ARISTA

Analysis of MAC Randomization Schemes in Wi-Fi Clients

Table of Contents

MAC Randomization in Different OSs 1
Android 1
iOS 2
Windows 2
MAC Randomization Testing 2
Android 11 2
Case 1: 'Wi-Fi enhanced MAC randomization' flag is disabled in Developer Mode. 2
Case 2: 'Wi-Fi enhanced MAC randomization' flag is enabled from Developer Mode. 6
Windows 10 10
Case 1: MAC randomization is disabled from the Wi-Fi Setting menu 10
Case 2: MAC randomization is enabled from the Wi-Fi Setting menu. 13
iOS 14 16
Summary 20

ARISTA

Analysis of MAC Randomization Schemes in Wi-Fi Clients

This site will be decommissioned soon. All content is migrated to Arista Community Central. Visit Arista Community Central for help articles and community engagement discussions on the complete range of Arista products.

The Hardware MAC address of a Wi-Fi client is exposed to sniffers in an RF environment. The MAC address of a Wi-Fi device, such as a mobile phone, tablets can be used by interested individuals or organizations to monitor or track the user, resulting in a breach of user privacy—for example, a person with a Wi-Fi device walking through a mall or any public space where Wi-Fi is deployed. By using the MAC address, the location of that person can be tracked. Along with the current location, the number of previous visits, time spent at a particular location or store can be derived easily.

To maintain user privacy, device or OS vendors such as Apple, Microsoft, and Google randomize the Wi-Fi client MAC address. With MAC randomization, when a client tries to connect to a Wi-Fi network, it uses a random MAC address instead of the Hardware MAC. Hiding the client Hardware MAC protects the privacy of the user. The implementation of MAC address randomization is not standardized, hence the behavior varies across OSes.

While MAC randomization ensures user privacy, it can also impact Wi-Fi network features that use client MAC addresses for legitimate purposes, e.g., access control, roaming, etc. Therefore, it is important to understand the details of MAC randomization.

Bit 7 of the MAC address (i.e the 2nd LSB of the first octet) is used to determine if it is locally generated or not. If it is set to 1, then the MAC address has been locally assigned, either by the device itself or by a local network authority, and is not guaranteed to be globally unique. On the other hand, if the bit is set to 0, then the MAC address is globally unique. The first 24 bits of a globally unique MAC address are used to determine the vendor (also called OUI, Organizationally Unique Identifier).

MAC Randomization in Different OSs

Android

Android 8 introduced the use of randomized MAC addresses for Wi-Fi clients that probe new networks and are not currently associated with any network. In Android 9, the MAC randomization feature was introduced as a Developer Mode option.

Android 10 introduced MAC randomization for association with Wi-Fi networks and the feature was turned on by default. The user can turn it on or off on a per-SSID basis. Android 11 has the same implementation of MAC randomization feature as Android 10. In addition, the Android 11 Developer Mode has a 'Wi-Fi enhanced MAC randomization' flag. Enabling it allows the MAC address to change every 24 hours after the device connects to an SSID that has MAC randomization enabled in the profile. The random MAC address

is also changed on forgetting an SSID and reconnecting to it.

iOS

With iOS 14, Apple devices have MAC randomization turned on by default with a per-SSID on-off flag. Further, randomized MAC addresses are used during probing. This is different from the SSID-specific randomized MAC used during association. The same behavior is observed in iPad OS and WatchOS.

Windows

Windows introduced MAC randomization in Windows 10. Users can enable or disable the feature for all or selected Wi-Fi networks. Windows 10 also allows users to randomize the MAC address every 24-hours.

The table below summarizes the implementation of MAC randomization in different OSs:

OS	Default Behavior	Per SSID Control	Comments
Android	Android 10 & 11 have MAC randomization ON by default.	Users can disable Wi-Fi MAC randomization in the SSID profile.	
iOS14	iOS has MAC randomization ON by default.	Users can disable Wi-Fi MAC randomization in the SSID profile.	iOS uses randomized MAC addresses for probing; these are different from SSID-specific random MAC addresses.
Windows 10	Windows 10 has MAC randomization OFF by default.	Users can change the random MAC address setting per SSID.	Users can choose to enable or disable randomization. Users can also generate a random MAC address every 24 hours.

