Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, June 21, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-6-21 |
| 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 June 21, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting June 21, 2022 10.00 to 12.00 ET**

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

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

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

**Secretary: Peter Yee, acting**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 10:03 a.m. EDT.**

Agenda slide deck [11-22/0910r01](https://mentor.ieee.org/802.11/dcn/22/11-22-0910-01-00bh-agenda-tgbh-2022-june-21.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
	+ Reminder: Comment Collection on D0.2 closes on June 29
* Issues Tracking: [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* Contributions (slide 16)
* Next meetings:
	+ June 28 10:00 ET
	+ July plenary (4 slots)

Any comments? None

Any objections to agenda? None

Agenda accepted unanimously.

1. **Organization topics**

The Comment Collection is now under way and closes on June 29.

1. **Issues Tracking**

The Chair noted that the Issues Tracking document is at r37.

1. **Multiple Schemes for TGbh**

Graham Smith presented [11-22/0908r01](https://mentor.ieee.org/802.11/dcn/22/11-22-0908-01-00bh-multiple-schemes-for-tgbh.pptx), which looks at how multiple solutions would work together. It covers NGID, MAAD, and IRM. It could be expanded to more solutions.

C- I don’t think having the STA select a MAC address is a good idea because of the possibility of a collision in the namespace. If the AP doesn’t own the namespace, two stations could choose the same MAC address. If the STA doesn’t trust the AP to choose a MAC address, the STA should go somewhere else. I don’t believe adding IRMA solves anything and actually causes a problem.

A- I accept your points. This is covered in Case 1.

Q- The PAR says that any solution should not decrease the users’ privacy. MAAD could allow the use of the same MAC twice, decreasing privacy.

A- The address is used for the probe and association, but not further reused.

C- It’s easy to track by a third party. In one association.

A- We are not dealing with changing MAC addresses post association.

C- The requirements indicate that probe and association could use different addresses.

C- I don’t know how the rule-based stuff could fit into your presentation, but it might.

C- The proposal gets the TG to decide whether the AP or the STA is in control of the address.

Q- If we leave the address control up to the STA, we have the concern about address duplication. Is that a problem we feel that we should be trying to solve? Currently, client devices do randomized address changes already and the STAs choose their random addresses however they do it. In the TIG, we discussed the odds for an address collision.

A- It did come up in IEEE 802.11aq and was deemed highly unlikely.

C- It is unlikely, even with 30,000 simultaneous connections. The bigger problem is poor STA implementations that end up raising the odds of a collision.

C- MAC addresses provided by the network is more systematic. It’s not just MAC address clashes, but also who owns and provides the service. The service being provided is remembering the device. That’s on the network. It’s very natural for the network to define the structure of that identifier. This model is no different than a web server with clients being connected and remembered through cookies. Clients don’t generally dictate the format of their cookies either. I wouldn’t be surprised if down the road, the AP puts structure in the IDs it provides, private to the AP. This would have nothing to do with identifying the device but would be something internal to the operation of the network. Pre-association identification works well this way. DMG probe requests/responses require beamforming. So, that requires control frames being sent to measure the best energy, before the actual probe request/response. That’s a pure waste of time for STAs the AP doesn’t want to interact with. Having the ability to know the STA’s ID during beamforming would be a great timesaver.

Payam Torab to consider giving a presentation on the above point.

Straw Poll 1: Given that multiple schemes can be easily be accommodated, should TGbh include more than one scheme in the Draft such that, for example, pre-association use cases may be addressed?

Y: 17

N: 3

A: 2

Straw Poll 2: On the understanding that some non-AP STAs may not want to have their MAC Address allocated for them, but others are OK with that, should TGbh include a “pre-association” scheme where the non-AP STA can choose its MAC address?

