

Liaison Statement from IEEE 802.11 Working Group to Wireless Broadband Alliance

Source: IEEE 802.11 Working Group¹ January 2024

Date: 2024-01-04

To: Bruno Tomas CTO, Wireless Broadband Alliance
bruno@wballiance.com

CC: Alpesh Shah Secretary, IEEE-SA Standards Board, Secretary,
IEEE-SA Board of Governors sasecretary@ieee.org

Paul Nikolich Chair, IEEE 802 LMSC p.nikolich@ieee.org

Jon Rosdahl Vice-chair, IEEE 802.11 WLAN Working Group
jrosdahl@ieee.org

Robert Stacey Vice-chair, IEEE 802.11 WLAN Working Group
robert.stacey@intel.com

Mark Hamilton Chair, IEEE 802.11bh Task Group
mark.hamilton2152@gmail.com

From: Dorothy Stanley Chair, IEEE 802.11 WLAN Working Group
dorothy.stanley@hpe.com

Subject: **Reply to WBA re: P802.11bh activities on randomized and changing MAC addresses**

Dear Bruno and WBA members,

Thank you again for the liaisons sent to us over the last two years:

- a) "Liaison Statement to IEEE 802.11", WBA Wi-Fi Devices Identification Group, 04/14/2023, <https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx>
- b) "Wi-Fi Devices Identification, A Way Through MAC Randomization", WBA Wi-Fi Devices Identification, March 2022
- c) "Liaison Statement to IEEE 802.11", WBA Wi-Fi Devices Identification Group, 02/23/2022, <https://mentor.ieee.org/802.11/dcn/22/11-22-0668-00-0000-liaison-statement-from-wba-re-wi-fi-devices-identification-group.pdf>
- d) "Wi-Fi Identification Scope, In a post MAC Randomization Era", WBA Testing & Interoperability Work Group, April 2021

This liaison communication provides an update on the P802.11bh mechanisms being proposed in P802.11bh Draft 1.0 and a description of the applicability of these mechanisms to the use cases and scenarios described in the received liaisons from the WBA.

The P802.11bh D1.0, "Randomized and Changing MAC Addresses" amendment is under

¹ This document represents the views of the IEEE 802.11 Working Group and does not necessarily represent a position of the IEEE, the IEEE Standards Association, or IEEE 802.

development and defines two mechanisms, *Device ID* and *Identifiable Random MAC address (IRM)* that enable private device identification of IEEE 802.11 STAs that use a randomized or changing MAC address. Each mechanism is independently optional. Either or both mechanisms may be supported by the non-AP STA and by the network.

Device ID: An AP may provide an identifier to a non-AP STA and the non-AP STA may opt-in to providing that identifier to any AP in the same ESS to allow the network to recognize the same non-AP STA when it returns to the ESS even if the non-AP STA changes its MAC address. Exchange of the Device ID information is protected from third parties to limit the tracking capability to the APs in an ESS.

Identifiable Random MAC Address (IRM): A non-AP STA may provide a random MAC address to an AP either when it associates or when it performs PASN authentication. The non-AP STA may then use that IRM MAC address as its Transmitted Address (TA) when it returns to that ESS or AP such that the non-AP STA may be identified pre-association.

Eleven (11) use cases were defined in the WBA Wi-Fi Devices Identification document, and we believe that eight (8) of the use cases are in scope of IEEE P802.11bh (note that the numbering used below is from the WBA document):

1. Private home network access restrictions / privileges (including parental controls, per-device, or per-user QoS) For Pay-per-Use networks - identification of complementary and paid-up users or devices.
2. IP Address allocation in private, public and enterprise networks.
3. Private home network device diagnostics and performance monitoring enterprise network or device diagnostics and performance monitoring.
4. Private home networks and enterprise networks band steering with multi-ESS networks (e.g., split-SSID installations)
5. Hospitality and venue network access with varying service levels
6. Pay-per-use network access.
7. Operators' public networks block devices that have expired or invalidated credentials and rapidly and repeatedly reattempt to connect.
10. Networks, typically using 802.1X, that use the device MAC to tie devices to certificates for certificate enrolment.

The following three (3) use cases are believed to be out of scope of IEEE P802.11bh:

8. Network blocks devices due to abusive behavior or upon lawful demand.
9. Passpoint networks record the acceptance of T&Cs on the AAA.
11. Any network operator responding to requests for communications records, lawful interception, and other law enforcement purposes.

A copy of the IEEE P802.11bh D1.0 draft is provided together with this liaison document for your review. The draft is also available at https://www.techstreet.com/ieee/standards/ieee-p802-11bh?product_id=2569955 .

We welcome your comments on the P802.11bh D1.0 draft, preferably prior to the next IEEE 802.11 meeting January 15th-19th 2024. We would also appreciate any comments on how the mechanisms defined in the draft map to the concerns raised in the liaison documents.

See http://www.ieee802.org/11/Meetings/Meeting_Plan.html for future meeting dates of the IEEE 802.11 Working Group. The most recent version of the IEEE 802.11 standard is [IEEE Std 802.11™-2020](#).

Best Regards,

Dorothy Stanley

Contact information:

Dorothy Stanley

IEEE 802.11 Working Group Chair

dorothy.stanley@hpe.com

+1 630 363 1389