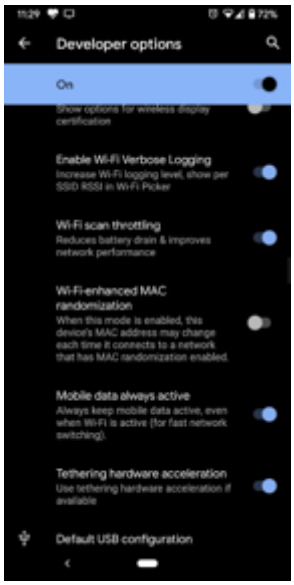
MAC Randomization Testing

We have considered the following OS versions for testing MAC randomization.

OS	Version	Build	Device Under Test
Android	11	RP1A.200720.009	Google Pixel3 & Pixel3A
Windows	10 Pro, version 1903	18362.959	Dell Latitude 5480
iOS	iOS14	14.0	iPhone 11

Android 11

Case 1: 'Wi-Fi enhanced MAC randomization' flag is disabled in Developer Mode.



Step 1

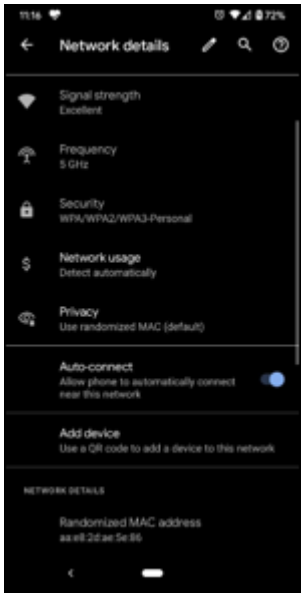
- Connect a new SSID
- A new random MAC address is generated for the SSID and the same is used in the Probe Request. The figure below shows the Probe Request generated by the device.

```
IEEE 802.11 Probe Request, Flags: ........
  Type/Subtype: Probe Request (0x04)
  Frame Control: 0x0040 (Normal)
  Duration: 0
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Source address: aa:e8:2d:ae:5e:86 (aa:e8:2d:ae:5e:86)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
  Fragment number: 0
  Sequence number: 1917
IEEE 802.11 wireless LAN management frame
  Tagged parameters (112 bytes)
    Tag: SSID parameter set: Broadcast
    Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
```

- The same address is used in the Association Request. The figure below shows the Association Request generated from the device.

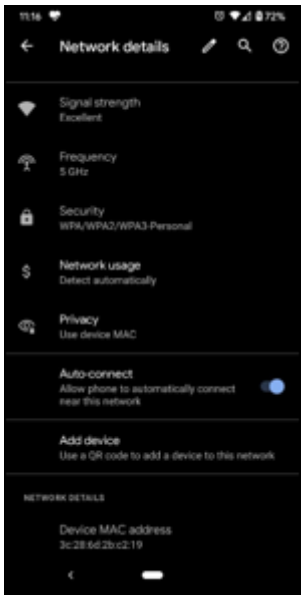
```
IEEE 802.11 Association Response, Flags: ........
  Type/Subtype: Association Response (0x01)
  Frame Control: 0x0010 (Normal)
  Duration: 0
  Destination address: aa:e8:2d:ae:5e:86 (aa:e8:2d:ae:5e:86)
  Source address: WibhuTec_c4:67:91 (00:11:74:c4:67:91)
  BSS Id: WibhuTec_c4:67:91 (00:11:74:c4:67:91)
  Fragment number: 0
  Sequence number: 258
IEEE 802.11 wireless LAN management frame
```

In the screenshot, the MAC address is aa:e8:2d:ae:5e:86. In binary format, it is '10101010:11101000:00101101:10101110:01011110:10000110'. In this, the 7th bit of the first octet is set to 1, indicating a locally generated MAC address.



