Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Plenary Meeting Minutes, January 2023Randomized and Changing MAC addresses (RCM) |
| Date: 2023-01 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter YEE | NSA-CSD | Mountain View, California |  | peter@akayla.com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh January 2023 Interim meeting.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting January 16, 2023, 10:30 a.m. to 12:30 p.m. EST**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the meeting to order at 10:42 a.m. EST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/2124r03](https://mentor.ieee.org/802.11/dcn/22/11-22-2124-03-00bh-agenda-tgbh-2023-jan-interim.pptx). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ January Interim meetings: Monday, 10:30-12:30; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00; PLUS: TGbi joint Thurs 13:30-15:30
	+ Approve November plenary and Nov/Dec/Jan teleconference minutes
	+ Timeline update review
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r09**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r13**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Contributions (slide 22)**
* **Way forward to D1.0 (slide 23)**
1. **Approve agenda**

The agenda was approved by unanimous consent. It includes a newly announced joint meeting with TGbi on Thursday PM1.

1. **Approve minutes**
* November plenary session: [11-22/2147r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2147-00-00bh-minutes-tgbh-plenary-meeting-november-2022.docx)
* Teleconference minutes:
	+ Nov 8: [11-22/2155r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2155-00-00bh-meeting-minutes-tgbh-november-8-2022.docx)
	+ Nov 29: [11-22/2148r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2148-00-00bh-802-11bh-telecon-minutes-november-29-2022.docx)
	+ Dec 1: [11-22/2154r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2154-00-00bh-minutes-tgbh-december-1st-meeting.docx)
	+ Dec 13: [11-22/2156r01](https://mentor.ieee.org/802.11/dcn/22/11-22-2156-01-00bh-802-11bh-telecon-minutes-december-13-2022.docx)
	+ Dec 15: [11-22/2185r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2185-00-00bh-802-11bh-telecon-minutes-december-15-2022.docx)
	+ Dec 20: [11-23/0035r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0035-00-00bh-802-11bh-telecon-minutes-december-20-2022.docx)
	+ Jan 10: [11-23/0043r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0043-00-00bh-802-11bh-telecon-minutes-january-10-2023.docx)

A motion to approve these minutes was made by Kurt Lumbatis (ARRIS/CommScope) and seconded by Carol Ansley (Cox Communications). The minutes were approved with unanimous consent.

1. **Timeline review**

The target for the initial WG letter ballot on a Draft 1.0, which is yet to be created, is March 2023.

1. **Clarification of requirements**

Graham Smith (SR Technologies) presented again his clarification of requirements document ([11-22/2150r02](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-02-00bh-clarification-of-requirements.pptx)). While this was presented during the last teleconference, he is repeating that presentation to provide information to the far larger audience available during this interim meeting. Please see the minutes ([11-23/0043r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0043-00-00bh-802-11bh-telecon-minutes-january-10-2023.docx)) of the January 10, 2023 teleconference for a summary of the presentation and the discussion at that time.

Q- In regards to adopting the MAAD MAC scheme in addition to Device ID, why can’t we use the MAAD MAC as the Device ID?

A- I said that because Device ID is already adopted, so it seemed confrontational to adopt MAAD MAC in place of Device ID.

C- I will make a presentation of a similar proposal that isn’t MAAD MAC. Some spoof AP issues are out of scope for TGbh. A pre-association scheme needs to be widely acceptable to the Wi-Fi industry. Otherwise, if it might not be available in all products.

C- To be clear, IEEE 802.11bh was supposed to be quick and dirty. Done quickly. We’ve failed miserably in this regard. To my mind, I think all the encryption schemes are suited for IEEE 802.11bi. TGbh should have done something simple and months ago at that. We got more and more complicated, looking too strongly at privacy. This led to being somewhat untimely. IEEE 802.11bi can do things better on their own timeline. We just need to decide the delineation between the two.

C- If we wait for IEEE 802.11bi, we might end up waiting for another 3 years.

C- Some of this might be a good discussion for Thursday’s joint TGbh/TGbi session.

1. **The discussion on pre-association schemes**

Jay Yang (Nokia) briefed [11-23/0061r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0061-01-00bh-discussion-on-pre-association-identification-schemes.pptx). The Device ID approach that is in the TGbh specification addresses the troubleshooting use case, but there are many pre-association identification use cases that need coverage if we are to be responsive to the Wireless Broadband Alliance (WBA) and the Wi-Fi Alliance (WFA). These are things like client steering, VBSS implementation, etc. During the November plenary, there was an indication of strong support for covering pre-association use cases. Any RCM implementation that enables a STA to use a random address in the MAC header could be subject to a DoS attack. A pre-association scheme could obviate some of that load by turning away STAs that are not recognized without going through computational complexity of a full authentication/association exchange. There are several schemes that deal with pre-association: old IRMA, MAAD, new IRMA, ID encoding, RRCM, and e-RRCM. There are security concerns with some of these pre-association schemes. They should provide the protections against replay attacks, identifier copying, and spoof AP association that come with the Device ID approach. Yang believes that with so many candidate solutions, there should be a vote amongst them to determine where to concentrate our efforts. How the pre-association schemes work (in an IE or in a MAC address) is also something to be determined.

C- I don’t think TGbh should worry about DoS attacks. These attacks exist without RCM. We are trying to address problems caused by RCM.

C- RCM can exacerbate DoS attack mitigation tools.

C- Those should be addressed as part of the REVme work. If you pump a lot of data, you distract the AP.

C- I would claim that our focus in TG is pretty specific.

C- I agree that pre-association client detection is out of scope. When we use the Device ID, it is voluntary. You should be able to authenticate without doing Device ID.

C- The straw poll in Bangkok showed a preference for a solution that includes pre-association.

C- I don’t see a lot of value for pre-association device identification. I only see that useful for network selection (2.4 vs. 5 GHz). I don’t see much use otherwise.

C- It sounds like you want to disband the group or not make progress.

C- I would point out that the allow list on the AP is supported by MAAD. You don’t need any encryption. The MAAD scheme will give you a list of STAs that are acceptable. The claim that an identifier should not be exposed on the air, even if it’s a one-time identifier. I don’t see a problem here. MAAD changes those identifiers frequently. I don’t see a problem with the cleartext transmission of the identifier by the STA.

C- That statement in the slides was Jouni Malinen’s (Qualcomm) strong concern that the MAC address might be used for access control decisions.

C- A simple method that works is better than a complicated method.

C- That could be another of the high-level questions for the group.

C- Based on the straw poll results, we can see the task group’s preference for a MAC address-based solution.

