it’s quite clear that as long as the device ID changes every time, it’s safe. The STA can decide if the ESS knows who it is or not. The only reason for using an opaque ID in option 2 is if you are retaining the underlying device ID. Option 2 is cleaner. We only have to provide hooks. We don’t need to describe how to use it and then say that the STA can provide the ID in message 1 and the AP can provide a new ID in message 2. I much prefer Option 2 over Option 1.

Q: Is there an indication in message 1 that device ID is being used? If that’s a flag, is there a “device ID zero” that needs to be part of message 1 in alignment with other uses?

A: According to the current text from Kurt Lumbatis, it’s explicitly stated that the first time, the STA doesn’t send it. Otherwise it’s there. I’ll have to think about adding a flag.

Q: To be clear, in your original presentation for Option 1, a flag was understood to be used. Is that true for Option 2? The activation flag is not indicated in the diagrams, but it’s there.

A: Yes. I believe that’s true.

Q: Does that answer the question on the flag?

A: Maybe. The AP may not know the STA anymore, so that could be a problem area. The first message looks radically different from other messages we are trying to send. An AP-forgotten device ID would look like the first case.

C: This is meant to build on top of Kurt’s status indicator, I believe.

C: The presence or absence of a zero-length identifier could signal the first time a STA is joining. And as Jay indicates [in the teleconference chat], PASN has the RSNE IE.

C: My assumption is that the presentation was just not showing Kurt’s status flags.

C: I think we are discussing two things. If the STA is coming for the first time and whether the STA activates device ID. Kurt’s document covers if the STA is coming for the first time or the STA has lost its device ID.

C: But it will send the indication that it wants a device ID.

C: Yes. That should be done in Authentication message 1.

C: The text also includes the response from the AP indicating whether the STA was recognized and given a new ID, or that it was not recognized and is given an ID to use, if it wants.

C: I believe that for Option 2, the device ID should always be assigned.

Q: Meaning that the AP can’t send a zero-length device ID to tell the STA to keep using its existing device ID.

A: Yes.

C: Unless it uses opaque.

C: While I agree it enhances privacy to do this, we have to remember the PAR. The fixed ID behavior is in the baseline, even with RCM. The second option increases privacy beyond what’s required.

C: We are discussing using the address for FTM. We are not associated. We are doing multiple FTMs to different APs. Under the current text, you don’t have to use the same MAC address for each FTM session. So, we should keep the same level of privacy. I don’t think option 2 is an enhancement over the privacy of the current standard.

C: Agreed.

C: I’m a little lost here. In general, we have issues with PMKID, which is handled similarly. For the device ID, we have no rules for how that’s assigned. If we are transmitting something we get from the AP for multiple PASN setups, that’s a serious privacy threat. We should always have some protection for the AP-assigned value. It shouldn’t be in the clear. I prefer that we always change the device ID every time rather than relying on encryption that doesn’t appear to be required. Or that we always send the device ID in an encrypted frame/IE.

C: I think the current draft does not talk about how often to present the same device ID. Implementation guidance would help. And this is Option 2. In Option 1, it’s always encrypted because that one uses messages 2 and 3.

Q: Can we add a note that says in PASN, the AP always assigns a different device ID. For other cases, we don’t need such a note.

C: That might be normative text, not a note.

C: I’m concerned how the various APs stay synchronized every time a device comes along. How do they stay synchronized if they are changing the device ID every time? I like the sub-option of using the opaque ID and keeping the device ID fixed. That way, the AP can use some opaque algorithms and not have to send messages across an undefined medium in order that all APs can recognize the STA. That would make the opaque ID normative.

C: I think we are getting lost in the weeds here. If we return to our use cases, I’m not sure how generating a new device ID every time a STA does PASN would be helpful for the network. All of our use cases arise from the network not being able to identify STAs. If we generate a new device ID with each PASN exchange, I don’t think we’re doing anything useful. IEEE 802.11bh is not very useful to a STA vendor. There’s not a lot of interest in implementing it. We should take a step back. We are solving this CID that says, “work with PASN.” If there’s no problem being solved by changing the device ID every time, let’s not do that.

C: This is solving a STA trackability issue. We get a device ID from the AP. It could be misused. Thus, it would be good to change it every time because we don’t have a good mechanism to protect it. The device ID should change every time, or it should be encrypted, especially if the STA has no control over the device ID value. Encryption seems the better option.

Q: Are you saying we should not use device ID in FTM and fall back to MAC addresses only? I’m trying to understand.

