Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, January 10, 2023Randomized and Changing MAC addresses (RCM) |
| Date: 2023-01-10 |
| 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 January 10, 2023.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting January 10, 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 9:32 a.m. EST.**

Agenda slide deck [11-23/0029r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0029-00-00bh-agenda-tgbh-2023-jan-10.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 24)
	+ Teleconference plan, going forward (slide 17)
* **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:** [**11-22/0973r13**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record:** [**11-22/0651r9**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Contributions (slide 16)**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Timeline**

The timeline currently indicates an initial WG letter ballot on a Draft 1.0 of the IEEE 802.11bh specification coming out of the March 2023 plenary meeting. How likely that is to happen will be a function of getting specification text locked down and an agreeing on the way forward. That latter part has been the problematic part of the equation to date.

1. **Teleconference time discussion**

It doesn’t seem like Thursday evening teleconferences are getting as many people to attend. A decision on whether to continue those meetings will take place during next week’s interim meeting.

1. **Clarification of Requirements**

Graham Smith (SR Technologies) presented [11-22/2150r02](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-02-00bh-clarification-of-requirements.pptx) on “Clarification of Requirements”. He highlighted text from the PAR that should be driving the work of the task group. The privacy provided by RCM must not be lessened, but it is a question as to whether it has to go beyond that. Smith gave the historical context from whence RCM arose. RCM was introduced in IEEE 802.11aq, which randomizes MAC addresses when roaming, but uses the same MAC address when returning to a known ESS. A spoofed AP would cause a non-AP STA to use the same MAC address as it would with a real AP, thus allowing some level of tracking, but it does not grant any access. Smith believes use of the same MAC address is too weak.

C- I think we need to return to this discussion. Passive scanners easily find a STA, but IEEE 802.11aq was designed around spoofed APs. But just use a random MAC address for Probe frames. There’s a difference between spoofed APs and other active attacks. I don’t care to solve the paparazzi case. Some different attacks using a spoofed AP may be worth dealing with – those in which the AP takes some action based on the MAC address prior to full authentication. Any mechanisms we provide should be able to foil active attacks of this type. Detecting device arrival should be based on a post-association status. Even single-use MAC addresses don’t suffice if there are certain cases in which they are reused. As to whether using the same MAC address for the same ESS is too weak, I don’t agree. But it is debatable whether MAC address reuse for the same ESS is done with user consent.

C- Using the same MAC address in a specific ESS has drawbacks. We might augment that with some additional features.

C- I see you spent several slides on spoof AP. IEEE 802.11bh is focused on returning STA identification without revealing its identifier unnecessarily. My own presentation will provide some additional thoughts.

C- In the paparazzi case, searching for the network can use any address. By the time the actual MAC address is detected when a STA attempts to connect to a spoofed AP, the paparazzi are very likely in visual range owing to the limited propagation range of IEEE 802.11. It doesn’t seem like a worthwhile attack to protect against. For a child returning home, the network doesn’t let them on without authentication. With a PSK, then STA differentiation would likely be for a different, higher-layer identity and authentication. Spoofing an AP might be an issue beyond IEEE 802.11bh. Also, most portable devices could be tracked by cellular technology as well.

Smith then addressed the complication of pre-schemes. If using the same MAC address when returning to the same ESS is acceptable, how much more complicated does an IEEE 802.11bh solution have to be? Currently, there are several pre-schemes: MAAD, IEEE 802.11aq, RRCM, IRMA, ID encoding, etc. The first two do not require much computing to employ, while the others use cryptographic mechanisms. There’s some level of memory required to retain the MAC address used when returning to an ESS in IEEE 802.11aq, which may be similar to other pre-schemes except that those pre-schemes change the remembered value with every association. Smith asks for a decision: 1) Do nothing; 2) adopt MAAD or similar non-computation scheme, or 3) adopt a more complex scheme. Decision making will take place during next week’s interim meeting.