C- I think we have to realize that all of the pre-association schemes have to benefit both sides of the conversation. Most of the protocols in IEEE 802.11 have an AP side and a STA side. RCM was a purely STA-side benefit, but did nothing for the AP. All of the use cases that were brought up are network-side problems. So, unless there’s a compelling reason for the STA sides to implement our solutions, then there’s little reason to believe a STA vendor will implement one. Instead of arguing which solution is the best, we should come up a reason why a STA vendor would implement any of these schemes.

C- A STA relies on the network to provide services. Thus, a STA vendor might want to implement one of these schemes if that allows the user to enjoy the benefits of the network if the network would not otherwise provide them if the STA did use a pre-association technique. It needs to provide some identity stability for the STA in order for the network to optimize the services it offers. Yes, there are many schemes that can provide that identity stability to the network. The pre-association identification of a STA provides the network with the ability to provide services.

Q- Aside from captive portal (which is not defined in IEEE 802.11), all of our use cases talk about problems on the network side. Can you provide an example of a STA being better served by an IEEE 802.11bh solution than it gets from RCM.

A- Network steering is one such use cases. Many providers steer STAs to suitable BSSes. There are many reasons for this steering, such aa a corporate reason (allow known users to use a certain AP but steer guests to a different BSS). Random MAC addresses broke that. The network was no longer aware that it was the same device coming back under a different guise.

C- Why should a STA do this? It’s not so much that the STA has to implement everything. You need something simple that a STA and an AP can do. Something like MAAD. If you want to do parental control, it’s done with by a list of MAC addresses. APs already do this. STAs already remember a MAC address for a particular ESS anyhow. MAAD is a small increment over that. Thus, it’s not that much work for a STA vendor. IRMA was withdrawn because of its complexity – no one would want to implement it. If we do anything, it has to be simple.

Yang offered a straw poll: Do you prefer “pre-association identification” (non-4-way handshake) to be communicated via an IE (or similar frame body protocol), or MAC Address?

* Option 1: IE/frame body
* Option 2: MAC Address
* Option 3: Abstain

C- As written, this leaves behind PASN (Pre-Association Security Negotiation) from IEEE 802.11az, which was discussed as a possible mechanism.

C- PASN is for a newly arriving device. This straw poll is about returning devices.

C- I’m fine with working on pre-association schemes, and I like using IEs. We should look at using PASN.

C- PASN does a 3-way handshake.

C- Can we add a 4th option for neither. And if we are going to push for a pre-association identification for returning STAs, the current MIB isn’t enough to handle that. It was designed for post-association identification. I think we need a separate MIB or mechanism to register user consent for both pre- and post-association.

C- Let’s not try to solve the problem now, let’s decide if we want to solve it at all. Aside from a neither option, a “none” option might be needed as well to register a desire not to do pre-association schemes. Or an option for both.

C- I wish there weren’t so many options. There won’t be a significant opinion out of this straw poll. You can anticipate the results of this vague straw poll with too many options. And if you want to relitigate the pre-association concept, do that separately. But we already ran that poll in Bangkok. We will learn nothing from this straw poll.

Q- Do you have another straw poll to run in its place?

A- No. This is just too detailed. The big deal isn’t whether to use an IE or a MAC address for the identifier. The big idea is whether we use pre-association schemes at all. And if I choose the MAC address option, should I select the both option to cover my bases?

C- I think we do motions because I can’t tell who voted how in a straw poll.

C- Both doesn’t make sense unless we do multiple schemes.

Q- Is this a multi-choice straw poll?

A- I don’t have a strong opinion on that part.

C- I would prefer that the straw poll be positive, not one that just rejects things.

C- The reason that neither is a useful option, is that the first two options can’t be looked at without dealing with user consent as well. Maybe add user consent into the question of the straw poll. When we look at the straw poll from the perspective of the future, I don’t want us to ask why we didn’t do user consent until now.

C- I believe that opt-in was always part of our scope.

The straw poll question is modified to put “opt-in” after “prefer”.

Q- Are you asking about a separate opt-in for pre-association identification over what was motioned in [11-22/1599r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-03-00bh-revisions-to-rsn-extension-element.docx)?

A- We have opt-in for post-association. We need one for pre-association.

The result of the straw poll (with single-choice options for IE/frame body, MAC address, and abstain) had a result of IE/frame body: 7, MAC address: 8, and abstain: 11. There were 9 participants who did not answer.

1. **The way forward**

We do have an existing draft (0.2), which has text the group agreed upon. We need to agree on what else goes in the document in preparation for a ballot in two months’ time. There are a lot of proposals from which to choose zero or more options. One question we can decide separately is whether the paparazzi spoof AP is something we need to deal with. This doesn’t appear to be a problem created by RCM and thus is outside of our scope to solve.

C- Because IEEE 802.11bh has us carrying an identifier, I think we need to spoofing AP. The spoofing AP has a chance to steal your identifier and thus needs to be considered.

Q- Do we think the spoof AP can steal the identifier?

A- That depends on the use case (and its solution). We should be consideringa third party that can steal an identifier.

Q- Are you asking if we are trying to stop an association from revealing an identifier? Or are we talking spoof APs in the context of one of the IEEE 802.11bh features? I don’t want to fix the problem in the base standard, but I do want to fix any problems that our solutions create.

A- Let’s address the existing issue first.

Q- Does anyone object to ruling the paparazzi spoof AP issue is outside of our scope, given that it was a pre-RCM problem as well?

[No objection.]

**Recessed at 12:31 p.m. EST**

**Meeting January 17, 2023, 1:30 p.m. to 3:30 p.m. EST**

**Mark Hamilton, the TG chair, called the meeting to order at 1:33 p.m. EST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/2124r04](https://mentor.ieee.org/802.11/dcn/22/11-22-2124-04-00bh-agenda-tgbh-2023-jan-interim.pptx). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ January Interim meetings: Monday, 10:30-12:30; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00; PLUS: TGbi joint Thurs 13:30-15:30
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [11-22/0651r9](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [11-22/0973r13](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Contributions (slide 22)**
* **Way forward to D1.0 (slide 23)**

[Agenda accepted with unanimous consent.]

1. **Identifier Status Codes**

Kurt Lumbatis presented [11-23/0083r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0083-01-00bh-identifier-status-codes.docx) (updated to [11-23/0083r02](https://mentor.ieee.org/802.11/dcn/23/11-23-0083-01-00bh-identifier-status-codes.docx)) on identifier status codes. It is intended to respond to comment identifiers (CIDs) 4 and 26 from the comment collection on Draft 0.2. Both request that if an identifier sent by a STA cannot be verified, then that status be indicated in a response from the AP. This is effected by a adding an identifier status octet to the Device ID KDE with values for “acknowledged” and “not recognized”. Lumbatis’ presentation only contains the Clause 9 text to specify the format of the identifier status field, not the procedures by which it is employed.

