aruba
a Hewlett Packard Enterprise company

MAC ADDRESS RANDOMIZATION

How To Tackle It With Aruba Infrastructure

Contents

Version Number	Date Last Updated	Changes
1.0	10/28/2020	Initial Publication

WHAT I NEED TO KNOW

What is MAC Randomization?

A MAC address is a physical hardware identifier that is assigned by the hardware manufacturer to a network device (Ethernet, Wireless, and Bluetooth as examples). Lately, several vendors have enabled changing the MAC address automatically to improve privacy. Detailed information is provided below.

How does this affect my products from Aruba Networks?

In short, there is not a significant effect on products from Aruba Networks. When MAC Randomization is enabled, most vendors will use the same MAC address for the same SSID every time it attaches. Since most clients/customers do not switch between multiple SSIDs on the same network, once the device is connected to a specific, the MAC address will not change in most circumstances.

Aruba Networks does not rely heavily on the MAC address for profiling the device type. While it is one of many factors in use, there are more accurate and detailed methods of profiling available. Detailed information can be found later in this document on a per-product basis.

Can I disable this on Aruba Networks hardware?

No, this is the device level configuration, and the infrastructure cannot enable/disable features on devices.

Is there a workaround provided by Aruba Networks?

A workaround is not needed as Aruba Networks products will handle MAC Randomization correctly in most cases. You can manually disable the feature or use a Mobile Device Management Platform to disable this feature on devices.

ClearPass Policy Manager makes use of additional credentials to identify the system or user in addition to the MAC address. Hence the devices with randomized MAC address will be identified regardless of the MAC address in use. Secure onboarding for BYOD devices is an additional option to work with unmanaged devices.

Corner Cases For MAC Randomization?

Yes, there are a few instances to be aware of, but they should not occur on a regular basis or be a normal occurrence. See the Technical Details section below for details on when and how MAC Randomization is enabled per device vendor.

- If the SSID is forgotten (removed from the device), software upgrade occurs, or factory reset of a device, the randomized MAC address can change.
- Duplicate MAC address from a client – exceedingly rare but can occur, and there is no remediation as two clients cannot have the same MAC address. You will need to disable MAC Randomization on one of the devices or follow the procedure from the device manufacturer to get a new randomized MAC.
- Clients connect to multiple SSIDs on the same infrastructure.

If the MAC address changes, there is no way to stitch the two random addresses together from a reporting standpoint (Airwave, Central, or any other reporting platform). It will also cause a new IP address request since DHCP offers are based on the MAC address of the client. If MAC caching is enabled and the MAC address changes, the client will look like a new device and not be MAC cached. However, upon reconnecting with the same MAC address, the cache will work.

If you are using device registration through ClearPass Policy Manager, the end-user will need to understand how to obtain their MAC address with randomization enabled, or they will need to disable the feature on their device. This can affect features like AirGroup/SSDP Protocols as examples.

TECHNICAL DETAILS

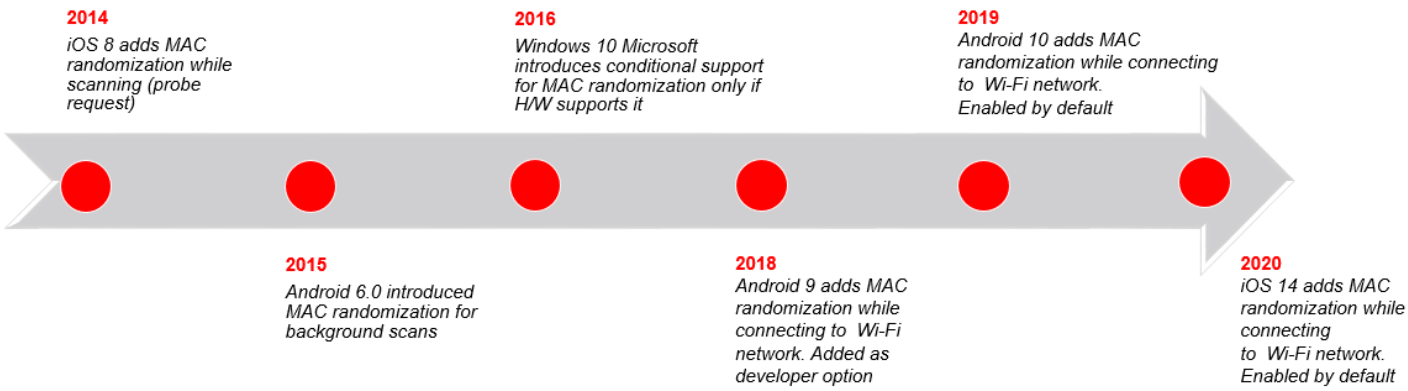
MAC Randomization Overview

Endpoint and user privacy continue to be a crucial aspect in today's data-driven networks since network-connected devices (primarily Wi-Fi) can be used to track your activity and identity. Some companies have highlighted this upfront that they log/record your access and then use this data for marketing purposes or even it's available for 3rd parties. 3rd parties can use endpoint mac-address to track devices and thus exposes user identity.
MAC randomization aims to prevent networks from using MAC addresses to build a history of device activity. In other words, a randomized MAC address adds another layer of privacy on a device to hide its identity. By enabling MAC address randomization, endpoint's security and privacy capabilities have increased to the next level.