Step 2

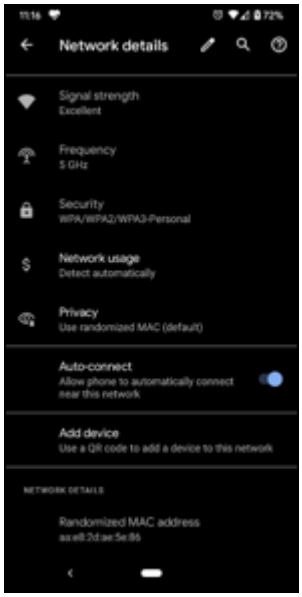
- Disable MAC randomization in the SSID profile.
- The client automatically disconnects and reconnects to the same SSID with the Hardware MAC address.



Step 3

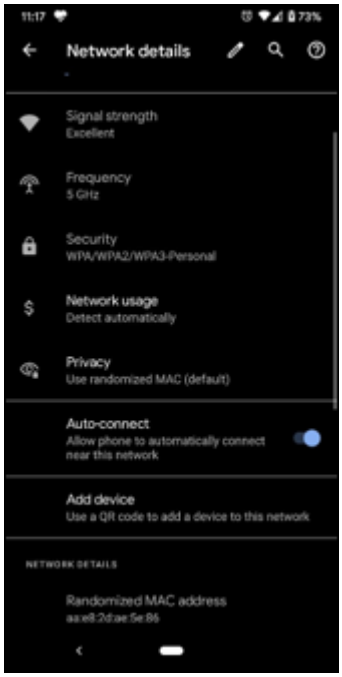
- Enable MAC randomization in the SSID profile.
- The client automatically disconnects and reconnects to the same SSID

- Random MAC address is used for this connection.
- The random MAC address is the same as in Step 1 (aa:e8:2d:ae:5e:86).

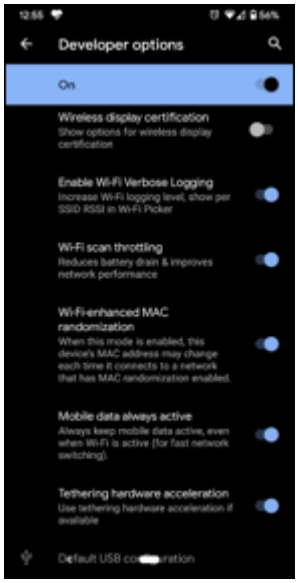


Step 4

- Forget the SSID profile while the device is connected to the Wi-Fi network; it is observed that the user gets disconnected from the network.
- Reconnect to the same SSID; Same random MAC address that was generated in Step 1 (aa:e8:2d:ae:5e:86) is used for reconnecting to the SSID.

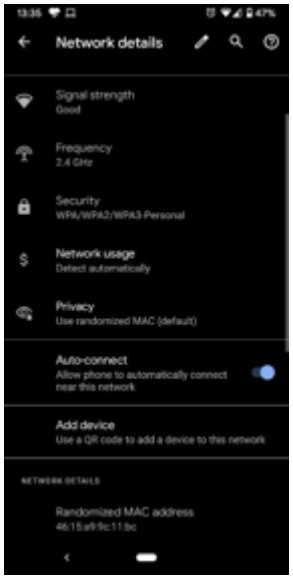


Case 2: ‘Wi-Fi enhanced MAC randomization’ flag is enabled from Developer Mode.



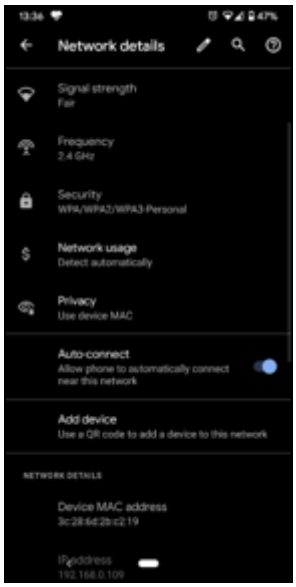
Step 1

- Connect a new SSID
- On connecting to the new SSID after a new random MAC address is generated and used for that Wi-Fi connection.