C- The table with the identifier status values needs a title. And it seems that a value should be specified for when the STA transmits the Device ID KDE since the signal is intended to be from the AP to the STA only. Thus, a value that doesn’t mean acknowledged/not recognized is needed.

C- Okay, 0 will mean unused, 1 acknowledged, and 2 will be not recognized.

C- The value of zero should be forbidden from the AP to the STA.

C- Okay.

C- Change acknowledged to recognized.

C- Okay.

C- I believe there are more CIDs that cover this case beyond 4 and 26. Perhaps you might be able to closer more CIDs with this text.

C- More CIDs will be covered in the matching Clause 12 text submission.

Q- You intend to move your Clause 9 text into the Clause 12 submission ([11-22/1329r12](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-12-00bh-cid-resolutoins-for-12-2-11.docx)) for a unified offering?

A- Yes.

C- I’d prefer zero to mean reserved.

C- Reserved in IEEE 802.11 already is defined as zero.

Q- Why does the STA care if the AP recognizes it? This goes back to my point from yesterday about making this a specification that STA vendors want to implement.

A- The non-AP STA could return an identifier that the AP doesn’t recognize. That status code allows the STA to know this.

C- We should handle this through text that says what the STA does when it gets such a status code. Otherwise, it’s just up in the air as to what the STA does.

C- There’s no consensus on this status information being useful and I’m going to vote against it. I do understand that there are differences, and the STA could do something, but that’s not justification for this added complexity that has no defined outcome.

C- I think the status code is help to the non-AP STA side. That STA can decide what to do. The scheme is complex. If the STA generates an identifier, this would be helpful in that case too, not just for the network-generated ID. PMKID is also acknowledge/not acknowledged. So, this is a similar case that should also be acknowledged/not acknowledged.

Q- With PMKID and SAE password identifier, we say what the STA should do based on the status it receives. What should we add to Clause 12 that says what the STA does when it receives one of these status values? What is STA going to do with this information?

A- This is helpful in the troubleshooting use case. Telling the STA that its ID wasn’t recognized would allow the user to tell the help desk that this occurred, and that troubleshooting isn’t working. The STA will have a clue as part of the troubleshooting process.

C- I agree with those saying there’s no point in having the field if there’s no behavior attached to do it. Just having it for the sake of having it is not useful.

C- What happens with the status value could be outside of the IEEE 802.11 specification. The value is percolated to upper layers.

C- If the idea of the ID scheme was that you gave an ID to a STA with no expectation that it changes, then if the STA uses it every time, then if the AP doesn’t recognize it, it sends a new one. Then the STA knows that it wasn’t recognized. But that morphed into the AP giving one for any random reason. I’d be happy not to have a status field. If we don’t, then let’s go back to the mere fact of sending a new ID is indicative of the AP not recognizing the one the STA sent.

C- The group should recall that the reason we are doing this is that the network behind the AP and the STA have some shared context. We are trying to connect the STA to that context. We could add something in Clause 12 that says if the STA gets a new ID from the AP, then it should recognize that the upper layer context has been lost and should take appropriate actions at the upper layer.

C- I think this table comes from text that is suggested for Clause 12.

C- If we don’t accept these changes, we can just reject CIDs 4 and 26.

C- Do we have a use case for what the STA can do with this information? The use case for troubleshooting could be used to inform the user of the problem as part of a backchannel call to the help desk. But I don’t see anything else. A sentence could be added that says that the value is passed up the stack by the STA for purposes outside of the scope of this specification.

C- If an ID is presented to the non-AP STA, the difference is the action by the non-AP STA based on the value. There doesn’t appear to be any since the actions are out of our scope.

C- That’s not quite true – the fact that the ID was recognized by the AP and that status was sent to the STA means that the STA should continue to use that ID because it is apparently valid.

C- The fact that the STA gets a new ID value conveys the same message in the negative case, while the lack of a new value means that the one transmitted by the STA was recognized.

C- In the Clause 12 text, does it need to say that no new identifier is provided, or should it just say that no identifier provided means “use the old one”? Some wordsmithing is needed here.

C- I agree with that. But I don’t know what it means to provide an identifier. I would accept a zero-length identifier meaning that the STA continues to use the last received identifier it was assigned.

C- I don’t think there’s a length field there for the identifier, so it can’t be zero length.

C- The ID blob length can be added to the KDE, but really, knowing the length of the KDE, only the ID blob has a variable length.

Q- Why isn’t the identifier always returned and the STA can see if it is the same or different?

A- That’s one way we could have done it, but we chose not to.

C- This text should all be in clause 12.

C- This should be wordsmithed offline. Perhaps interested parties go do so in an ad hoc fashion, since we are going in circles here.

C- There’s a straw poll in the chat that might help us move forward.

Straw poll: Do you support informing the non-AP STA whether the AP recognized the provided identifier?

The result was 13/7/6 (Y/N/A).

Kurt Lumbatis to post an update to the text for discussion on the reflector.

1. **Way forward discussion (slides 23-29 of the agenda deck)**

Q- [Slide 27] For people who understand client-side issues, would having rules around what the non-AP STA’s MAC address is set to be problematic?

A- I brought up this concern in the past. If we have to do something here, I would prefer placing the identifier in the IE. It becomes tricky if the non-AP STA does not coordinate both the identifier MAC address and the real MAC address.

A- MAC address use as an identifier is difficult for implementation.

A- If we think it’s hard, no one has to do it. It’s an optional feature. Why does the previous commentor say it is hard to do it?

A- I’ve provided technical reasons why it’s difficult. This can come down to hardware implementations. Sure, it’s optional. Vendors can choose not to implement it. If they don’t, then this won’t be deployed. So, we should not try to add things that are not likely to get implemented. Understand the implications of that. This is supposed to be a simple update to existing devices to fix problems. If it doesn’t work for existing devices, then we have a significant problem here.

C- If we take IEEE 802.11aq and expand it to require that the STA remember the MAC address for an SSID and pop it again on return, then what’s the problem? The MAAD scheme is of interest, so what’s the difference between remembering the MAC address and remembering an identifier.

C- I agree with the previous commentor. IEEE 802.11aq allows the STA to use any MAC address. I do not understand the difficulty between the IEEE 802.11bh proposal and the IEEE 802.11aq features. Maybe there’s not much difference. Maybe there is a hardware limitation for some vendors. I hope I can know more about this part.

C- At a high level, there’s a huge difference between who generated the address and who has to remember. In many STAs, many processes are running in parallel. If we mandate the network supply the MAC address, then multiple addresses could be supplied and cause confusion, or parallel processes on the STA might have to be done in lockstep to prevent clashes. I’m pretty sure that it won’t get implemented.

Q- Does it matter where on the non-AP STA the address is generated?

A- No. It matters that it was on the non-AP STA.

