

Randomized and Changing MAC Address

draft-ietf-mac-address-randomization-06

IETF 117 – MADINAS WG

Juan Carlos Zúñiga – Cisco
Carlos J. Bernardos – UC3M
Amelia Andersdotter – Sky UK

July 2023



Introduction and goals (reminder)

- Privacy, an increasing concern
 - Layer-2 globally unique identifiers (MAC addresses) have been assigned to devices and are transmitted in the clear in, for instance, beacons, probe requests, or after association
 - MAC addresses can easily be intercepted and used to track location or behavior
- Several projects in IETF, IEEE 802 and among mobile OS vendors to deal with plain-text, unique, permanent MAC addresses
 - Assigning a random MAC address to a device per connection, per SSID, after some time period
 - Area of extensive research (see reference Martin et al (2017) in draft for more comprehensive list of research in this area, or IEEE 802.11 RCM TIG final report in 11-19/1442r9, also in draft)
- Goal of this draft: document Current State of Affairs regarding MAC address randomization

Table of contents

1. Introduction	2
2. Terminology	3
3. Background	3
3.1. MAC address usage	3
3.2. MAC address randomization	4
3.3. Privacy Workshop, Tutorial and Experiments at IETF and IEEE 802 meetings	5
4. Recent RCM activities at the IEEE 802	6
5. Recent MAC randomization-related activities at the WBA	7
6. MAC randomization-related activities at the IETF	8
7. OS current practices	9
8. A taxonomy of MAC address selection policies	9
8.1. Per-Vendor OUI MAC address (PVOM)	10
8.2. Per-Device Generated MAC address (PDGM)	10
8.3. Per-Boot Generated MAC address (PBGGM)	10
8.4. Per-Network Generated MAC address (PNGM)	10
8.5. Per-Period Generated MAC address (PPGM)	11
8.6. Per-Session Generated MAC address (PSGM)	11
8. IANA Considerations	11
9. Security Considerations	11
10. Acknowledgments	11
11. References	11
11.1. Normative References	11
11.2. Informative References	12
Authors' Addresses	16



A taxonomy of MAC address selection policies

- Per-Vendor OUI MAC address (PVOM)
 - This form of MAC address selection is the historical default
- 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
- Per-Boot Generated MAC address (PBGM)
 - This form of MAC address is randomly generated by the device, each time the device is booted
 - *Not* stored in non-volatile storage, does not persist across power cycles
- Per-Network Generated MAC address (PNGM)
 - This form of MAC address is generated each time a new network connection is created, stored and indexed per SSID
- Per-Period Generated MAC address (PPGM)
 - This form of MAC address is generated periodically
- Per-Session Generated MAC address (PSGM)
 - This form of MAC address is generated on a per session basis

OS current practices

Android 10+	iOS 14+
The randomized MAC address is bound to the SSID	The randomized MAC address is bound to the BSSID
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 WiFi network	The randomized MAC address is reset when the device forgets a WiFi network
MAC address randomization is enabled by default for all the new WiFi networks. But if the device previously connected to a WiFi 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 WiFi networks

OS current practices

OS	Linux	Android 10	Windows 10	iOS 14+
Random per net.	Y	Y	Y	Y
Random per connec.	Y	N	N	N
Random daily	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

**Starting in Android 12, Android uses non-persistent randomization in the following situations: (i) a network suggestion app specifies that non-persistent randomization be used for the network (through an API); or (ii) 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)



Changelog

- -ietf-*-00:
 - Adopted version
- -ietf-*-01:
 - Addressed comments from Hai Shalom
- -ietf-*-02:
 - Move section 7 (OS current practices) to GitHub
- -ietf-*-03, -04:
 - Added section on taxonomy, removed BCP 14 terminology, other GitHub pull requests accepted
- -ietf-*-05, -06:
 - Title updated. Added new policy, Security consideration section

Next steps

- Document is ready
- Get reviews
 - from WG participants, WBA, IEEE and OS vendors
- WGLC?