INDIO NETWORKS

MAC ADDRESS RANDOMIZATION

A primer on the development, current scenario and future implications.

Introduction

Media Access Control (MAC) is a burned-in 48-bit unique identifier for each of your personal, daily-use computer & mobile devices. It's represented by 12 hexadecimal digits. In layman's terms, it's a permanent name associated with your mobile, tablet or laptop's network hardware or chip. An example of how a MAC address looks like: **00:1B:44:11:3A:B9**.

Although MAC randomization has been around for a long time, it was used only during probing. The association of the station (your device) with the Access Point or Router and their associated Service Set Identifier (SSID), always exposed the original MAC address of your device.

However, in 2020, that changed, for the better or for worse, is a matter of perspective. Apple, Android OS and other OS vendors started using a default, Private (randomized) WiFi address.

It is a random MAC address different from your "real" MAC address at association, and for every SSID. This process is called MAC randomization. The random MAC address overrides the burned-in MAC address.

What does this mean? This means that your network stack never identifies a device uniquely as "X" or "Y" since the original MAC ID is hidden to all SSIDs and changes with each one.

MAC IDs have been used for multiple networking operations, from authentication and provisioning to granular management and control. This development has caused a massive disruption in the wireless and networking industry.

Reasons for MAC randomization

MAC randomization efforts can be traced back to a couple of years. Companies had started experimenting with tiny steps to improve privacy around WiFi deployments. MAC IDs have been used for multiple purposes since the advent of networking came about.

However, MAC IDs were constantly exposed to radio frequency environments which compromise privacy and lead to heavy data collection and analytics. To protect device identity and integrity over WiFi networks, MAC randomization was taken as the primary solution.

Identifying randomized MAC addresses

If the second character of the MAC address consists of 2, 6, A or E, then the address is said to be randomized. Identifying which MAC addresses within your network are random can help you understand the extent of the utilization of this technology.

x2 - xx - xx - xx - xx - xx
x6 - xx - xx - xx - xx - xx
xA - xx - xx - xx - xx - xx
xE - xx - xx - xx - xx - xx

(Source: Wikipedia)

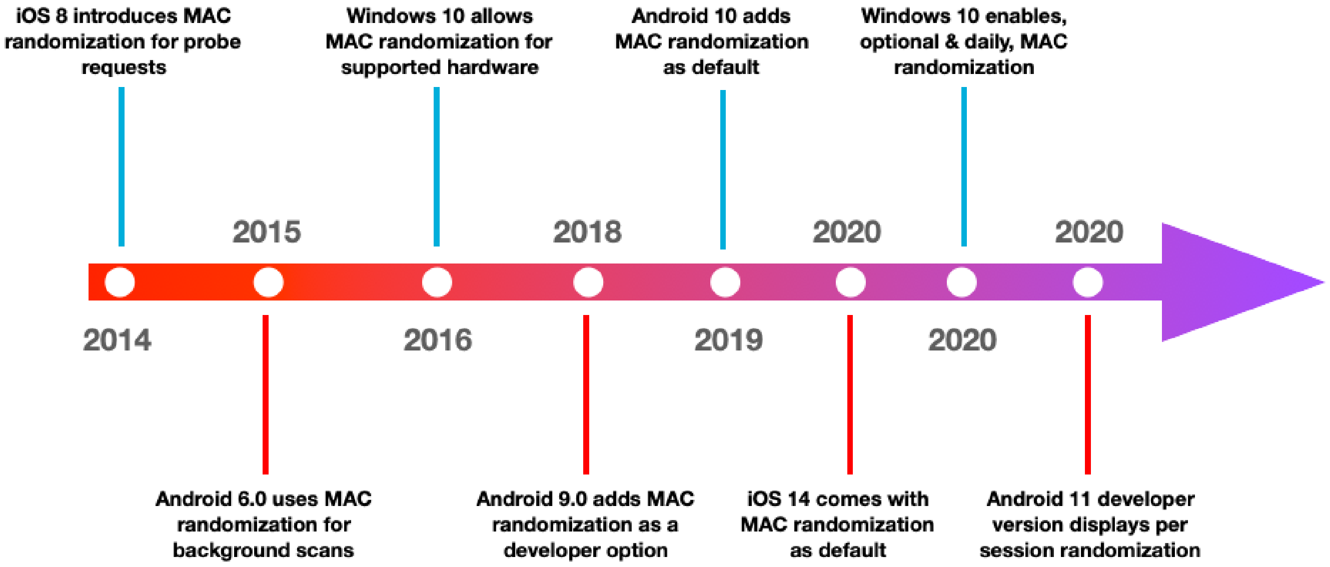
	MAC RANDOMIZATION ENABLED AS DEFAULT	RANDOMIZED MAC PERSISTENT PER SSID	OFFERS THE ABILITY TO CYCLICALLY RANDOMIZE MAC PER SSID	CAN BE DISABLED AS DEFAULT FOR ALL SSIDs
APPLE (iOS14)	YES	YES	NO	NO, BUT CAN BE TOGGLED OFF PER SPECIFIC SSID
ANDROID (OS 10)	YES	YES	NO	NO, BUT CAN BE TOGGLED OFF PER SPECIFIC SSID
WINDOWS (OS 10)	YES	DEPENDS ON RANDOMIZATION SETTINGS	YES	YES (Only through PowerShell)

Implications of MAC randomization from an end-user perspective

Looking from an end user perspective, this development essentially makes your device hard to track & uniquely identify over networks. An added level of obfuscation over your details increases the level of privacy and security on your devices. While you would not directly experience any benefits as such, your device would be protected against identification in RF rich environments. Most people using WiFi services for general purposes would probably not even notice that their MAC address is being randomized. However, if you are a regular visitor to a business which offers WiFi, the network you have previously associated with, will not recognize your device the next time you visit. You would have to repeat the process of registration and authentication every time you wish to connect to the WiFi.

