Stream: Internet Engineering Task Force (IETF)
RFC: 9724
Category: Informational
Published: January 2025
ISSN: 2070-1721
Authors: JC. Zúñiga, *Cisco*; CJ. Bernardos, Ed., *UC3M*; A. Andersdotter, *Safespring AB*

RFC 9724
State of Affairs for Randomized and Changing Media Access Control (MAC) Addresses

Abstract

Internet users are becoming more aware that their activity over the Internet leaves a vast digital footprint, that communications might not always be properly secured, and that their location and actions can be tracked. One of the main factors that eases tracking of Internet users is the wide use of long-lasting, and sometimes persistent, identifiers at various protocol layers. This document focuses on Media Access Control (MAC) addresses.

There have been several initiatives within the IETF and the IEEE 802 standards committees to address some of the privacy issues involved. This document provides an overview of these activities to help coordinate standardization activities in these bodies.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9724.

Copyright Notice

Table of Contents

1. Introduction

Privacy is becoming a huge concern, as more and more devices are connecting to the Internet either directly (e.g., via Wi-Fi) or indirectly (e.g., via a smartphone using Bluetooth). This ubiquitous connectivity, together with the lack of proper education about privacy, makes it very easy to track/monitor the location of users and/or eavesdrop on their physical and online activities. This is due to many factors, such as the vast digital footprint that users leave on the Internet with or without their consent and the weak (or even null) authentication and encryption mechanisms used to secure communications. A digital footprint may include information shared on social networks, cookies used by browsers and servers for various reasons, connectivity logs that allow tracking of a user's Layer 2 (L2) address (i.e., MAC address) or Layer 3 (L3) address, web trackers, etc.

Privacy concerns affect all layers of the protocol stack, from the lower layers involved in the access to the network (e.g., MAC/L2 and L3 addresses can be used to obtain the location of a user) to higher-layer protocol identifiers and user applications [CSCN2015]. In particular, IEEE 802 MAC addresses have historically been an easy target for tracking users [wifi_tracking].

There have been several initiatives within the IETF and the IEEE 802 standards committees to address some of these privacy issues. This document provides an overview of these activities to help coordinate standardization activities within these bodies.

2. Background

2.1. MAC Address Usage

Most mobile devices used today are Wi-Fi enabled (i.e., they are equipped with an IEEE 802.11 wireless local area network interface). Like any other kind of network interface based on IEEE 802 such as Ethernet (i.e., IEEE 802.3), Wi-Fi interfaces have an L2 address (also referred to as a MAC address) that can be seen by anybody who can receive the radio signal transmitted by the network interface. The format of these addresses (for 48-bit MAC addresses) is shown in Figure 1.