Q- The IRMA scheme was the same as the MAAD scheme, but the STA told the AP what address it would use. The proposal was not pushed too much because there were strong opinions that the network should be allocating the identifier. Maybe the IRMA scheme should have been pushed harder. Would that sort of scheme work for the STA side?

A- It would be easier, but I cannot promise that it would be as easy as one would like. I prefer not to mess up the MAC address. Having getting the address from the rule, from an AP, or from the existing STA, I would prefer the last of those options.

C- All of the problems we are solving are on the network side, and hence the network has to own the identifier space. That’s why there was a push for network-generated identifiers. STA-generated identifiers could be problematic because of poor implementations and the relatively small amount of address space.

C- We already let STAs generate randomized MAC addresses, so I would hope that they can do that all right. IRM could run with the current MAC randomization process on the STA, but some of the other schemes dictate the identifier/MAC address generation scheme.

Q- Has anyone seen a clear direction or had a change of mind that is worth straw polling at this point?

A- [No response.]

C- [Slide 29] How about a non-AP STA generated (non-MAC-address) identifier capability?

C- The only reason I can think of for having the non-AP STA generate an identifier is when it is not associated. Otherwise, it’s not worthwhile. I would look at that question as being for non-associated uses only.

C- I don’t understand the leap that this only makes sense pre-association.,

C- The current mechanism in the draft is for the identifier to be given to the non-AP STA by the AP for use when the non-AP STA returns to the network. That’s self-contained. There’s no reason for the non-AP STA to generate an identifier. But for non-associated use cases, then it maybe it makes sense.

C- The whole point of all of this stuff is to allow the client and the network can point out their shared context. What if that context was done outside of IEEE 802.11 (like a business relationship with a network provider)? The STA presents its user ID from that relationship, which might be useful. But that’s not a pre-association use case. Think about this more offline. I don’t want to bias this discussion, that’s just my thinking.

C- Your use case sounds outside of the scope of IEEE 802.11 and should be done at the upper layers. Maybe I would use the upper layer for pre-association use cases too. I need a more specific explanation of this use case.

C- What is the identifier is more important than who is creating it.

C- Having the non-AP STA generate a non-MAC address identifier would be the worst case. The network has to be able to make use of the identifier. The network identifies STAs by its own internal identifier. If the non-AP STA generates an identifier, then the network has keep a mapping. MAC addresses, generated well, would be better, but best would be AP generated identifiers.

C- Once we get passed the network-generated ID, the why of a non-AP STA identifier generation gets tricky. We have troubles agreeing on rules for identifier generation and where it goes (MAC address and IE). If we can agree on the barebones minimum, if it can only be generated in one place, is the AP okay? Then move up from there? We can get to a Draft 1.0 that way.

C- The simple, straightforward thing is what’s in the draft. Do we stop there, or do we add more things? Your suggestion sounds like no, we should not. But we have 8 other schemes being proposed, each with their own proponents. Does the group think we need more than what’s currently in the draft?

Q- When I read the straw poll text, I see a non-AP STA generated identifier. This doesn’t say having both sides generate it. Does this text really exclude the network-generated identifier?

A- The straw poll is not trying to exclude anything. It’s just asking if STA-generated identifiers are needed. It doesn’t say anything about replacing the network-generated identifier. Your question is valid, but the text wasn’t written in that context.

C- If you run the straw poll, I hope it is specified that there are no implications regarding network-generated identifiers.

C- One reason for doing non-AP STA ID generation is that I don’t trust the AP enough to do that. And that it might be coming from the upper layer.

C- [11-23/0119r02](https://mentor.ieee.org/802.11/dcn/23/11-23-0119-02-00bh-way-ahead-decisions.pptx) might be worth discussing to cut down on our options or make decisions on what to add.

**Meeting recessed at 3:31 p.m. EST.**

**Meeting January 18, 2023, 8:00 a.m. to 10:00 a.m. EST**

**Mark Hamilton, the TG chair, called the meeting to order at 8:03 a.m. EST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/2124r05](https://mentor.ieee.org/802.11/dcn/22/11-22-2124-05-00bh-agenda-tgbh-2023-jan-interim.pptx). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ January Interim meetings: Monday, 10:30-12:30; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00; PLUS: TGbi joint Thurs 13:30-15:30
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [11-22/0651r9](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [11-22/0973r13](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Contributions (slide 22)**
* **Way forward to D1.0 (slide 23)**

[Agenda approved with unanimous consent.]

1. **Use case for OWE mode**

Jay Yang presented [11-23/0022r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0022-01-00bh-use-case-for-owe-mode.pptx). He notes that this OWE mode is for public, open networks usually with captive portals. The portal is usually displayed with a limited mode Web UI to input some sort of authentication credentials, typically user name and password. With RCM, the captive portal tends to require the Web UI authentication on each association, which is a suboptimal user experience. OWE (Opportunistic Wireless Encryption, RFC 8110) is an encryption method to improve the privacy of users connected to public networks. There’s no authentication in OWE – the STA and the AP use Diffie-Hellman public keys exchanged with each other in order to generate a PTK between them. Yang offers a possible solution for returning STA identification in public networks that combines the captive portal (which is not defined in IEEE 802.11) with OWE and IEEE 802.11bh STA identification. This involves the STA associating the first time with OWE providing encryption coverage. The AP gives the STA a Device ID. On return, the STA performs OWE and supplies that Device ID in order for the AP to recognize it. In addition, the AP can provide a new Device ID to the STA. Given the unauthenticated nature of OWE, Yang notes that it’s possible for a fake AP to mount a man-in-the-middle attack by tricking the STA into associating with it and getting the Device ID from the STA, which the fake AP then uses to connect to a legitimate AP as though it were the STA. By doing so, the fake AP would be able to use the network’s services without incurring any potential charges for that usage, those charges being billed back to the real STA. Yang asks if the task group should figure out a means for the STA to identify the AP when it returns to a network so that it does not supply its Device ID to a fake AP.

C- I’m not sure what the need is for this use case. Public venues should use secure networks, such as Passpoint, despite the complexity that has been pointed out. The clearest solution is to use browser cookies by the captive portal rather than an IEEE 802.11bh-based solution. The association can then be bound at the network layer. I needed a clearer justification for using your solution over an upper layer-based solution.

C- Passpoint and captive portal have implementation limitations and challenges. Use of cookies by the captive portal, but dynamic verification codes for guest users still seem to be required.

Q- Even with IEEE 802.11bh verification, the dynamic code is still required?

A- No, it can be skipped.

C- Then cookies can do that as well.

C- But IEEE 802.11bh users a layer 2 identification.

C- But this can be done at an upper layer too. There’s no requirement for a layer 2 solution.