C- IEEE 802.11aq doesn’t require the use of the same MAC address every time. That is, however, how many RCM implementations work. In any case, I don’t find MAAD to provide much benefit. That would mean we do nothing or something more complex. And I don’t find the complex schemes worthwhile. So that leaves us with providing guidance on IEEE 802.11aq. So far, I’ve not heard justification for doing more. We should pick the simplest possible solution. We should not promote access control schemes that provide no security.

C- I’m dead against keeping IEEE 802.11aq and simply codifying the current practice of using the same MAC address with the same ESS. The MAAD scheme gives a step up in protection.

C- IEEE 802.11bh has already proposed Device ID, in which the ID is held in the KDE. Most members think we should cover pre-association identification schemes. Device ID is easy because the security context is already in place. But for pre-schemes, we need a security context. As for complexity, look at DPP, which WFA has approved. It’s very complex and yet it’s acceptable.

C- The level of complexity is a question for the STA implementers and to a lesser extent the AP implementers.

C- We can vote during the next meeting and then move forward based on that.

C- I support a straw poll to cover the way forward. I don’t know how much we should focus on complexity in IEEE, but there is a concern where we may end up specifying something that STA vendors aren’t interested in implementing. I’m not saying we stop doing what we think is right, but there is a risk that that work will be moot.

1. **Use cases discussion (OWE mode)**

Jay Yang (Nokia) briefed [11-23/0022r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0022-00-00bh-use-case-for-owe-mode.pptx). OWE (Opportunistic Wireless Encryption) is defined in [RFC 8110](https://www.rfc-editor.org/rfc/rfc8110) to enhance the privacy of users connecting to public Wi-Fi hotspots. Currently, IEEE 802.11bh specifies a network-generated ID that is supplied during the 4-way handshake. Yang suggests a combination of the two, but he notes that this would then require that a STA be able to determine if an AP is a fake before providing the Device ID. Otherwise, the combination is susceptible to a man-in-the-middle attack.

Q- Is the requirement for granting a new device ID per association in the current specification? And I agree with your concerns about OWE.

A- OWE, as the name implies, is not authenticated. Whatever is exchanged in the 4-way handshake is open to spoofing attacks. I’m not sure this is something we need to solve. But then again, Device ID is in our draft and relies on the 4-way handshake. How a STA recognizes a real AP is not detailed in this presentation. I don’t see an easy way to do that either. I’m not ready to support a straw poll about solving this “problem” without further information as to its feasibility. Sure, we should make it clear that when OWE is used, Device ID should not be, because the real requirement for Device ID is not the 4-way handshake, but establishment of an RSN. I don’t want to commit to doing something that’s infeasible.

C- [11-22/1079r08](https://mentor.ieee.org/802.11/dcn/22/11-22-1079-08-00bh-cr-for-sta-generated-id.docx), option 2 might be worth reviewing.

C- This is an open network case. It’s not something we should be looking at. The AP recognizes the STA only because it possesses the PSK, but it doesn’t care about the STA ID. The STA doesn’t even have to recognize the AP. How far are you prepared to protect a Device ID on an open network?

C- IEEE 802.11bh is supposed to focus on recognizing returning STAs. In the current Device ID, we always assume the AP has the password. Why don’t we allow Device ID to be applied in OWE networks?

Q- I’m struggling to understand why pretending to be a particular STA matters in an OWE network. Why do it?

Q- It would be useful to give the high-level use case where Device ID would be used in Open networks. We decided early on that it would be limited to RSN. Let’s just say that you shall not use Device ID in OWE networks. Or add a statement that if you do in fact use Device ID and OWE together, the Device ID is subject to attack. But really, what is the use case? Without that, we shouldn’t spend more effort on this.

A- The specification supports many implementations. Why wouldn’t an Open AP want to identify returning users?