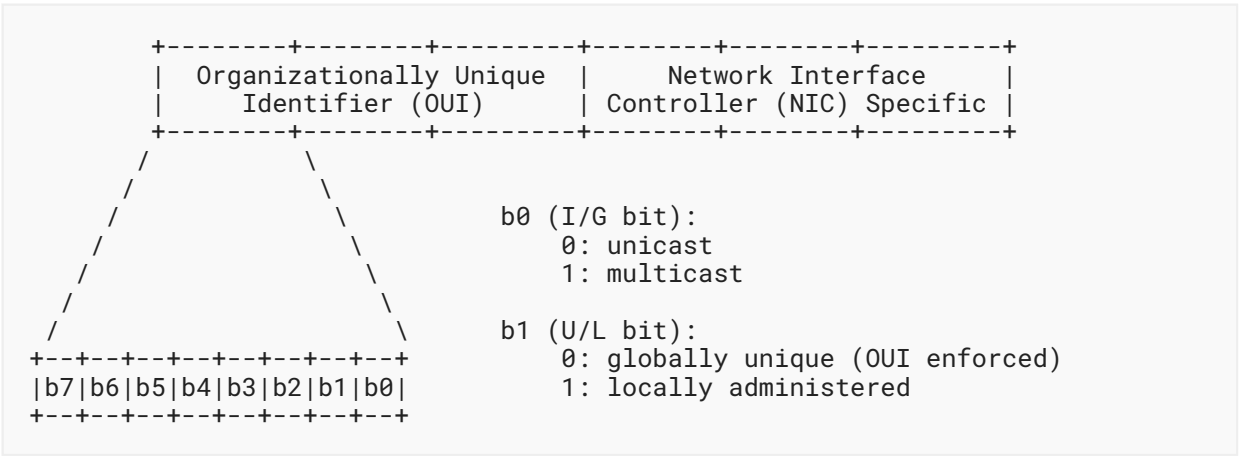

Figure 1: IEEE 802 MAC Address Format (for 48-Bit Addresses)

MAC addresses can be either universally or locally administered. Universally and locally administered addresses are distinguished by setting the second least significant bit of the most significant byte of the address (the U/L bit).

A universally administered address is uniquely assigned to a device by its manufacturer. Most physical devices are provided with a universally administered address, which is composed of two parts:

Organizationally Unique Identifier (OUI): The first three octets in transmission order, which identify the organization that issued the identifier.

Network Interface Controller (NIC) Specific: The following three octets, which are assigned by the organization that manufactured the NIC, in such a way that the resulting MAC address is globally unique.

Locally administered addresses override the burned-in address, and they can be set up by either the network administrator or the Operating System (OS) of the device to which the address pertains. However, as explained in later sections of this document, there are new initiatives in the IEEE 802 and other organizations to specify ways in which these locally administered addresses should be assigned, depending on the use case.

2.2. MAC Address Randomization

Since universally administered MAC addresses are by definition globally unique, when a device uses this MAC address over a shared medium to transmit data -- especially over the air -- it is relatively easy to track this device by simple medium observation. Since a device is usually directly associated to an individual, this poses a privacy concern [link_layer_privacy].

MAC addresses can be easily observed by a third party, such as a passive device listening to communications in the same L2 network. In an 802.11 network, a device (also known as an IEEE 802.11 station or STA) exposes its MAC address in two different situations:

- While actively scanning for available networks, the MAC address is used in the Probe Request frames sent by the device.
- Once associated to a given Access Point (AP), the MAC address is used in frame transmission and reception, as one of the addresses used in the unicast address fields of an IEEE 802.11 frame.

One way to address this privacy concern is by using randomly generated MAC addresses. IEEE 802 addressing includes one bit to specify if the hardware address is locally or globally administered. This allows local addresses to be generated without the need for any global coordination mechanism to ensure that the generated address is still unique within the local network. This feature can be used to generate random addresses, which decouple the globally unique identifier from the device and therefore make it more difficult to track a user device from its MAC/L2 address [enhancing_location_privacy].

Note that there are reports [contact_tracing_paper] of some mobile OSes reporting persistently (every 20 minutes or so) on MAC addresses (as well as other information), which would defeat MAC address randomization. While these practices might have changed by now, it is important to highlight that privacy-preserving techniques should be conducted while considering all layers of the protocol stack.

2.3. Privacy Workshop, Tutorial, and Experiments at IETF and IEEE 802 Meetings

As an outcome to the STRINT W3C/IAB Workshop [strint], a tutorial titled "Pervasive Surveillance of the Internet - Designing Privacy into Internet Protocols" [privacy_tutorial] was given at the IEEE 802 Plenary meeting in San Diego in July of 2014. The tutorial provided an update on the recent developments regarding Internet privacy, the actions undertaken by other Standards Development Organizations (SDOs) like the IETF, and guidelines that were being followed when developing new Internet protocol specifications (e.g., the considerations described in [RFC6973]). The tutorial highlighted some privacy concerns that apply specifically to link-layer technologies and provided suggestions on how IEEE 802 could help address them.

