MAC Randomization: Behavior and Impact

Introduction

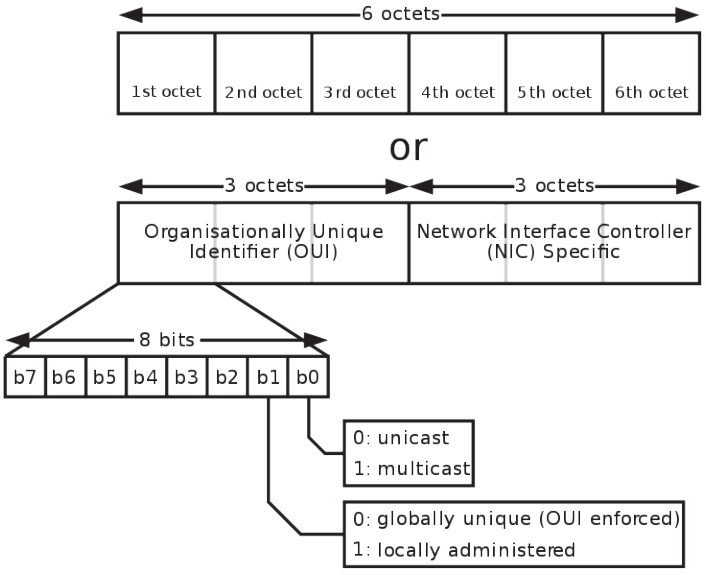
The hardware MAC address of a WiFi device is exposed to sniffing devices in an RF environment. When the user of a mobile device uses that device to connect to a WiFi network at a public place such as a cafe or a shopping complex, the user can be tracked on the basis of the device MAC address. Along with the current location, the number of last visits, time spent at a particular location can also be derived easily.

MAC randomization was introduced by OS vendors to address these privacy concerns. Randomizing MAC addresses in Probe Requests to SSIDs was introduced as a first step towards maintaining user privacy. An increased awareness of mobile privacy concerns has encouraged the growth and adoption of randomized MACs. In recent times OS vendors have enhanced this feature further to randomize MAC addresses not only in the Probe Requests of a wireless connection but also for associated clients. While this makes tracking WiFi users much more difficult, it also impacts normal operations of a WiFi network where client MAC addresses are used for legitimate purposes such as access control, roaming, etc. This impact is not limited to a particular WiFi vendor and affects the WiFi industry in general.

How is a MAC randomized?

A MAC address can be either universally addressed or locally administered. A universally administered MAC is globally unique in nature, assigned by the device manufacturer. A locally administered address is assigned to a device by a network administrator, overriding the burned-in address for physical devices.

The IEEE 802.1 bit 7 of a 48 bit MAC address is used to determine if the MAC address is locally administered. A value of 1 indicates a locally generated MAC address, either by the device itself or by a local network authority and is not guaranteed to be unique.



(By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here.

MAC Randomization Support by OS Vendors

OS vendors like Google, Microsoft have, over the past year, rolled out support for the use of a locally generated random MAC address each time a device communicates with a new WiFi network. A different random MAC is used for each wireless network (SSID). Apple recently announced support for random MAC addresses for associated clients with iOS 14, expected to release in September 2020.

The implementation of MAC randomization behaviour in terms of the frequency of MAC generation, probing and association behaviour, default ON/OFF, etc. varies across OS vendors.

	Behaviour Across Operating Systems		
Action	**iOS 14**	**Android 11**	**Windows 10**
Default	ON, users cannot change the default behavior	ON , users cannot change the default behavior	OFF. Users can change default settings to ON/OFF.
Connection to an SSID for the first time	On connecting for the first time to an SSID, a new random MAC is generated for the connection.	On connecting for the first time to an SSID, a new random MAC is generated for the connection.	• **MAC Randomization OFF** On connecting to a new SSID, Hardware MAC is used for the connection • **MAC Randomization ON** On connecting to a new SSID random MAC address is used for that connection
Connection to existing SSID	On disconnecting and reconnecting to the same SSID, the same random MAC is used for the connection.	On disconnecting and reconnecting to the same SSID, the same random MAC is used for the connection.	• With MAC Randomization ON, disconnecting and reconnecting to the same SSID results in the same MAC address being used.
Disable MAC Randomisation for an SSID	On disabling MAC randomisation, the device is automatically reconnected to the SSID with Hardware WiFi MAC address.	On disabling MAC randomisation, the device is automatically reconnected to the SSID with Hardware WiFi MAC address.	• **MAC Randomization OFF** On disabling MAC randomisation, the user has to manually reconnect to the same SSID (Hardware MAC address is used) • **MAC Randomization ON** On disabling MAC randomisation, the user has to manually reconnect to the same SSID (Hardware MAC address is used)
MAC Randomisation Disable for all SSID	NA	NA	On disabling MAC randomisation for all SSIDs, the device uses Hardware MAC address for reconnection.
SSID Profile Forget and Reconnection	On forgetting the SSID and reconnecting to it, the same SSID specific random MAC is used for the connection.	On forgetting the SSID and reconnecting to it, the same SSID specific random MAC is used for a connection.	• **MAC Randomization is OFF** On forgetting the SSID and reconnecting to it, Hardware MAC address is used for the connection • **MAC Randomization is ON** On forgetting the SSID and reconnecting to it, a newly generated random MAC address is used for the connection.

Impact and Mitigation

Except for Windows where randomization is disabled by default, the current implementations of MAC randomization across OS vendors do not enable time based randomization. This means that a device uses the same local MAC address per WiFi network though a different one for each network.

For Arista WiFi customers, MAC based features viz RADIUS MAC authentication, Google authentication and MAC based allow/block lists will be impacted. To continue supporting these features, a No MAC Randomization policy will need to be implemented at customer premises.

On the first client connect after upgrading to iOS14, the timers configured for guest WiFi access (login timeout and blackout time) will be reset. All guest users will be treated as new users irrespective of their earlier status. Guest users authenticating via any of the available methods.i.e social authentication or web forms, will need to re-login to the splash page after upgrading to iOS14.

In conclusion, the approach towards handling MAC randomization in WiFi products will keep evolving as OS vendors change feature behaviors to satisfy an increasingly privacy conscious market.

The Arista team is here to guide you through these changes and ensure minimal impact to WiFi services.
Contact us at **support-wifi@arista.com** to discuss more.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062