This would become a cumbersome task for users who work as freelancers or regular travellers who visit hotels and cafes frequently. If onboarding of users becomes a lengthy, every day process, users might burn out and stop using Guest WiFi. Businesses spend time, money and effort on trying to provide seamless WiFi services to their customers.

MAC randomization further creates problems with MAC Access Lists. For example, parental control functions work on the basis of blacklisting MAC addresses on the network. If a MAC address randomizes on a timer-basis, the network would not recognize the device as blacklisted. The device would be able to gain access to the network irrespective of the Access Control List (ACL) rules set by the administrator.


iOS 8 introduces MAC randomization for probe requests
2014
2015
Android 6.0 uses MAC randomization for background scans
Windows 10 allows MAC randomization for supported hardware
2016
2018
Android 9.0 adds MAC randomization as a developer option
Android 10 adds MAC randomization as default
2019
2020
iOS 14 comes with MAC randomization as default
Windows 10 enables, optional & daily, MAC randomization
2020
2020
Android 11 developer version displays per session randomization

Effects on Enterprise Mobility and Mobile Device Management

A BYOD proliferation and an addition of personal devices in workplaces has always been a tough security problem to deal with. However, networking and wireless technology companies have come up with solutions which solve these problems. Enterprise Mobility Management and Mobile Device Management (MDM) solutions rely extensively on the uniqueness of the MAC for network control, operation and management.

MAC randomization presents several challenges to enterprise networks, such as:

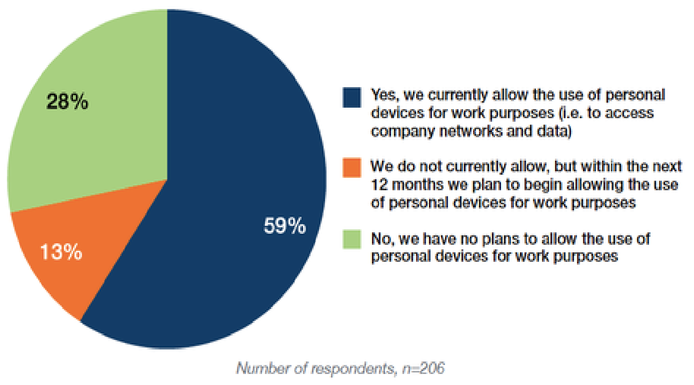
- Tracking devices over multiple SSIDs
- Authentication of users
- Achieving granular network control
- Incorrect location analytics

Solving the problem of MAC randomization

Currently, there are no concrete solutions which exist to help us solve the problem of MAC randomization. Efforts are underway to resolve the issue and uniquely identify devices through other methods. One easy way out is to simply tell your users to disable the private WiFi address feature through the settings.

Another way to resolve the problem is through modifying network profiles on MDMs and configuring them to disable private WiFi address through host agents.

DOES YOUR ORGANIZATION CURRENTLY ALLOW BYOD?



Source (Tech Pro Research)

Problems with MAC randomization

Currently, the documentation provided by OS vendors who offer MAC randomization is relatively low. In its initial stages, Apple's iOS operating system in its beta testing versions was shown to aggressively randomize the MAC. However, in its stable release, the private WiFi address for a specific SSID does not randomize even post forgetting the network.

While Android 11's developer versions had introduced a timer-based randomization n option, the stable release of the OS provides per Passpoint profile randomization.

Another reason why companies are not aggressively working on MAC randomization might be; In case a MAC address is randomized while a connection is live, the connection will be lost and the user would have to reconnect to the Access Point again. In such a test case, recurring randomization would mean repetitive attempts at forming a connection.

Research also suggests that MAC addresses are not the only unique identifier available to sniff device and gather data through them.

Putting the future in perspective

As the number of devices grow, as we continue to digitize markets, economies and all things across all aspects of life, security concerns will keep on growing. And companies who manufacture products will keep tightening their security parameters to ensure utmost security across all levels is maintained.

Networking and wireless technology companies need to continuously evaluate and revisit their approaches to make sure that they are in line with what the world is going to come about to, in terms of security and added levels of abstraction.

A few years down the line, we may not have the option to disable MAC randomization, those in this sphere must strive to build products that are ahead of the curve in terms of their adaptability.

Indio Networks LLC

815-A Brazos St, #326,
Austin, TX - 78701 U.S.A.
+1 (866) 554 5090
+91 (020) 6715 7379