Following the discussions and interest within the IEEE 802 community, on 18 July 2014, the IEEE 802 Executive Committee (EC) created the IEEE 802 EC Privacy Recommendation Study Group (SG) [ieee_privacy_ecsg]. The work and discussions from the group have generated multiple outcomes, such Project Authorization Requests (PARs) that resulted in the following documents:

- "IEEE Recommended Practice for Privacy Considerations for IEEE 802(R) Technologies" [IEEE_802E]
- "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture - Amendment 2: Local Medium Access Control (MAC) Address Usage" [IEEE_802c]

In order to test the effects of MAC address randomization, experiments were conducted at the IETF and IEEE 802 meetings between November 2014 and March 2015 -- IETF 91, IETF 92, and the IEEE 802 Plenary in Berlin. The purpose of the experiments was to evaluate the use of MAC address randomization from two different perspectives: (1) the effect on the connectivity experience of the end user, as well as any effect on applications and OSes, and (2) the potential impact on the network infrastructure itself. Some of the findings were published in [CSCN2015].

During the experiments, it was observed that the probability of address duplication in a network is negligible. The experiments also revealed that other protocol identifiers (e.g., the DHCP client identifier) can be correlated and can therefore still be used to track an individual. Hence, effective privacy tools should not work in isolation at a single layer; instead; they should be coordinated with other privacy features at higher layers.

Since then, MAC address randomization has been further implemented by mobile OSes to provide better privacy for mobile phone users when connecting to public wireless networks [privacy_ios] [privacy_windows] [privacy_android].

3. Activities Relating to Randomized and Changing MAC Addresses in the IEEE 802

Practical experiences with Randomized and Changing MAC addresses (RCM) in devices (some of which are explained in Section 6) helped researchers fine-tune their understanding of attacks against randomization mechanisms [when_mac_randomization_fails]. Within the IEEE 802.11 group, these research experiences eventually formed the basis for a specified mechanism that randomizes MAC addresses, which was introduced in IEEE Std 802.11aq [IEEE_802.11aq] in 2018.

More recent developments include turning on MAC address randomization in mobile OSes by default, which has an impact on the ability of network operators to customize services [rcm_user_experience_csd]. Therefore, follow-on work in the IEEE 802.11 mapped effects of a potentially large uptake of randomized MAC identifiers on a number of commonly offered operator services in 2019 [rcm_tig_final_report]. In the summer of 2020, this work emanated in two new standards projects. The purpose of these projects was to develop mechanisms that do not decrease user privacy but enable an optimal user experience when (1) the MAC address of a device in an Extended Service Set (a group of interconnected IEEE 802.11 wireless access points and stations that form a single logical network) is randomized or changes [rcm_user_experience_par] and (2) user privacy solutions descibed in IEEE Std 802.11 [rcm_privacy_par] apply.

IEEE Std 802 [IEEE_802], as of the amendment IEEE 802c-2017 [IEEE_802c], specifies a local MAC address space structure known as the Structured Local Address Plan (SLAP) [RFC8948]. The SLAP designates a range of Extended Local Identifiers for subassignment within a block of addresses assigned by the IEEE Registration Authority via a Company ID. A range of local MAC addresses is designated for Standard Assigned Identifiers to be specified by IEEE 802 standards. Another range of local MAC addresses is designated for Administratively Assigned Identifiers, which are subject to assignment by a network administrator.

IEEE Std 802E-2020 ("IEEE Recommended Practice for Privacy Considerations for IEEE 802(R) Technologies") [IEEE_802E] recommends the use of temporary and transient identifiers if there are no compelling reasons for a newly introduced identifier to be permanent. This recommendation is part of the basis for the review of user privacy solutions for IEEE Std 802.11 devices (also known as Wi-Fi devices) as part of the RCM efforts [rcm_privacy_csd]. Annex I of IEEE Std 802.1AEdk-2023 ("MAC Privacy Protection") [IEEE_802.1AEdk] discusses privacy considerations in bridged networks.

As of 2024, two task groups in IEEE 802.11 are dealing with issues related to RCM addresses:

- The IEEE 802.11bh task group, which is looking at mitigating the repercussions that RCM addresses create on 802.11 networks and related services.
- The IEEE 802.11bi task group, which is chartered to define modifications to the IEEE Std 802.11 MAC specification [IEEE_802.11] to specify new mechanisms that address and improve user privacy.