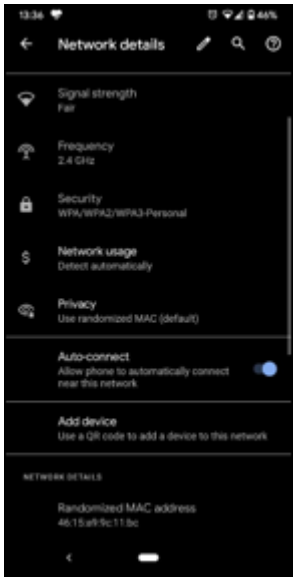
Step 2

- Disable MAC randomization in the SSID profile.
- The client automatically disconnects and reconnects to the same SSID.
- The client gets reconnected to the SSID with its Hardware MAC address.



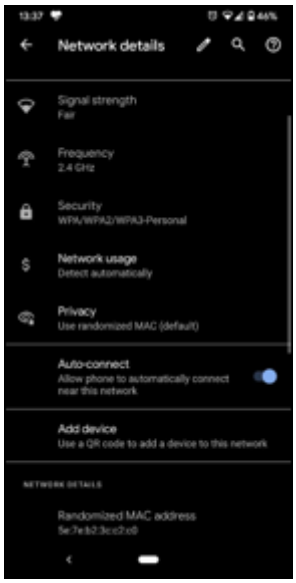
Step 3

- Enable MAC randomization in the SSID profile.
- The client automatically disconnects and reconnects to the same SSID
- Random MAC address is used for the connection; MAC address is the same as in Step 1 (4e:15:a9:9c:11:bc).



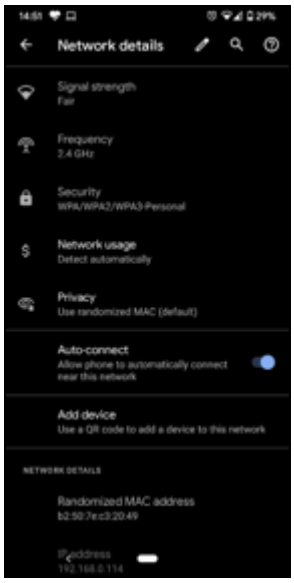
Step 4

- Forget the SSID profile while the device is connected to the Wi-Fi network; the device gets disconnected from the network.
- Reconnect to the same SSID
- A new random MAC address for that wireless connection (5e:7e:b2:3c:c2:c0).