A: We should try to solve a problem. How would it help the network to track a STA dealing with FTMs if it sends out a device ID every time and it doesn’t even know who the device is until it assigns a new device ID.

C: In option 1, you’ll note that even though the AP generated a new ID, the device responded with an old ID. And the AP can throw away the new ID, as can the STA.

C: Actually, it can’t because (on slide 4) it gets returned in the lower left of the diagram.

C: Okay, but the AP can always recognize the STA.

C: I’ll still question the utility of a new device ID each time.

C: This is a TGbh issue. Whenever FTM is done, IEEE 802.11az needs to use the same MAC address each time. That’s what we are trying to fix. We need to deal with FTM sub-cases – whether it’s the STA that wants to know where it is or whether it’s the AP that wants to know where the STA is. And then options of whether the STA cares if it is tracked. In that last case, the STA can keep one ID even though the network tries giving it a new one. Option 2 is cleaner in that a new device ID is mandatory. I’d like to see text on this. You only need the hooks. Defining the usage is up to FTM.

C: [11-22/1806r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1806-02-00bh-cr-for-pasn.docx) has the proposed text to match these diagrams. Okan is looking for input from the group so he can clean up the document.

C: We have no good encryption mechanism for message 1. Maybe we should take a time out and define a general mechanism that covers device IDs and PMKIDs.

Q: Doesn’t slide 7 (opaque ID) show a way to encrypt the device ID in message 1?

A: Do we have such a mechanism?

A: Annex Z is used to encrypt the device ID.

C: But third parties tracking STAs can watch the opaque ID to track the STA.

C: So, we are changing the identifier every time. I thought APs didn’t want to do that.

C: My understanding is that device ID is not changed, but the opaque ID appears different each time. The encryption makes it look different.

Q: So, we have to go with opaque ID if we take this path.

A: The STA doesn’t have a lot of involvement in this particular case.

C: After looking at the comment and solution, I sort of agree with Dan. What problem are we solving here? I don’t think we understand the problem to even decide if this is an issue for TGbh. TGbh has enough issues of its own. I think this could be solved more easily in TGbi. And we are in comment collection resolution without involvement of the commenter. We’re wasting time. Let’s reject the comment.

C: That’s an option.

C: For me, CIDs 19 and 20 are problems we want to solve. They say that the AP or ESS should recognize the device. Why do they want to do that? It allows them to use RCM for each FTM session, to prevent tracking. That makes each FTM session independent and hidden from third parties. If the STA doesn’t want to be identified in Authentication message 1, it doesn’t send the opaque ID. It can still use different MACs. The proposed scheme is to allow the ESS to identify the STA if the STA is willing. Even if we protect PMKID, then PMKID has to be mandatory. This scheme is supposed to obviate that requirement. I don’t want to reject the CID, that’s not my preference. That’s up to the group.

C: The underlying requirement is for privacy for the STA that is doing ranging. If I compare what’s done in this solution, there’s a ton of overhead on top of what are very short FTM sessions. Sure, we could do it in TGbh, but I think TGbi is more appropriate. We should consider overhead in our solutions.

Q: How does this apply to TGbi? PASN has four modes. Will TGbi cover all of that? The proposal covers everything.

A: TGbi is discussing protecting more PII than MAC addresses, so I could see TGbi solving the problem in CIDs 19 and 20. There are more and better tools in TGbi for this.

Q: Is there a request in TGbi to handle these CIDs? Is that your intention?

A: I think the problem needs more characterization. I would encourage the commenter go to TGbi and discuss the problem there.

C: IRM solves the problem. I’d like to see your solution first.

C: My solution is to reject the comments.

C: We have to decide if we feel the solution is more appropriate in TGbh or TGbi.

C: Just because the commenter submitted the comment here does not mean we have to agree that we are the right task group to address it.

C: TGbh and TGbi are there for privacy. From an engineering point of view, TGbi wants to change the MAC during the association, so I’m not sure it’s applicable. Even if we view FTM sessions as a kind of association, I’m not sure that’s the way to look at it. I think TGbi is associated only. The commenter could submit comments to TGbi as well.

C: My personal take is that TGbi will consider any issue that is appropriate to privacy. If these comments require a broader solution, perhaps TGbi is the right place. I don’t believe they only deal with associated use cases. Shall we run the straw poll?

Proposed straw poll:

Which option should 802.11 focus on?
a) Option 1 (Auth Msg2 & Auth Msg3)

b) Option 2 (Auth Msg1 & Auth Msg2)

c) Neither

d) Either

Q: Could we add an option that says, “reject the comment and point to TGbi”?