4. Recent Activities Related to MAC Address Randomization in the WBA

In the Wireless Broadband Alliance (WBA), the Testing and Interoperability Work Group has been looking at issues related to MAC address randomization and has identified a list of potential impacts of these changes to existing systems and solutions, mainly related to Wi-Fi identification.

As part of this work, the WBA has documented a set of use cases that a Wi-Fi Identification Standard should address in order to scale and achieve longer-term sustainability of deployed services (see [wba_paper]).

5. IPv6 Address Randomization in the IETF

[RFC4862] specifies Stateless Address Autoconfiguration (SLAAC) for IPv6, which typically results in hosts configuring one or more "stable" addresses composed of a network prefix advertised by a local router and an Interface Identifier (IID). [RFC8064] formally updated the original IPv6 IID selection mechanism to avoid generating the IID from the MAC address of the interface (via EUI64), as this potentially allowed for tracking of a device at L3. Additionally, the prefix part of an IP address provides meaningful insights of the physical location of the device in general, which together with the IID based on the MAC address, made it easier to perform global device tracking.

[RFC8981] identifies and describes the privacy issues associated with embedding MAC stable addressing information into IPv6 addresses (as part of the IID). It describes an extension to IPv6 SLAAC that causes hosts to generate temporary addresses with randomized IIDs for each prefix advertised with autoconfiguration enabled. Changing addresses over time limits the window of time during which eavesdroppers and other information collectors may trivially perform address-based network-activity correlation when the same address is employed for multiple

transactions by the same host. Additionally, it reduces the window of exposure of a host as being accessible via an address that becomes revealed as a result of active communication. These temporary addresses are meant to be used for a short period of time (hours to days) and then deprecated. Deprecated addresses can continue to be used for already-established connections but are not used to initiate new connections. New temporary addresses are generated periodically to replace temporary addresses that expire. To generate temporary addresses, a node produces a sequence of temporary global scope addresses from a sequence of IIDs that appear to be random in the sense that (1) it is difficult for an outside observer to predict a future address (or identifier) based on a current one and (2) it is difficult to determine previous addresses (or identifiers) knowing only the present one. Temporary addresses should not be used by applications that listen for incoming connections (as these are supposed to be waiting on permanent/well-known identifiers). If a node changes network and comes back to a previously visited one, the temporary addresses that the node would use will be different, which might be an issue in certain networks where addresses are used for operational purposes (e.g., filtering or authentication). [RFC7217], summarized next, partially addresses the problems aforementioned.

[RFC7217] describes a method to generate IIDs that are stable for each network interface within each subnet but change as a host moves from one network to another. This method enables the "stability" properties of the IIDs specified in [RFC4291] to be kept, while still mitigating address-scanning attacks and preventing correlation of the activities of a host as it moves from one network to another. The method defined to generate the IPv6 IID is based on computing a hash function that takes the following as input: information that is stable and associated to the interface (e.g., a local IID), stable information associated to the visited network (e.g., the IEEE 802.11 Service Set Identifier (SSID)), the IPv6 prefix, a secret key, and some other additional information. This basically ensures that a different IID is generated when one of the input fields changes (such as the network or the prefix) but that the IID is the same within each subnet.

To mitigate the privacy threats posed by the use of MAC-derived IIDs, [RFC8064] recommends that nodes implement [RFC7217] as the default scheme for generating stable IPv6 addresses with SLAAC.

In addition to the documents above, [RFC8947] proposes a DHCPv6 extension that:

> allows a scalable approach to link-layer address assignments where preassigned link-layer address assignments (such as by a manufacturer) are not possible or are unnecessary.

And [RFC8948] proposes DHCPv6 extensions that:

> enable a DHCPv6 client or a DHCPv6 relay to indicate a preferred SLAP quadrant to the server so that the server may allocate MAC addresses in the quadrant requested by the relay or client.