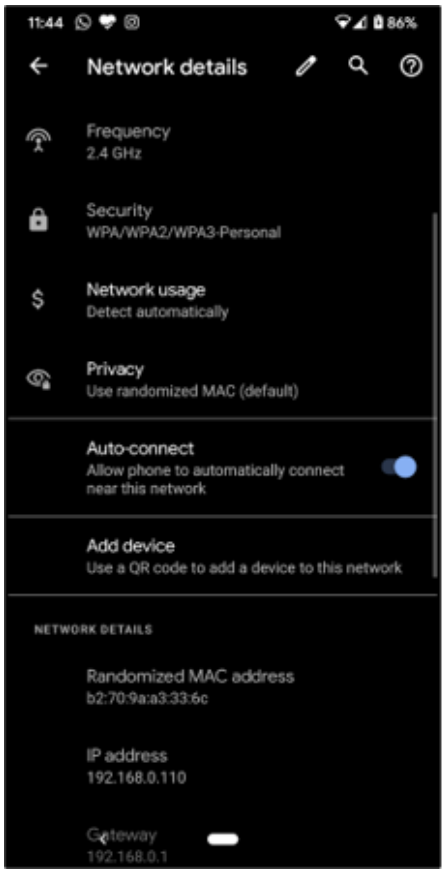
Step 5

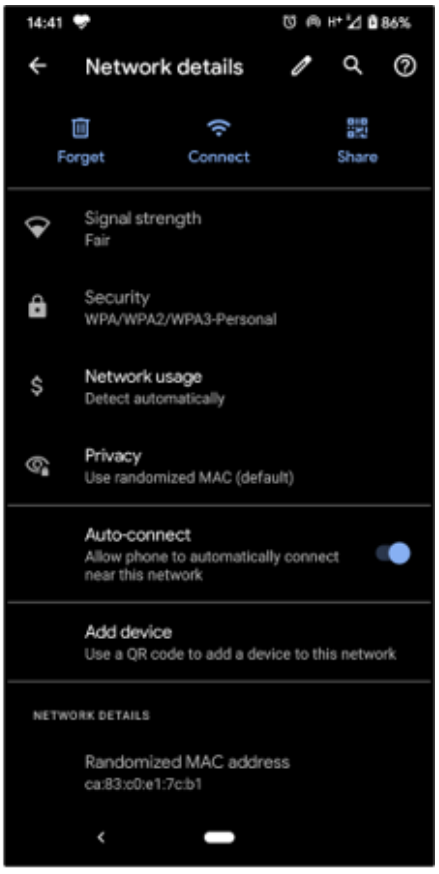
- Reboot the device.
- After reboot, the device gets connected to the same SSID with a new random MAC address (different from random MAC address generated in step 1).



Step 6

- Connect the client to the same SSID after 24 hrs.
- After 24 hrs observed that client gets connected with new random MAC address.

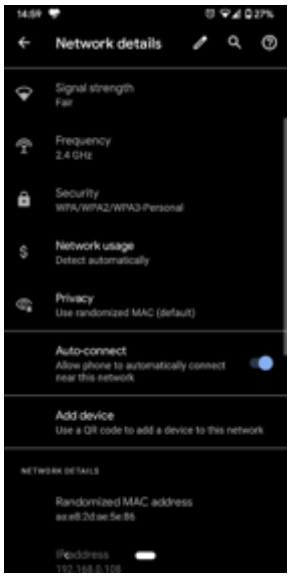




MAC Addresses: Day 1 (left) and Day 2 (right)

Step 7

- Disable'Wi-Fi enhanced MAC randomization' from Developer Mode
- Upon disconnecting and reconnecting the client manually, a random MAC address is used for the Wi-Fi connection; the MAC address is same as the one used in Step1 of Case 1 (aa:e8:2d:ae:5e:86).