C- The cookies are stored on the STA. The STA would still need to provide its verification information. If a layer 2 solution is used, the captive portal can be skipped.

Q- If [slide 10] were using an old-style captive portal, what would be the security mechanisms that prevents return identification from being attacked by a man-in-the-middle? Do we need to solve this existing problem that occurs regardless of RCM? I don’t think IEEE 802.11bh needs to do a better solution to that problem than already exists. Malicious users can fake their ways through captive portals.

A- Your case is a fake captive portal instead of a fake AP stealing credentials. I’ll think more about that case.

C- The STA is the one the fake AP wants to attack, not so much the network service. You would want to steal the STA’s traffic to find something sensitive.

C- Public Service Announcement: don’t type sensitive information into a captive portal.

C- I agree that this kind of fake AP is something for IEEE 802.11bh in particular. There is an attacker who wants to obtain a valid ID for connecting.

C- There might be some TGbi discussion to be had here.

C- Regarding the question of ID cloning by an attacker, OWE doesn’t solve it, so our current IEEE 802.11bh draft should not be recommended for use with OWE. If the user is knowledgeable except over a protected connection, then mechanisms for HTTPS security would come into play. I don’t think we need to solve this particular problem at the IEEE 802.11 level. I would be hesitant about providing sensitive information to a captive portal. It’s very easy to talk to fake captive portals without being aware of it. It’s too easy to get a certificate that verifies up to a root of trust and looks like it is a valid domain name. I don’t think we can come up with better mechanisms at layer 2, especially using OWE. Passpoint already solves this problem securely.

C- We want to enhance the current specification to make it better so that the STA can recognize that it’s talking to a fake AP. I see a lot of use of captive portals but not Passpoint, which I think is down to Passpoint’s complexity. I think the specification should allow both solutions, with the market making the choice. I’d like the STA to get some key from the legitimate AP and be able to do authentication on return. The user inputs identification information one time and then doesn’t need to do that again. That would be a benefit to the user.

Q- I don’t understand the extension of OWE into our scope.

A- 20 years ago, STAs used fixed MAC addresses. Those addresses were used to identification returning STAs. New STAs had to provide authentication information. RCM broke use of the MAC address for returning STAs. We can create the next generation of captive portal capability.

Straw poll: Do you agree 11bh group should consider an approach for the public Wi-Fi to identify the returned STA? (Note: Public Wi-Fi means the security mode of the AP is set to Open or OWE mode.)

Q- Is this supposed to cover both Open and OWE modes? Or one or the other.

A- The current solution is based on Open mode, but I can remove that and make it OWE only.

C- I agree that Open needs to go because the identifiers can’t go in the clear.

The modified straw poll removes “Open or” from the note.

The result of the straw poll was: 9/11/4 (Y/N/A).

1. **The Way Ahead Decisions**

This discussion ([11-23/0119r03](https://mentor.ieee.org/802.11/dcn/23/11-23-0119-03-00bh-way-ahead-decisions.pptx)) by Graham Smith is based on his [11-22/2150r02](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-02-00bh-clarification-of-requirements.pptx) presentation from yesterday. While IEEE 802.11aq doesn’t require use of the same MAC address upon return to a known ESS, it’s generally implemented that way. The STA has to remember the ESS/SSID and the STA-generated MAC address that it uses with that ESS/SSID. This should have an opt-in capability bit to allow the user to choose to use this mode of operation. This is simple to implement and covers every use case, yet it requires no computations.

An IRM-type (Identifiable Random MAC) scheme has the STA telling the AP the MAC address it will use on the next association. The STA still keeps a list of ESS/SSIDs and matching IRM MAC addresses, switched on by an opt-in capability bit. This is simple to implement but is more secure than using the “same MAC address” in IEEE 802.11aq implementations, also without requiring computations. It shouldn’t be much harder for a STA to do this if it can do “same MAC address”.

Another option is a non-encrypted ID in an Information Element (IE) scheme. The STA has to remember this ID to match it with the ESS/SSID and there needs to be an opt-in indicator. This too should be simple to implement, hard to copy, and capable of meeting every use case without computations. It does require a new IE and some amount of uniqueness to reduce the likelihood of ID clashes.

A more complex scheme would add encryption of the ID in the IE. Keys would have to be exchanged and derived in order to support ID encryption. Now the STA has to maintain a list of ESS/SSIDs and matching IDs and keys. This is still opt-in. Security is greater in this case and every use case can be met, but some amount of computation is required by the cryptograpy.

Smith would like to run separate straw polls for each option above and then hold a motion to adopt the highest vote gaining option for incorporation into the draft.

Q- Does the first option mean the IEEE 802.11bh disbands?

A- No, because IEEE 802.11aq doesn’t specify that the same MAC address should be used on return, nor does it cover opt-in. It would be the quickest option for us to finish.

Q- How does the second option relate to IEEE 802c? The IEEE RAC was against randomized MAC addresses stomping on certain address forms. When you set the local bit on a MAC address, it’s to be used on the local LAN segment, which is the purview of the AP, not the STA. Thus, the STA should not be usurping the role of the AP to manage the LAN. Are we going to be hit by the RAC again if we adopt this option?

A- We got random MAC through in IEEE 802.11aq with the local bit set.

C- We got it through using squirrelly language that everyone misinterprets. I’m not sure what squirrelly language we would have to add to IEEE 802.11bh to dodge the RAC.

C- My understanding of how this relates to IEEE 802c is that IRM says nothing about it. The existing rules for choosing an address would be used with IRM, applied for each newly generated MAC address.

C- I agree with that. ANQP has a local MAC Address policy element that tells the STA the range it can use for MAC address selection.

C- Maybe Graham can clarify on the second option that the STA chooses its next time address using the existing IEEE 802c rules as the first step.

C- That applies to the first option as well.

C- I was asking for the network to provide a new mechanism for specifying the range of addresses.

C- That feels like something that IEEE 802.1 should be doing, not us.

C- That would also affect RCM in general and wouldn’t be unique to IEEE 802.11bh. Saying you can only pick a future MAC address from a prescribed range is not unique to IEEE 802.11bh.

C- That still feels out of scope to me, it doesn’t solve a problem that randomized MAC addresses created. It’s trying to make randomized MAC addresses better, but not something that was broken by them. It feels like something that IEEE 802.1 is working on.

Q- Why did you put MAAD in option 2?

A- Two major STA manufacturers said that couldn’t implement the MAAD scheme easily. MAAD has the AP telling the STA which address to use. IRM has the STA choosing its address.

C- I’d like to hear the reason why MAAD can’t be used again.