In addition to MAC and IP addresses, some DHCP options that carry unique identifiers can also be used for tracking purposes. These identifiers can enable device tracking even if the device administrator takes care of randomizing other potential identifications like link-layer addresses or IPv6 addresses. [RFC7844] introduces anonymity profiles that are:

> designed for clients that wish to remain anonymous to the visited network

and that:

> provide guidelines on the composition of DHCP or DHCPv6 messages, designed to minimize disclosure of identifying information.

[RFC7844] also indicates that the link-layer address, IP address, and DHCP identifier shall evolve in synchrony.

6. Taxonomy of MAC Address Selection Policies

This section documents different policies for MAC address selection. Some OSes might use a combination of multiple policies.

> Note: The naming convention for the terms defined in this section aligns with 802.11/Wi-Fi terminology in that the "A" for "address" is not included in the acronym. For example, "PVOM" stands for "Per-Vendor OUI MAC address", and "PNGM" stands for "Per-Network Generated MAC address".

6.1. Per-Vendor OUI MAC Address (PVOM)

This form of MAC address selection is the historical default.

The vendor obtains an OUI from the IEEE. This is a 24-bit prefix (including two upper bits that are set specifically) that is assigned to the vendor. The vendor generates a unique 24-bit value for the lower 24 bits, forming the 48-bit MAC address. It is not unusual for the 24-bit value to be used as an incrementing counter that was assigned at the factory and burnt into non-volatile storage.

Note that IEEE Std 802.15.4 [IEEE_802.15.4] uses 64-bit MAC addresses, and the IEEE assigns 32-bit prefixes. The IEEE has indicated that there may be a future Ethernet specification that uses 64-bit MAC addresses.

6.2. Per-Device Generated MAC Address (PDGM)

This form of MAC address is randomly generated by the device, usually upon first boot. The resulting MAC address is stored in non-volatile storage and is used for the rest of the device lifetime.

6.3. Per-Boot Generated MAC Address (PBGM)

This form of MAC address is randomly generated by the device each time the device is booted. The resulting MAC address is **not** stored in non-volatile storage. It does not persist across power cycles. This case may sometimes be a PDGM where the non-volatile storage is no longer functional (or has failed).

6.4. Per-Network Generated MAC Address (PNGM)

This form of MAC address is generated each time a new network attachment is created.

This is typically used with Wi-Fi networks (i.e., 802.11 networks) where the network is identified by an SSID Name. The generated address is stored in non-volatile storage, indexed by the SSID. Each time the device returns to a network with the same SSID, the device uses the saved MAC address.

It is possible to use PNGM for wired Ethernet connections through some passive observation of network traffic (such as spanning tree protocols [IEEE_802.1Q], the Link Layer Discovery Protocol (LLDP) [IEEE_802.1AB], DHCP, or Router Advertisements) to determine which network has been attached.

6.5. Per-Period Generated MAC Address (PPGM)

This form of MAC address is generated periodically, typically around every twelve hours. Like PNGM, it is used primarily with Wi-Fi.

When the MAC address changes, the station disconnects from the current session and reconnects using the new MAC address. This will involve a new 802.1x session, as well as obtaining or refreshing a new IP address (e.g., using DHCP or SLAAC).

If DHCP is used, then a new DHCP Unique Identifier (DUID) is generated so as to not link to the previous connection; this usually results in the allocation of new IP addresses.

6.6. Per-Session Generated MAC Address (PSGM)

This form of MAC address is generated on a per-session basis. How a session is defined is implementation-dependent, for example, a session might be defined by logging in to a portal, VPN, etc. Like PNGM and PPGM, it is used primarily with Wi-Fi.

Since the address only changes when a new session is established, there is no disconnection/reconnection involved.

7. OS Current Practices

By default, most modern OSes (especially mobile ones) do implement some MAC address randomization policies. Since the mechanism and policies that OSes implement can evolve with time, the content is hosted at <https://wiki.ietf.org/en/group/madinas/RFC9724>. For completeness, a snapshot of the content at the time of publication of this document is included below. Note that the extensive testing reported in this document was conducted in 2021, but no significant changes have been detected at the time of publication of this document.