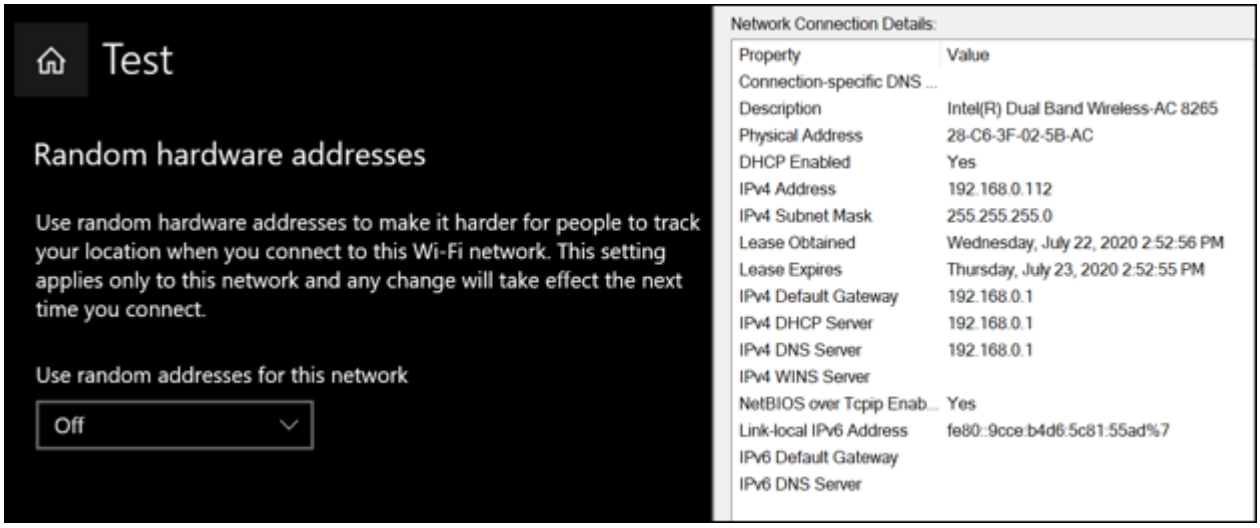
Windows 10

Case 1: MAC randomization is disabled from the Wi-Fi Setting menu

Step 1

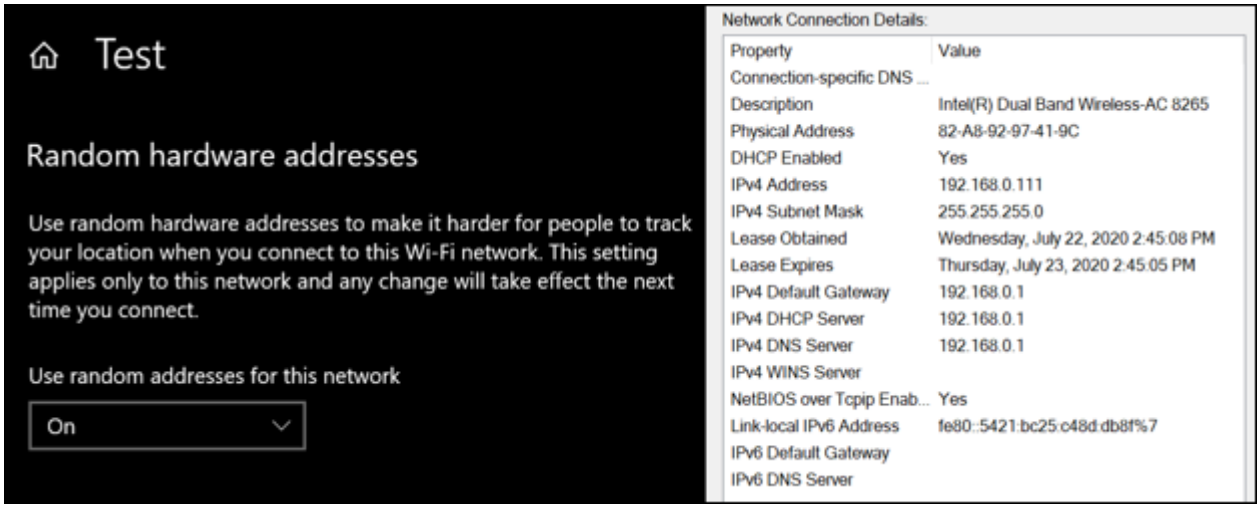
- Connect to an SSID
- Random MAC address is not generated and the client gets connected to the SSID with the Hardware MAC address

- Randomization is disabled by default in the Network (SSID) profile.