Timeline

The use of random MAC addresses in endpoints is nothing new; initially, the randomized MAC address was used to probe for known SSIDs by the devices. Here are some of the examples of early implementations.

Figure 1: MAC Randomization Timeline



- **2014**: Apple added MAC address randomization to its devices starting from iOS 8. In iOS 8, randomized addresses are only used while unassociated and in sleep mode. In iOS 9, it was extended to location and auto-join scans.
- **2015**: Android 6.0 uses MAC randomization for background scans.
- **2016**: Windows 10 Microsoft introduces conditional support for MAC randomization, i.e., underlying hardware had also to support it.
- **2018**: In Android 9 {Android P}, it was introduced only as a developer option to cause the device to use a randomized MAC address when connecting to a Wi-Fi network.
- **2019**: Android 10 adds per network MAC randomization support.
- **2020**: Apple initially added automatic randomization of the MAC address every 24 hours, but later on changed its decision. Apple added per network MAC randomization support with iOS 14, iPadOS 14, and watchOS 7.

Recent Changes

With the current implementation, devices started using random MAC addresses for the association to the wireless networks. Now supported endpoints use a random device identifier instead of the real address when connecting to wireless networks.

Vendor Implementations

The implementation of MAC randomization differs depending on the vendor. Below you will find the current behavior of popular device types:

Windows 10

It can be configured globally, i.e., for all the wireless networks or the specific network only. When a global option is enabled, random hardware addresses are used to connect to any Wi-Fi network. If enabled for a particular network, then random hardware addresses are used the next time the device connects to that network.
The MAC address generated is per SSID (MAC is tied to SSID) and does not change after the client disconnects and reconnects.
If the user once connected with "Use random hardware address" to the SSID and marks it "Forget" and joins back to the same SSID, then a new random MAC Address is generated.

Android

Android implemented MAC randomization for Wi-Fi/5G/LTE connections with V10; the feature is enabled by default at an individual network level. The MAC address is tied to the SSID and retained after the client reboot or client connect/disconnect.
Once a random MAC address is used for a given network profile, the mobile device will continue to use the same random MAC address even after the user deletes the network profile and recreates the SSID/network profile.

Apple

Apple implemented its new MAC randomization feature as "Private Address" in iOS14 and iPadOS14. When the device is upgraded from previous versions of iOS, randomization will be enabled for all the existing SSIDs.
The MAC address generated per SSID (MAC is tied to SSID) does not change after the client disconnects and reconnects.
When a user upgrades from a previous version of iOS to iOS 14, the randomization will be enabled for all of the existing SSIDs.
Apple devices with iOS 14 and iPadOS 14 will keep using the same mac-address per SSID even if SSID is forgotten or if the client disconnects and connects back to the same SSID.

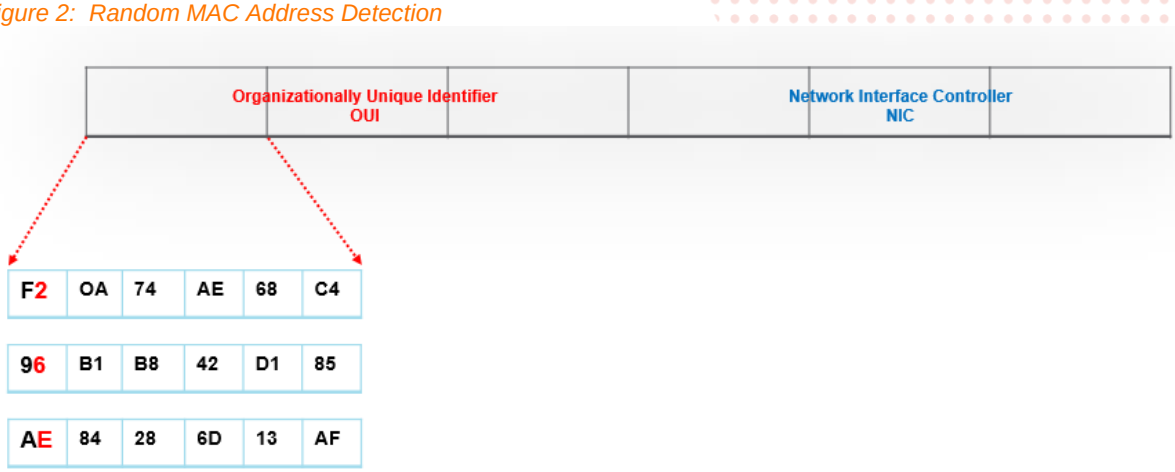
Table 1: Vendor Implementation

Operating System	Randomization Support	Default State	Per Network Support
Apple iOS 13	No	No	No
Apple iOS 14	Yes	Enabled	Yes
Apple iPadOS 14	Yes	Enabled	Yes
MacOS 10.15	No	No	No
Android 10	Yes	Enabled	Yes (Can be Disabled in UI)
Android 11	Yes	Enabled	Yes (Can be Disabled in UI)
Windows 10	Yes	Disabled	Yes (Can Be Disabled Via PowerShell Only)