C- I explained the reasons multiple times yesterday why MAAD is difficult for us to implement. I’m not going to repeat them again. Regarding the proposed addition of an AP-assigned MAC address, please don’t do it in the second option. It should be a different option so I can vote against it. Regarding IEEE 802c rules on locally administered MAC addresses, I don’t want to repeat the IEEE 802.11aq experience. That wasn’t fun for anyone. We have a MIB variable that can do SLAPP procedures or locally administered MAC address procedures. The AP can provide information on the local policy used in a BSS. We could add some wording around that into IEEE 802.11bh. My concern is the security of a very small address range that could have clashes.

Q- What is the third option (non-encrypted ID in IE scheme)?

A- It’s a means of not using the MAC address as the identifier because some participants have expressed concern around MAC addresses being used for access control decisions. So, it’s really similar to a random MAC address identifier, just in a different place in the frame.

Q- What would we put into an amendment for the first option? Do we need to opt-in at all? The STA changes its MAC address on return if it doesn’t want to be tracked.

A- IEEE 802.11aq didn’t say “pick the same MAC every time on return.” We could document that need to pick the same address for continued identification.

C- Let’s say we did option 1 and wanted to be tracked. There’s no need for a capability bit to opt-in. What would happen if opt-in was indicated yet the STA used a different MAC address. Then the network still couldn’t identify it. The only way it could be identified was by actually using the same MAC address. We should remove the capability bit as its pointless.

C- I was trying to capture from what I heard in the group about a desire to have a capability bit.

C- For option 1, I would set a MIB variable to tell the non-AP STA to return the same address, as is done in most IEEE 802.11aq implementations. That might be all that’s needed. In any case, it might be a notification bit instead of a capability. The notification is that the scheme is being used by the STA.

C- So, an activated bit not a capability bit.

C- Correct.

C- I think there needs to be a handshake so the STA knows the AP supports this mechanism (the first option).

C- Good point – does this bit go from the AP to the STA as well as from the STA to the AP.

C- I think the handshaking would be useful information for both parties. The statement that the non-AP STA must use the same address when it returns is not correct. The non-AP STA only does so if it wishes to be identified as returning. I recommend we do not mandate behavior for a returning STA.

C- The MIB variable is how that would be done.

C- I think it is beyond the MIB variable. You could decide to do something on return.

C- Then we are getting into the dynamicism of the MIB variable.

C- It’s helpful to the AP to know if it needs to retain the STA’s address for future lookup.

C- Regarding that comment on the MIB variable, I disagree. We have lots of MIB variables that operate that way to direct a STA’s actions. They can be changed when desired. I will point out that option 1 is already deployed and used. We would just need to document it to produce something useful.

C- Something we could add under option 1 is that the fact that the exchange of the indication that this mechanism is using would be helpful to let both sides know when it’s worth bothering to store address information.

C- Allow/deny lists are broken. The AP only saves the addresses of things it cares about. Option 1 doesn’t require any storage beyond that.

C- Storage could also be upper layer as well.

Q- Tomorrow, could we run the straw polls? Hopefully the Webex voting mechanism works for everybody.

A- Exit Webex, kill any Webex processes on your computer, and then restart Webex. That seems to fix the problem. [But manual counting via the chat remains an option.]

C- Please run a test straw poll at the beginning so everyone can be ready for the real one.

C- I’ve done the zombie process killing, so I’m concerned about Webex. Maybe try using a separate device (phone or tablet). That seems to work much better than Webex on a PC.

**Meeting recessed at 10:00 a.m.**

**Meeting January 19, 2023, 8:00 a.m. to 10:00 a.m. EST**

**Mark Hamilton, the TG chair, called the meeting to order at 8:01 a.m. EST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/2124r06](https://mentor.ieee.org/802.11/dcn/22/11-22-2124-06-00bh-agenda-tgbh-2023-jan-interim.pptx). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ Next meetings plan (slides 31, 32, 33)
	+ Timeline update review
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [11-22/0651r9](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [11-22/0973r13](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Contributions (slide 22)**
* **--- Reserve last 15 minutes for the following ---**
* **Way forward to D1.0 (slide 23)**
* **Respond to Liaison from WBA:** [11-21/0703r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx), [11-21/1141r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1141-00-00bh-excerpts-of-wba-document-wi-fi-id-scope.pptx), [11-22/0668r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0668-00-0000-liaison-statement-from-wba-re-wi-fi-devices-identification-group.pdf), [11-22/0653r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0653-00-0000-2022-march-wba-whitepaper-re-device-identification.pdf)

[Agenda approved with unanimous consent.]

1. **Way forward discussion (continued)**

Graham Smith offered the revised [11-23/0119r04](https://mentor.ieee.org/802.11/dcn/23/11-23-0119-04-00bh-way-ahead-decisions.pptx), which has been updated with option descriptions based on comments voiced yesterday. He went over option 1 and took questions from the floor.

C- In general, opt-in could be for pre-association or for association.

C- For option 1, an additional disadvantage: it’s easier to track a device than the other options assuming the ESS is widely used, despite the improvements brought by RCM.

C- The opt-in bit is pointless. The STA shows that is has opted in by using the same MAC address as it previously used. If it wants to opt out, it will use a random MAC address instead.

C- The bit tells the network that the STA is planning to reuse this address, so that the network can plan on saving the address for later match. And the AP using the bit tells the STA that it is willing to remember the STA’s address.

C- I mostly agree with it being pointless, but it might be an informative indication bit.

C- I think an opt-in bit helps the user to express a choice.

C- Everything we here is optional based on the user’s desire. But there’s no need to express that in an over-the-air bit. An indication bit has limited utility.

C- Do we need to say anything about the bit in the spec or is that an implementation detail. And whether it is over-the-air or just a MIB thing is in question.

C- I think we need a handshake between the AP and the non-AP STA in order to establish the state of the feature.

C- This is mostly what Android does except for the opt-in bit, except when you set a user flag to not remember the address.

C- From the whole capability bit perspective, a STA shows up with a MAC address and the STA reuses it. That’s how things worked before RCM. Maybe there’s some subtlety here, but this was the expected behavior from the beginning. That doesn’t need to be signaled. I don’t see a need for a capability bit.

C- This presentation is to cover the options and hold straw polls on them. Let’s not debate the technical details of these options in depth when we are going to eliminate most of them.

C- I don’t find any value in this bit. It complicates implementation. But the easy to track disadvantage is a big red flag to me.

C- I see the opt-in question as being irrelevant. The STA does what it wants. The only reason for a bit that flags the behavior on both sides is to help the STA and AP save on memorizing things that neither wants remembered.

In option 2, the non-AP STA uses the rules of IEEE 802c and IEEE 802.11aq in coming up with a random address, which essentially means use of the local bit.

C- I disagree that option 2 is more secure. There’s a similar level of privacy maintained by switching the MAC address every time, but it’s not more secure.