Table 1 summarizes current practices for Android and iOS at the time of writing this document (the original source is available at [private_mac]) and also includes updates based on findings from the authors.

Android 10+	iOS 14+
The randomized MAC address is bound to the SSID.	The randomized MAC address is bound to the Basic SSID.
The randomized MAC address is stable across reconnections for the same network.	The randomized MAC address is stable across reconnections for the same network.
The randomized MAC address does not get re-randomized when the device forgets a Wi-Fi network.	The randomized MAC address is reset when the device forgets a Wi-Fi network.
MAC address randomization is enabled by default for all the new Wi-Fi networks. But if the device previously connected to a Wi-Fi network identifying itself with the real MAC address, no randomized MAC address will be used (unless manually enabled).	MAC address randomization is enabled by default for all the new Wi-Fi networks.

Table 1: Android and iOS MAC Address Randomization Practices

In September 2021, we performed some additional tests to evaluate how OSes that are widely used behave regarding MAC address randomization. Table 2 summarizes our findings; the rows in the table show whether the OS performs address randomization per network (PNGM according to the taxonomy introduced in Section 6), performs address randomization per new connection (PSGM), performs address randomization daily (PPGM with a period of 24 hours), supports configuration per SSID, supports address randomization for scanning, and supports address randomization for scanning by default.

OS	Linux (Debian "bookworm")	Android 10	Windows 10	iOS 14+
Random. per net. (PNGM)	Y	Y	Y	Y
Random. per connec. (PSGM)	Y	N	N	N
Random. daily (PPGM)	N	N	Y	N
SSID config.	Y	N	N	N
Random. for scan	Y	Y	Y	Y
Random. for scan by default	N	Y	N	Y

Table 2: Observed Behavior in Different OSes (as of September 2021)

According to [privacy_android], starting with Android 12, Android uses non-persistent randomization in the following situations:

- A network suggestion application specifies that non-persistent randomization be used for the network (through an API).
- The network is an open network that hasn't encountered a captive portal, and an internal config option is set to do so (by default, it is not).

8. IANA Considerations

This document has no IANA actions.

9. Security Considerations

Privacy considerations regarding tracking the location of a user through the MAC address of a device are discussed throughout this document. Given the informational nature of this document, no protocols/solutions are specified, but the current state of affairs is documented.

Any future specification in this area would need to look into security and privacy aspects, such as (but not limited to) the following:

- Mitigating the problem of location privacy while minimizing the impact on upper layers of the protocol stack
- Providing the means for network operators to authenticate devices and authorize network access, despite the MAC addresses changing according some pattern
- Providing the means for the device not to use MAC addresses that it is not authorized to use or that are currently in use

A major conclusion of the work in IEEE Std 802E [IEEE_802E] concerned the difficulty of defending privacy against adversaries of any sophistication. Individuals can be successfully tracked by fingerprinting, using aspects of their communication other than MAC addresses or other permanent identifiers.

10. Informative References

[contact_tracing_paper] Leith, D. J. and S. Farrell, "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, DOI 10.1109/INFOCOM42981.2021.9488728, May 2021, <https://ieeexplore.ieee.org/document/9488728>.

[CSCN2015] Bernardos, CJ., Zúñiga, JC., and P. O'Hanlon, "Wi-Fi Internet Connectivity and Privacy: Hiding your tracks on the wireless Internet", 2015 IEEE Conference on Standards for Communications and Networking (CSCN), DOI 10.1109/CSCN.2015.7390443, October 2015, <https://doi.org/10.1109/CSCN.2015.7390443>.

[enhancing_location_privacy] Gruteser, M. and D. Grunwald, "Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis", Mobile Networks and Applications, vol. 10, no. 3, pp. 315-325, DOI 10.1007/s11036-005-6425-1, June 2005, <https://doi.org/10.1007/s11036-005-6425-1>.

