IEEE P802.11
Wireless LANs

|  |
| --- |
| P802.11bh and P802.11bi Press release/Blog post |
| Date: 2021-05-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | HP Enterprise | 3333 Scott BlvdSanta Clara, CA 95054 | +1 630-363-1389 | dstanley@ieee.org  |
|  |  |  |  |  |

Abstract

This document contains the draft blog post/press release related to establishment of the P802.11bh and P802.11bi projects, prepared by IEEE staff together with subject matter experts: Mark Hamilton, Peter Yee, Stephen Orr (P802.11bh Chair and Vice chairs) and Carol Ansley, Stephen McCann, and Jerome Henry (P802.11bi Chair and Vice chairs).

This document is posted for 802.11 WG information and EC comment and approval.

**Data Privacy and Ease-of-Use in Wireless Networks**

How Two New IEEE 802.11 Standardization Projects Aim to Strike the Balance

Wireless technology has evolved enormously since the 1999 Macworld trade show, at which Apple CEO Steve Jobs introduced Apple’s AirPort wireless base station and iBook—the first Wi-Fi products widely marketed to consumers enabled by the [IEEE 802.11b™ Standard](https://standards.ieee.org/standard/802_11b-1999.html?utm_source=beyondstandards&utm_medium=post&utm_campaign=working-group-2021&utm_content=802). They were a great success, and PC vendors soon followed suit, sparking a revolution in wireless technology.

In the more than two decades since, devices that incorporate [IEEE 802.11™ Wireless LAN Standards](https://beyondstandards.ieee.org/tag/wg-ieee-802-11/) have become ubiquitous, and conformance to the standards has become indispensable because of the robust, reliable, and affordable network connectivity it offers.

Today, the evolution of wireless systems has brought privacy concerns to the forefront driven by user demand and GDPR requirements. The global wireless industry is faced with the growing need to protect users’ personally identifiable information from increasingly sophisticated user-tracking and user-profiling activities, while continuing to improve wireless services and the user experience.

Striving to address this challenge, IEEE Standards Association (IEEE SA) has formed two standardization projects within the IEEE 802.11 Wireless LAN Working Group:

* [IEEE P802.11bh™, Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Operation with Randomized and Changing MAC Addresses](https://standards.ieee.org/project/802_11bh.html?utm_source=beyondstandards&utm_medium=post&utm_campaign=working-group-2021&utm_content=802)
* [IEEEP802.11bi™, Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Enhanced Service with Data Privacy Protection](https://standards.ieee.org/project/802_11bi.html?utm_source=beyondstandards&utm_medium=post&utm_campaign=working-group-2021&utm_content=802)

**How Does MAC Address Randomization Affect the User Experience?**

Behind the formation of these projects is the growing trend to randomize MAC (media access control) addresses to alleviate tracking of users through their devices. In networking, a device’s MAC address identifies the device to a network, enabling the network to give it access. Device manufacturers typically assign, or “burn-in,” a globally-unique, hardware-based MAC address during manufacturing.

For years, these globally-unique and static MAC addresses have worked well. But with today’s more sophisticated data-gathering, pattern-matching, and information analysis techniques, a static MAC address may allow an outside entity to more easily identify a particular device and track its location.

Because alternate MAC addresses can be created in software to mask the original burned-in one, some device manufacturers have begun to use this technique to randomize a device’s MAC address, or regularly change it, to make data-gathering and analysis by outside entities more difficult.

However, while this does increase user privacy, it also leads to potential connectivity issues and possible disruption of the user experience. An example is when users wish to make use of a public Wi-Fi network in a coffee shop, doctor’s office, or elsewhere. Because many captive portals use static MAC addresses as identifiers, the user may need to log-in repeatedly and re-submit information as their MAC address changes. In other cases, the user may need to authenticate and log-in again when the device idles, disconnects, and reconnects via a different MAC address.

Another example is when families set parental controls on children’s devices for screen time and content. These limits are often enforced by a device’s MAC address, and if the address changes, the controls may no longer apply.

Network operators, too, may experience challenges, because continually changing device identifiers makes it difficult for operators to understand such things as whether a user is legitimate or how many devices are actually connected to a network at a given time, to apply advanced network analytics and troubleshooting, or to maintain control of their networks and users for business purposes.

**Wireless Network Privacy Issues**

In addition to the simple tracking of a user’s MAC address, data-gathering can also enable derivation of locations, movements, and contacts. Although the tracking of other aspects of the wireless signaling protocol are less obvious, nonetheless this can still be achieved.  Big data approaches enable the detection of patterns in the wireless communications, resulting in a trail of “electronic fingerprints” wherever users go.

This information can be exposed to third-party actors who passively monitor the radio links and decode exposed information. Users are less likely to be aware that some information is also visible and at times even intentionally provided to operators of “visited” networks, such as hotspots, hospitality networks, retail stores, and others.

**How Will IEEE 802.11 Standards Address the Challenge?**

The two new IEEE 802.11 projects are charged with defining changes or additions to specifications in two related areas:

* **IEEE P802.11bh** considers short-term issues related specifically to MAC address randomization, and quickly develops (i.e., in 18-24 months) an amendment to IEEE 802.11 that addresses them. The goal is to preserve the efficiency of existing services that might otherwise be restricted, such as network support, diagnostics and troubleshooting, and to reliably detect a device’s arrival in a trusted network environment. IEEE 802.11bh will also design mechanisms to optimize the user experience when a device’s MAC address is changing.

* **IEEE P802.11bi** considers privacy concerns, beyond MAC address randomization, from a broader, longer-term perspective. It will address and standardize privacy solutions to prevent tracking of a user location and movement. It will build on the work already done for IEEE 802.11aq-2018, which also addressed privacy concerns as a part of its work.

**Get Involved**

Today, IEEE 802.11 standards have become integral to our everyday life, enabling wireless communications in the office, at home, and on the road. As the standards continue to evolve to serve critical and urgent demands from industry and consumers, we welcome engineers, individuals concerned with privacy, and those who have already participated in IEEE 802.11 development globally, from both industry and academia, to join the projects and contribute their knowledge and talents to the advancement of wireless networking standards.

[**Learn more about IEEE 802.11 standards and get engaged with us**](https://standards.ieee.org/featured/802/index.html?utm_source=beyondstandards&utm_medium=post&utm_campaign=working-group-2021&utm_content=802#get-involved)**.**

###

**References:**