C- Compared to an identifier-based scheme, this scheme requires that the STA use a MAC address that it has advertised to the AP. That takes away the flexibility of the STA.

C- Another disadvantage is that the MAC address must be changed, which can cause issues with upper layer components in the ESS that were expecting the same MAC address. There’s a reason why STAs reuse the same MAC address on a per ESS basis. This option would cause the upper layer software to need to be adapted, it’s not just an issue for the AP.

C- It’s no worse than option 1 in that regard.

C- Option 2 claims to have the same level of privacy as RCM. But it allows tracking of the STA by the network.

C- That’s the same as RCM when the STA chooses to use the same address for a particular network.

C- The point in option 2 is that the level of privacy is the same as RCM when a STA fixes its address for use in an ESS.

Option 3 is similar to IRM, except the identifier is provided in an Information Element (IE).

Options 1-3 are simple. Option 4 covers more complex schemes with an encrypted identifier and key exchange, the highest level of privacy, etc.

Q- We already have network-generated ID in the draft. That’s like option 3. Why are we having this discussion?

A- These options/schemes don’t conflict with that. These are options that could be used, but the existing network-generated ID scheme in the draft is not any of the ones in this presentation.

C- Option 4 has 3 schemes listed. RRCM is one of them, but it doesn’t exchange keys. They are locally generated.

C- Something we haven’t analyzed, is whether these schemes can be used for PMKID privacy. That needs some privacy protection. It would be nice to not duplicate work, but that hasn’t been analyzed here.

C- That’s a topic for the joint TGbh/TGbi meeting this afternoon. That may be a huge rathole and it’s not clear the task group has agreement on that.

C- The 8-bit status field discussed earlier this week could be reused to cover PMKID privacy.

As given on slide 7 of the presentation, straw polls were run to see if TGbh should adopt any of the options. The results are listed as Y/N/A.

SMA: 9/13/3

IRM: 6/16/4

Non-encrypted ID in IE: 4/19/2

A more complex scheme: 9/13/4

Q- The IE we are talking about in option 3, is that included in the 4-way handshake, or somewhere else, in the open, that could be used for pre-association?

A- The ID is placed in an IE that is used the Association Request. A new ID is provided in an IE during the 4-way handshake.

C- I’d like to see a straw poll to confirm the network-generated version of option 3.

Straw poll (option 5): network-generated ID sent by a STA in an IE. The ID is given to the STA by the AP during the initial association for use at subsequent associations.

C- This is what we have in the draft except that we haven’t defined the IE. The scheme in the annex will render that into an encrypted form and it will change every time. It is provided in the 4-way handshake. Option 5 just means we have to define the IE and which frames it is conveyed in.

C- Not everyone agrees with what is shown for option 5 is what is in Draft 0.2.

C- We don’t need to straw poll something that is in the draft already.

C- We have said no to all of the pre-association schemes so far. We’ve had polls that says we should support pre-association use cases. We have to have one of these techniques that supports pre-association. That could be option 5 (network-generated ID passed back to the AP during association).

C- We covered that in vote 4, which had the encrypted IE. Option 5 should be option 3 copied with the source of the ID being the network.,

Q- Are we just trying to say for this straw poll that we are asking if people are in favor of keeping what’s in the draft?

A- No, people are asking for something new.

C- That’s the ID in an IE in an unencrypted frame. It’s a twist on what’s in the current draft, although we haven’t said exactly what that is. It could be an IE in an Association Request or other pre-association frame. It’s not clear if the “blob” needs to be encrypted or if the ID changes per association.

C- I’m confused. If this is a blob that hides the information, that’s what’s in the draft. We just have to define the IE and in which frames it is used.

C- So, option 5 becomes define the IE and where it is used.

C- I’m against this without encryption.

C- Option 5 is close to option 3, but now we are talking about encoding the blob. This is different. I want to see a full proposal.

Q- The ID here is not changed per frame but per association, right?

A- That’s a valid question. We need to sort out these questions before running a straw poll. Somebody needs to a run a presentation before we can make a decision.

1. **Way forward**

We aren’t close to having a Draft 1.0 unless we use what we have in the draft as what is balloted.

C- We need to resolve the comments on the current draft first.

1. **TGbi joint meeting**

A joint discussion will be held about the overlap of our scopes and whether a TGbh solution can be leveraged by TGbi, or do they just ignore us. And we need to consider how to ensure our TGbh solution does not cause bigger problems for TGbi.

1. **March plenary planning**

Do we need more than 4 sessions during the March plenary?

C- Book 4 slots and let’s see how things go in the meantime.

1. **Teleconferences**

Shall we do weekly calls between now the March plenary?

C- I think weekly is overkill and prefer semi-weekly.

C- TGbi will meet every other week on Thursdays when TGbe isn’t meeting. Maybe TGbh meets the same weeks as TGbe.

Weekly calls will be scheduled. The lunar new year won’t be a problem because we can’t schedule that quickly. We did try scheduling Tuesday morning and Thursday evening sessions. The evening sessions did not garner much participation. I don’t think we should schedule Thursday evening going forward because of the lack of participation. Thus, the teleconferences will be scheduled for Tuesday morning (9:30 a.m. ET) and held weekly.

1. **Response to WBA**

We need to make more progress before we can get back to the WBA.

**Meeting recessed at 10:05 a.m.**

**Meeting January 19, 2023, 1:30 p.m. to 3:30 p.m. EST [Joint session with TGbi]**

**Mark Hamilton, the TG chair, called the meeting to order at 1:35 p.m. EST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-23/0135r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0135-00-00bh-agenda-joint-tgbh-tgbi-2023-jan-interim.pptx). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Any concerns with overlap of scope between TGbh/TGbi? Clarify the scope, if/as needed.**
* **Can TGbh adopt a solution that can help or be leveraged into TGbi?**
* **How do we ensure TGbh does \_NOT\_ adopt a solution that makes TGbi a harder problem, and/or causes TGbi to “undo” TGbh and do something different.**

[Agenda approved with unanimous consent.]

1. **General discussion of the last three agenda points**

Q- Any thoughts on spoof AP?

A- There are 4-5 requirements that deal with Association and spoof APs. The ordering of TGbh, TGbi, and TGbe is not expected to be an issue, so these requirements aren’t expected to be perturbed by TGbe’s schedule, which is likely later than TGbh’s but earlier than TGbi’s. TGbi will look at means for a STA to recognize a valid AP without identifying itself to the AP. Most of the TGbi requirements are directed toward obfuscating STA behavior against third-party observers.

C- TGbh is mostly looking at how to identify at STA that wants to be identified, while TGbi is mostly looking at how to protect a STA that doesn’t want to be identified.

Q- How does a new STA identify itself in pre-association use cases?

A- We have not had any submissions about that topic. It’s not clear if that will be dealt with only on the first encounter, or a later one.