[IEEE_802] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", IEEE Std 802-2014, DOI 10.1109/IEEESTD.2014.6847097, June 2014, <https://doi.org/10.1109/IEEESTD.2014.6847097>.

[IEEE_802.11] IEEE, "IEEE 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", IEEE Std 802.11-2020, DOI 10.1109/IEEESTD.2021.9363693, February 2021, <https://doi.org/10.1109/IEEESTD.2021.9363693>.

[IEEE_802.11aq] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area network--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery", IEEE Std 802.11aq-2018, DOI 10.1109/IEEESTD.2018.8457463, August 2018, <https://doi.org/10.1109/IEEESTD.2018.8457463>.

[IEEE_802.15.4] IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Std 802.15.4-2024, DOI 10.1109/IEEESTD.2024.10794632, December 2024, <https://doi.org/10.1109/IEEESTD.2024.10794632>.

[IEEE_802.1AB] IEEE, "IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery", IEEE Std 802.1AB-2016, DOI 10.1109/IEEESTD.2016.7433915, March 2016, <https://doi.org/10.1109/IEEESTD.2016.7433915>.

[IEEE_802.1AEdk] IEEE, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security - Amendment 4: MAC Privacy protection", IEEE Std 802.1AEdk-2023, DOI 10.1109/IEEESTD.2023.10225636, August 2023, <https://doi.org/10.1109/IEEESTD.2023.10225636>.

[IEEE_802.1Q] IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks", IEEE Std 802.1Q-2022, DOI 10.1109/IEEESTD.2022.10004498, December 2022, <https://doi.org/10.1109/IEEESTD.2022.10004498>.

[IEEE_802c] IEEE, "IEEE Standard for Local and Metropolitan Area Networks:Overview and Architecture--Amendment 2: Local Medium Access Control (MAC) Address Usage", IEEE Std 802c-2017, DOI 10.1109/IEEESTD.2017.8016709, August 2017, <https://doi.org/10.1109/IEEESTD.2017.8016709>.

[IEEE_802E] IEEE, "IEEE Recommended Practice for Privacy Considerations for IEEE 802(R) Technologies", IEEE Std 802E-2020, DOI 10.1109/IEEESTD.2020.9257130, November 2020, <https://doi.org/10.1109/IEEESTD.2020.9257130>.

[ieee_privacy_ecsg] IEEE 802 LAN/MAN Standards Committee, "IEEE 802 EC Privacy Recommendation Study Group", <http://www.ieee802.org/PrivRecsg/>.

[link_layer_privacy] O'Hanlon, P., Wright, J., and I. Brown, "Privacy at the link-layer", W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT), February 2014.

[privacy_android] Android Open Source Project, "MAC randomization behavior", Android OS Documentation, <https://source.android.com/devices/tech/connect/wifi-mac-randomization-behavior>.

[privacy_ios] Apple Inc., "Use private Wi-Fi addresses on Apple Devices", Apple Support, <https://support.apple.com/en-us/102509>.

[privacy_tutorial] Cooper, A., Hardie, T., Zuniga, JC., Chen, L., and P. O'Hanlon, "Pervasive Surveillance of the Internet - Designing Privacy into Internet Protocols", IEEE 802 Tutorial, 14 July 2014, <https://mentor.ieee.org/802-ec/dcn/14/ec-14-0043-01-00EC-internet-privacy-tutorial.pdf>.

[privacy_windows] Microsoft Corporation, "How to use random hardware addresses in Windows", Microsoft Support, <https://support.microsoft.com/en-us/windows/how-to-use-random-hardware-addresses-ac58de34-35fc-31ff-c650-823fc48eb1bc>.

[private_mac] Pantaleone, D., "Private MAC address on iOS 14", Wayback Machine archive, September 2020, <https://web.archive.org/web/20230905111429/https://www.fing.com/news/private-mac-address-on-ios-14>.