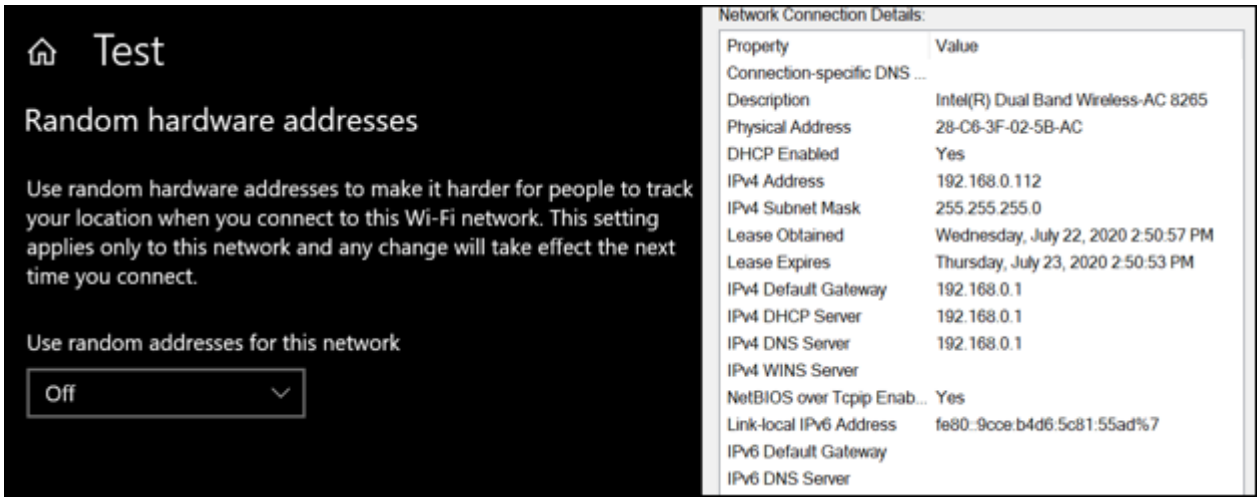
Step 2

- Enable SSID-specific MAC randomization while the device is connected to the Wi-Fi network;
- The ongoing association is not broken and the client stays connected to the SSID.
- Disconnect from the Wi-Fi network and reconnect manually to the same SSID
- A randomized MAC address is used for the new association.



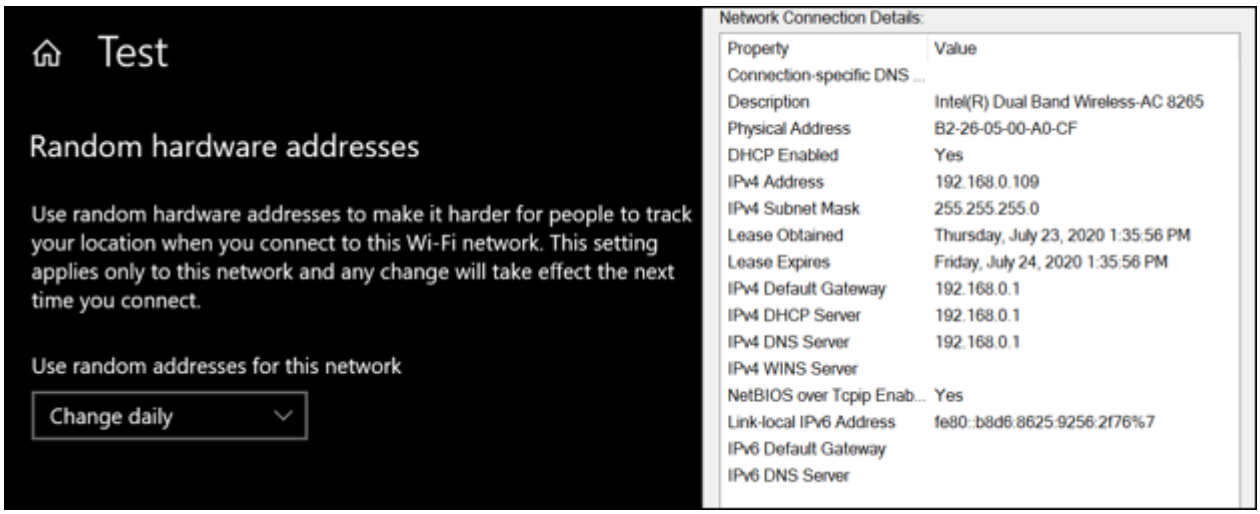
Step 3

- Disable SSID-specific MAC randomization;
- The ongoing association is not broken and the client stays connected to the SSID.
- Disconnect from the Wi-Fi network and reconnect to the same SSID;
- Hardware MAC address is used for the new association.