Y: 10

N: 7

A: 6

1. **Rule-based Random MAC-Identification proposal (RRCM)**

Okan Mutgan (Nokia) showed [11-22/0818r04](https://mentor.ieee.org/802.11/dcn/22/11-22-0818-04-00bh-use-case-further-discussion-and-rule-based-random-mac-identification-proposal.pptx). The current draft does not cover identification for probing and authentication/(re)association. This scheme has the STA and AP generate one or more random MAC address(es), which can be used for different purposes. The authors of the proposal have slightly modified it based on previous input from the task group. Updated proposed draft text can be found in [11-22/0888r02](https://mentor.ieee.org/802.11/dcn/22/11-22-0888-02-00bh-proposed-text-for-rule-based-random-mac-identification.docx). PKBDF2 is replaced with KDF-Hash-256. The key hierarchy is somewhat altered. AES-CTR mode has been replaced with KDF-Hash-48. Tags are no longer used.

Q- Is the same key (RMAK) used for all future associations?

A- No, because a new PTK is generated per association, so a new RMAK is generated too.

Q- You generate more than one key so that probe requests can use different keys. If the STA is just searching for an AP, it can use any (random) MAC address. Once it finds that AP, it can then use a recognizable address to associate. I’m not convinced that a STA needs to use a recognizable address until it finds an AP of interest, then it can use such an address.

A- If a STA is not associated to an AP, it can send broadcast messages for probes. In certain cases, STAs may still send broadcast messages when connected to an AP. For example, if they want to connect to a different AP, they could notify multiple APs of their desire, using a recognizable address.

Q- Is the broadcast address meant to be the RA address for the probe or the SSID?

A- It’s the wildcard address.

C- IRMA did something like this (except for being STA controlled), but people complained about the amount of computations done per association. If the group has changed its mind on computational costs, IRMA should be reconsidered.

C- IRMA is still more computationally intensive.

Straw Poll: Do you agree the proposed text in 11-22/0888r02 should be incorporated into TGbh Amendment?

Y: 7

N: 5

A: 10

Q- The text in the above proposal is based on REVme’s draft. Should it not be based on TGbh Draft 0.2?

A- I had not looked at it that way, but we wanted to get an idea if it was worth doing any such changes if the group was interested in the proposal.

**Meeting adjoined at 11: a.m. ET.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 6/21 | Andersdotter, Amelia | Sky UK group |
| TGbh | 6/21 | Ansley, Carol | Cox |
| TGbh | 6/21 | Baron, Stephane | Canon Research Centre France |
| TGbh | 6/21 | De la Oliva, Antonio | InterDigital, UC3M |
| TGbh | 6/21 | Kain, Carl | US DOT; Nobis |
| TGbh | 6/21 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 6/21 | Harkins, Dan | HPE |
| TGbh | 6/21 | He, Dingjun |  |
| TGbh | 6/21 | Henry, Jerome | Cisco |
| TGbh | 6/21 | Jiang, Yiming | Nokia |
| TGbh | 6/21 | Levy, Joseph | InterDigital |
| TGbh | 6/21 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 6/21 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 6/21 | Mutgan, Okan | Nokia |
| TGbh | 6/21 | Nezou, Patrice | Canon Research Centre France |
| TGbh | 6/21 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 6/21 | Petrick, Al | InterDigital |
| TGbh | 6/21 | Riegel, Max | Nokia |
| TGbh | 6/21 | Sam, Harvey | Broadcom Corporation |
| TGbh | 6/21 | Sevin, Julien | Canon Research Centre France |
| TGbh | 6/21 | Smith, Graham | SRT Wireless |
| TGbh | 6/21 | Smith, Luther | CableLabs |
| TGbh | 6/21 | Thakore, Darshak | CableLabs |
| TGbh | 6/21 | Thakur, Sid | Apple |
| TGbh | 6/21 | Torab, Payam | Meta |
| TGbh | 6/21 | Yang, Jay | Nokia |
| TGbh | 6/21 | Yee, Peter | NSA-CSD |