C- I would use Passpoint in that case. OWE is not the right answer. OWE is used when you don’t care about the identity of the STA. That’s not what it’s all about. There’s no authentication in OWE. You never authenticate a STA in the first place, so you have no way of knowing who it is, going forward either. I have never heard of OWE being deployed either, although Open networks are not allowed in the 6 GHz band. Some non-IEEE 802.11 specifications do mandate use of OWE.

Q- But why not make it more secure?

Q- Are you thinking of a captive portal sitting behind an OWE network?

A- Yes.

Q- Does user consent (opt-in) play into this? Then the user chooses whether his STA identification is used to simplify returning to the open network.

A- Yes, but we can do better than that and give a better experience.

C- I’m persuaded that I’ll spoof an AP at Starbucks to get a free coffee.

The straw poll will be run during the interim meeting next week.

C- We probably need more discussion of the use case to inform that straw poll.

1. **Identifier status code**

Kurt Lumbatis (ARRIS/CommScope) introduced [11-22/2186r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2186-00-00bh-device-identifier-status-codes.pptx). This was written in response to an earlier decision that we needed a status field in the Device ID element. The status field indicates success, not recognized, or a request a new text-based identifier. The element is sent by both APs and STAs, hence the mixing of actual status and a request in one field. The request could also be for a MAAD address, if that’s of interest.

Q- We decided that if a STA came in with an incorrect ID, then the AP would provide a new one. So, now we are saying we will give you a new one and a status?

A- We decided recently that we don’t have to give a new ID but rather indicate a lack of recognition.

C- I don’t recall that being the case.

C- There was a request to add a status field because you couldn’t tell the difference between “identifier not recognized” and identifier rotation.

C- I extended that status code field to allow specification of the type of identifier desired.

C- If a STA is given a new ID, so what? You’ll soon know if you have been recognized because the upper layer becomes active and provides service. If the upper layer doesn’t recognize the STA, it will do something different. The cases can be differentiated.

C- With a status code, we can put a lot of information here. To keep it simple, just success/not recognized would work. If the group wants, we can add the ability to request other identity types. The status code should be sent from the AP to STA. I’m not sure about STA to AP.

C- The same element is used in both directions, so we can’t define the status code separately as being for AP to STA only.

C- The STA could just send Success/NoOp always.

C- Or we make it optional and clarify that it’s only sent in one direction.

C- I would prefer to have one ID and one KDE. I’m fine with an optional present field, but add a control field rather than doing this based on what frame it is in. I think it’s simpler to just sent Success/NoOp when it doesn’t matter.

C- I can make a text submission next week based on today’s discussion.

C- It’s not clear you have enough direction from the group on what to do in the STA-to-AP case.

C- Sending 0 is simple.

**Meeting adjoined at 11:31 a.m. EST.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 01/10 | Ansley, Carol | Cox |
| TGbh | 01/10 | Baron, Stéphane | Canon |
| TGbh | 01/10 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 01/10 | Halasz, Dave | Morse Micro |
| TGbh | 01/10 | Levy, Joseph | InterDigital |
| TGbh | 01/10 | Lumbatis, Kurt | ARRIS/CommScope |
| TGbh | 01/10 | Malinen, Jouni | Qualcomm |
| TGbh | 01/10 | Montemurro, Mike | Huawei |
| TGbh | 01/10 | Mutgan, Okan | Nokia |
| TGbh | 01/10 | Orr, Stephen | Cisco |
| TGbh | 01/10 | Petrick, Al | InterDigital |
| TGbh | 01/10 | Riegel, Max | Nokia |
| TGbh | 01/10 | Sam, Harvey | Broadcom Corporation |
| TGbh | 01/10 | Sevin, Julien | Canon |
| TGbh | 01/10 | Smith, Graham | SRT Wireless |
| TGbh | 01/10 | Smith, Luther | CableLabs |
| TGbh | 01/10 | Thakur, Sidharth | Apple |
| TGbh | 01/10 | Yang, Jay | Nokia |
| TGbh | 01/10 | Yee, Peter | NSA-CSD |