Random MAC Address Detection

The generation of random MAC addresses is governed according to rules set by IEEE. There is a bit that gets set in the OUI portion of a MAC address to signify a randomized / locally administered address. The quick synopsis is looking at the second character in a MAC address; if it is a **2, 6, A, or E**, then it is a randomized address

Figure 2: Random MAC Address Detection



Product Impact Considerations

This section provides a feature level impact analysis. In cases where there are common misconceptions about impacts, we have outlined these areas in which there is no impact.

Airwave

Feature	Impact	Analysis
Licensing	None	AirWave license is based on the number of devices that are going to be monitored by AirWave.
Monitoring	None	Client monitoring is based on Username and Mac Address. So if the user's client has MAC randomized, we show all the Mac Addresses for the user in the list.
Reporting	Varies	The client reports are based on Client MAC, so we would see more entries in the reports with varied MAC address for each client.
VisualRF	None	It displays devices that the location engine has calculated a location for; the client MAC address has no impact on this feature.
RAPIDS	Minimal	It does not include clients. The ad hoc network by clients will be treated as rogue AP with SSID and MAC. The count may increase with unique MAC's.
Management	None	Not applicable to clients.
Database/Disk space	Minimal	The unique identifier in AirWave is MAC Address, so with unique MAC Addresses, there will be more client tables, more client RRD files will be created, which may impact performance slightly and increase the storage requirement for the client RRD.

Central

Feature	Impact	Analysis
Licensing	None	There is no impact on licensing since it's based on the number of devices.
Monitoring	None	Client monitoring is based on Username and Mac Address.
Reporting	Minimal	Client reporting is based on Username and Mac address. Overall reporting has minimal impact; please refer to the corner cases section for the details.
VisualRF	None	VisualRF displays devices that the location engine has calculated a location for. Client MAC address has no impact on this feature.
User Experience Insight (UXI)	None	It does not include clients. UXI leverages machine learning to surface critical problems through onsite sensors. Sensors mimic user and IoT behavior.
New Trend Charts (Health/SNR/Tx/Rx)	None	These charts are generated for connected clients (post association).
Live Captures (PCAP Enhancements)	None	Packet captures are generated for already connected clients (post association).
AI Insights	Minimal	Minimal impact on AI Insights except for a few cases mentioned under the Corner Cases section, e.g., Clients connect to multiple SSIDs on the same infrastructure.
AI Assist	Minimal	AI Assist is a troubleshooting service that is triggered based on certain events. For example, Client onboarding failure. In some cases, use client mac-address as part of the automated troubleshooting workflow.

ClearPass Policy Manager/ClearPass Device Insight

Feature	Impact	Analysis
Licensing	None	ClearPass Policy Manager licenses are based on the RADIUS session state. MAC addresses would be associated with a new session, and the old would close, thereby freeing the license from overuse.
Dot1.x Connect	None	ClearPass Policy Manager 802.1X authentications do not use the MAC address as the identity.
Mac Auth	Minimal	ClearPass Policy Manager MAC Address Bypass (MAB) or MAC Auth is not impacted by MAC address randomization once the system has joined the network. The device MAC address does not change once the client is connected to the network unless users manually select the “Forget Network” option. Guest workflows are not impacted. Device registration workflows are generally not affected as well.
CPDI Profiler	Minimal	ClearPass Policy Manager profiling signatures are modified; profiling signatures do not use the MAC OUI when MAC randomization is detected. This behavior is over-ridden with customer-defined custom signatures that may supersede the definitions within the CPPM definitions.
ClearPass Guest	None	ClearPass Policy Manager Guest workflows are not impacted by MAC address randomization. The MAC address is retained across user visits, allowing the information to be retained through multi-event/day visits.
Onboard	None	ClearPass Policy Manager Onboard associates a user to a system. The MAC address is not the identity source in the process and, therefore, not impacted.

BYOD	None	BYOD users who leverage ClearPass Policy Manager Onboard or 802.1X will not be impacted on existing clients. Onboarding new clients will follow the existing workflows.
Insight	None	ClearPass Policy Manager's Insight reporting provides all reporting information regardless of the MAC address type used.
CPDI-CPPM integration	Minimal	Tag-based enforcement might not work if the MAC vendor is selected as part of the tag. Everything else should work fine.

IN A NUTSHELL

MAC address randomization has evolved since 2014. Aruba infrastructure is well designed to tackle these changes. Aruba's forward-looking design helped Aruba tackle these changes seamlessly and with minimal impact to its portfolio. Aruba provides innovative solutions to solve customer use cases w.r.t. device connectivity, profiling, visibility, access policy, and policy enforcement to deliver high-performance networks with unmatched user experience.

For any questions comments, please reach us at airheadsteam@hpe.com.