A: I saw the neither option as going that way.

C: I wanted something explicit.

C: I don’t want to add that option to my straw poll.

C: Fine, then we can always run another straw poll if necessary.

Q: How about we go back to the neither/either of the original straw poll?

A: We can do that.

C: We know that Graham has done a partial solution for these two CIDs. A motion on them would point to that document as a partial solution plus something with the rest of the solution. I think Smith’s solution is really for CID 20. CID 19 is more standalone. We are sort of splitting the CIDs into the device ID bit and the rest.

C: There are other reasons to add device ID to PASN, but I don’t see the need here.

C: And the suggestion of changing Neither to Abstain is not an equivalence, but I’ll do whatever gathers the most useful information.

C: Okay, don’t make that change.

C: Remove either and allow multiple choices.

C: Why not run the original straw poll and then from the results determine if we need another straw poll.

C: An alternative straw poll would be to ask whether we want to address device ID in combination with PASN.

A straw poll addressing that latter point was run:

Should TGbh address Device ID used in combination with PASN?

a) Yes

b) No

c) Abstain

Result: 8/6/3 (Y/N/A)

The original straw poll was run for completeness, despite the requesters not caring to do so.

Result: 0/7/3/5 (a/b/c/d)

C: I don’t know what that means, but we have more data. Any further comments?

C: We’ll think about it.

C: If there’s no progress made on this, wait until May to deal with it. Those two CIDs could be rejected for lack of consensus. Encourage the group to build on the other good work done here. And encourage the commenter to participate in TGbi.

C: We may do so with the remaining 3 CIDs.

C: Between option 2 and either, that’s 12 in favor.

Q: Do we need to talk about option 2 requiring the opaque ID from Annex Z? Do a straw poll on that?

A: If we go to option 2, we should get STA input on the identifier, otherwise it’s not good for the STA.

Q: Input on the device ID itself?

A: Yes. The STA should participate in the obfuscation of the value over the air. If it only comes from the AP, the STA has no control and it’s kind of risky. We could easily add STA-generated parameters.

C: I’d like a contribution on that because I’m not understanding how this helps.

C: If we go with option 2, Annex Z is one choice, an example for protecting the device ID.

C: If so, I’d like a contribution on that as well. That way the AP understands what to do with the information it is getting. We will continue the discussion next time and on the reflector.

**Meeting adjoined at 11:30 a.m. EST.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 04/18 | Bredewoud, Albert | Broadcom |
| TGbh | 04/18 | Chappell, Matthew | Cox Communications |
| TGbh | 04/18 | De la Oliva, Antonio | InterDigital |
| TGbh | 04/18 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 04/18 | Harkins, Dan | HPE |
| TGbh | 04/18 | Henry, Jerome | Cisco |
| TGbh | 04/18 | Kain, Carl | USDOT, Noblis |
| TGbh | 04/18 | Kneckt, Jarkko | Apple |
| TGbh | 04/18 | Levy, Joseph | InterDigital |
| TGbh | 04/18 | Liu, Yong | Apple |
| TGbh | 04/18 | Lumbatis, Kurt | ARRIS/CommScope |
| TGbh | 04/18 | Luo, Yuanqiu | Futurewei |
| TGbh | 04/18 | Luo, Ye | Nokia |
| TGbh | 04/18 | McCann, Stephen | Huawei |
| TGbh | 04/18 | Montemurro, Mike | Huawei |
| TGbh | 04/18 | Mutgan, Okan | Nokia |
| TGbh | 04/18 | Nezou, Patrice | Canon |
| TGbh | 04/18 | Orr, Stephen | Cisco |
| TGbh | 04/18 | Petrick, Al | InterDigital |
| TGbh | 04/18 | Riegel, Max | Nokia |
| TGbh | 04/18 | Sam, Harvey | Broadcom Corporation |
| TGbh | 04/18 | Sevin, Julien | Canon |
| TGbh | 04/18 | Smith, Graham | SRT Wireless |
| TGbh | 04/18 | Smith, Luther | CableLabs |
| TGbh | 04/18 | Thakur, Siharth | Apple |
| TGbh | 04/18 | Thakore, Darshak | CableLabs |
| TGbh | 04/18 | Li, Yan | ZTE |
| TGbh | 04/18 | Yang, Jay | Nokia |
| TGbh | 04/18 | Yee, Peter | NSA-CSD |