C- I’d like to hear more on the direction of that topic.

C- You’re welcome to make a presentation on that topic. We have 53 requirements or so. Most of them do not have solutions. It’s early days.

C- I don’t know how to deal with a new STA joining an AP, only how to deal with a returning one. TGbh and TGbi might have different solutions.

C- That doesn’t sound like a problem created by randomized MAC addresses and therefore likely out of scope for TGbh. It’s an interesting problem and might relate to some of the solutions TGbh is creating, but that’s to be determined. But it really feels like it is out of scope.

C- We can talk about this topic offline. Also, please join TGbi sessions for more discussion.

C- When we started, there was already discussion about the need for two groups. TGbh was expected to take two years, TGbi four years. Both groups seem to be slipping, schedule wise. Somehow, it would be good to have one solution that works between the groups. Which solution should be leveraged for the grand solution isn’t clear.

Q- When the scope of the groups first came up, I noticed that TGbi’s title was “data privacy”. I see that you’re looking at PII. That seems different from data privacy. What’s the word?

A- We take data to mean PII information, not data frames. The user’s PII data is the question of TGbi. We’re not trying to do something to data privacy. In retrospect, a different title for the task group would have been good.

C- What about data in packets that is used for fingerprinting. That’s not PII necessarily, but it can allow tracking.

C- We are not addressing a distinctive quaver in spectral output. We’re not looking at PHY. We are looking at the MAC layer. Things like putting less data in probe requests and other things to reduce packet size, with the belief that this will make less fingerprintable data available.

Q- Is there any indication that PMKID will be carried in other frames beyond Association that makes a STA identifiable?

A- We haven’t had any solutions that include that, but there many requirements that remain to be addressed.

Q- Are there thoughts on a technical solution that can be shared between the groups? I’m not aware of one.

A- The most straightforward thing for TGbh to do is to look at TGbi’s requirements document. After that, presenting a solution in TGbi that works for TGbh would be interesting. If that can be done with PMKID, that could be an interesting solution.

C- We tried to make the scope of the two groups distinct, which is different from whether there is a single solution that solves things for both groups.

C- One thought: we should have more joint meetings, maybe combining several slots per meeting.

C- We could consider having a single joint slot at each meeting.

C- Or maybe one at the start of the week and one at the end.

C- I support having future joint sessions for coordination purposes. If that prevents having two solutions that look alike but aren’t quite so, that would be good.

Q- I wonder how many people attend both meetings. The task group memberships seem to overlap a lot. There might not be much value in joint meetings if the overlap is great. Does TGbi have use cases that are common to TGbh’s?

Q- How many people go to both TGbh and TGbi?

A- It looks like well less than a quarter of the room. So, not that much overlap.

C- Both groups seem to be floundering. Maybe everyone focuses on TGbh first and we put TGbi on hold for a while. Do that by means of a framework for advancing the work in sequence.

C- TGbi has a lot of other areas that we are trying to touch, so it wouldn’t be helpful to stop TGbi to wait for TGbh despite there being areas of overlap between the groups.

C- I’d be nervous if the WG said to focus on TGbh first, because TGbi could go down a path that doesn’t work well for TGbh’s needs. So, that optimization (sequencing) might be suboptimal.

C- I just think that having people from both groups focusing on one thing first would be beneficial.

C- We do try to ensure the meetings don’t occur in the same time slot so that interested parties can attend both.

C- When we formed the two groups, we expected TGbh to be quick, while TGbi would take a slower, more deliberative path. So maybe a not wholly sequential process could work, given the slippage in both groups’ sessions.

C- When solutions are proposed in TGbh, it would be good if the submitters were aware of possible TGbi impacts.

C- I don’t want to make TGbi’s life harder because of what TGbh does. But TGbi undoing some of TGbh’s work isn’t out of the realm of the possible. Sharing might bring some optimization, but it’s not a big thing. As for a common solution, I agree that I don’t want to tie the two projects together. Sequencing them might be better.

Q- Are there any specific thoughts or actions that should be recommended? Joint meetings at face-to-face sessions? Or teleconferences? If so, when? And what would the agenda be? Technical discussions? Or more about process, procedures, and update sharing?

A- The only thing I would add is that if we hold joint sessions, then both TGs need to report on where they are at, otherwise we can’t tell if we are treading on each other’s toes. The other thing is to raise areas of specific concern. Those are the only reasons for having a joint meeting.

A- I don’t think we need formalization of the relationship. Both chairs and groups are flexible. If there’s an issue of concern in one group, I don’t see the other refusing to deal with it. Having a formal review puts a lot of work on the chairs. Anyone is free to institute a joint meeting for topics that go across both groups. I’d like the joint meeting to be on demand.

A- Because the groups overlap, a uniform solution will be more efficient. We should have joint sessions on the overlap areas. As for the timeslot, one or two can be set up, depending on many topics are to be raised.

A- I’m not sure we need joint review meetings. That sounds very strange. Everything being done in both groups is open. Anyone can look at the documents of each. I don’t want to schedule more meetings just to share things.

C- It probably makes sense for the chairs to determine if there are enough topics in common that justify a joint meeting.

C- If you’re going to have joint meetings, there should be a status report, but I don’t mean to imply that a joint meeting is needed. But if you have one, then a formal start is needed. I’m not particularly supporting joint meetings at all but getting everyone on the same page is a good way to start one.

C- I’d like to see a joint meeting if there is an overlap, but it’s hard to know when there’s one. Frequently each group points at the other to solve a problem, but it’s not clear between the groups that there’s mutual pointing going on.

C- That’s something that the chairs need to recognize. And if they don’t, then members should bring it to their attention.

C- If both chairs notice a topic being kicked back and forth, then they can schedule it to be discussed, but I’ve not seen a lot of this kicking back and forth even happening. So, a joint meeting needn’t be scheduled on a regular basis.

C- A couple of times, it was brought up that there might be solutions applicable to both projects. The proponents might want to bring the synergy to the attention of both groups. That seems like the most productive purpose. We don’t need a joint session unless that’s the case. Then the chairs can arrange a joint meeting to let both groups hear it. This could be a joint teleconference. I’d prefer that those are used for technical work, not formalized status briefings.

C- There’s device identification in TGbh. Some members want that ID to be protected. That would seem to be something that TGbi would be interested in too.

C- I don’t remember much of a specific case of this. I do remember mentioning TGbi requirements in the area, but not specific solutions being discussed.

C- Rather than rehashing history, if someone sees a situation that should be handled with a joint meeting, raise it.

C- Any other thoughts on having demand-driven joint meetings?

[None.]

C- I’d love to hear if it anyone has a common solution for TGbh and TGbi.

**Meeting adjourned at 2:49 p.m. EST.**