[rcm_privacy_csd] IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group CSD on user experience mechanisms", doc.:IEEE 802.11-20/1346r4, 2020. Download available at <https://mentor.ieee.org/802.11/dcn/20/11-20-1346-04-0rcm-csd-draft-for-privacy-amendment-of-rcm-project.docx>.

[rcm_privacy_par] IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group PAR on privacy mechanisms", doc.:IEEE 802.11-19/854r7, 2020. Download available at <https://mentor.ieee.org/802.11/dcn/20/11-20-0854-07-0rcm-par-proposal-for-privacy.docx>.

[rcm_tig_final_report] IEEE 802.11 WG RCM TIG, "IEEE 802.11 Randomized And Changing MAC Addresses Topic Interest Group Report", doc.:IEEE 802.11-19/1442r9, 2019. Download available at <https://mentor.ieee.org/802.11/dcn/19/11-19-1442-09-0rcm-rcm-tig-draft-report-outline.odt>.

[rcm_user_experience_csd] IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group CSD on user experience mechanisms", doc.:IEEE 802.11-20/1117r5, 2020. Download available at <https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx>.

[rcm_user_experience_par] IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group PAR on user experience mechanisms", doc.:IEEE 802.11-20/742r6, 2020. Download available at <https://mentor.ieee.org/802.11/dcn/20/11-20-0742-06-0rcm-proposed-par-draft.docx>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8947] Volz, B., Mrugalski, T., and CJ. Bernardos, "Link-Layer Address Assignment Mechanism for DHCPv6", RFC 8947, DOI 10.17487/RFC8947, December 2020, <https://www.rfc-editor.org/info/rfc8947>.

[RFC8948] Bernardos, CJ. and A. Mourad, "Structured Local Address Plan (SLAP) Quadrant Selection Option for DHCPv6", RFC 8948, DOI 10.17487/RFC8948, December 2020, <https://www.rfc-editor.org/info/rfc8948>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[strint] W3C/IAB, "STRINT Workshop: A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)", <https://www.w3.org/2014/strint/>.

[wba_paper] Wireless Broadband Alliance, "Wi-Fi Device Identification – A Way Through MAC Randomization", WBA White Paper, July 2022, <https://wballiance.com/resource/wi-fi-device-identification-a-way-through-mac-randomization/>.

[when_mac_randomization_fails] Martin, J., Mayberry, T., Donahue, C., Foppe, L., Brown, L., Riggins, C., Rye, E., and D. Brown, "A Study of MAC Address Randomization in Mobile Devices and When it Fails", arXiv:1703.02874v2, DOI 10.48550/arXiv.1703.02874, March 2017, <https://doi.org/10.48550/arXiv.1703.02874>.

[wifi_tracking] Vincent, J., "London's bins are tracking your smartphone", The Independent, 9 August 2013, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/updated-london-s-bins-are-tracking-your-smartphone-8754924.html>.

Acknowledgments

The authors would like to thank Guillermo Sanchez Illan for the extensive tests performed on different OSes to analyze their behavior regarding address randomization.

The authors would also like to thank Jerome Henry, Hai Shalom, Stephen Farrell, Alan DeKok, Mathieu Cunche, Johanna Ansohn McDougall, Peter Yee, Bob Hinden, Behcet Sarikaya, David Farmer, Mohamed Boucadair, Éric Vyncke, Christian Amsüss, Roman Danyliw, Murray Kucherawy, and Paul Wouters for their reviews and comments on previous draft versions of this document. In addition, the authors would like to thank Michael Richardson for his contributions on the taxonomy section. Finally, the authors would like to thank the IEEE 802.1 Working Group for its review and comments (see <https://datatracker.ietf.org/liaison/1884/>).

Authors' Addresses

Juan Carlos Zúñiga
Cisco
Montreal QC
Canada
Email: juzuniga@cisco.com

Carlos J. Bernardos (EDITOR)
Universidad Carlos III de Madrid
Av. Universidad, 30
28911 Leganes, Madrid
Spain
Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Amelia Andersdotter
Safespring AB
Email: amelia.ietf@andersdotter.cc