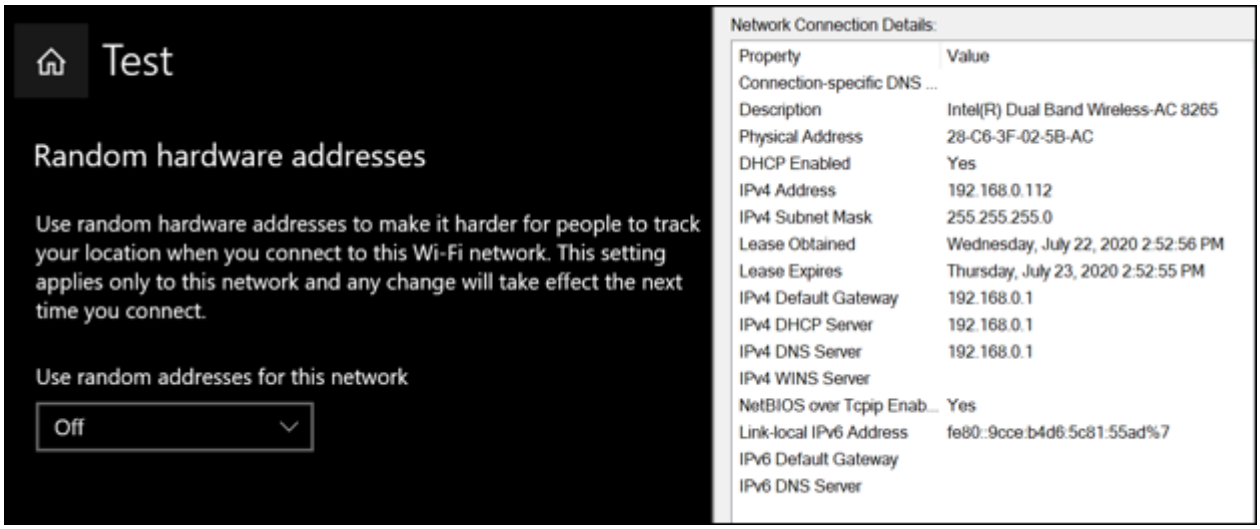
Step 4

- Select the ‘ Change daily’ option while the device is connected to a Wi-Fi network
  - Random MAC address is generated and the same is used for that wireless connection on the next calendar day.
  - The random MAC address generated on day1 is ‘82-A8-92-97-41-9C’ and MAC generated on day 2 is ‘B2-26-05-00-A0-CF’.



Step 5

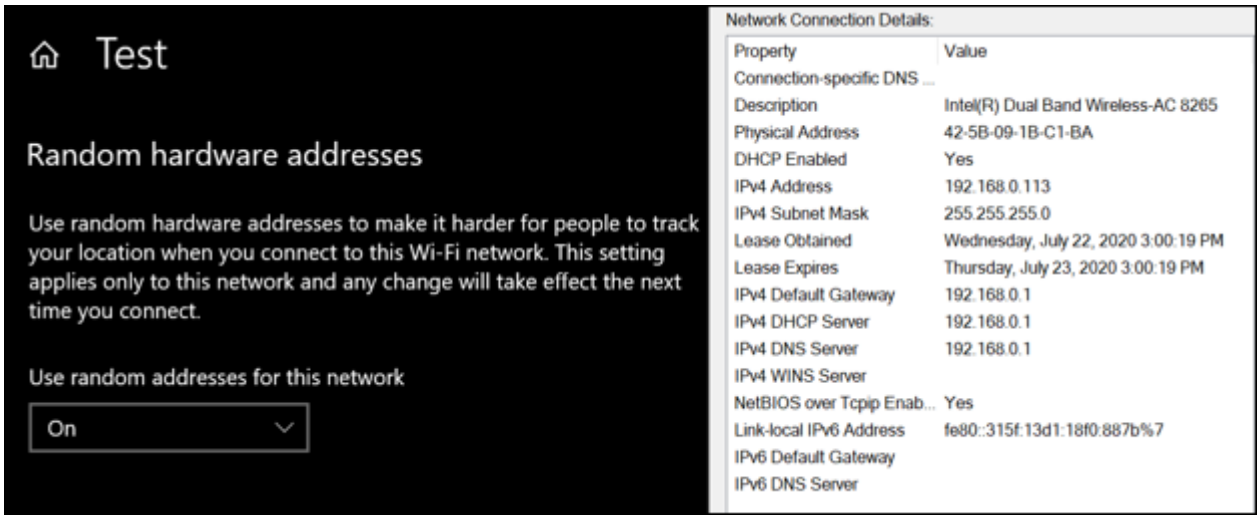
- Forget the SSID
  - The client is disconnected from the Wi-Fi network
- Reconnect to the same SSID
  - Hardware MAC address is being used for the new association; note that by default randomization is disabled for a new network (SSID) profile.



Case 2: MAC randomization is enabled from the Wi-Fi Setting menu.

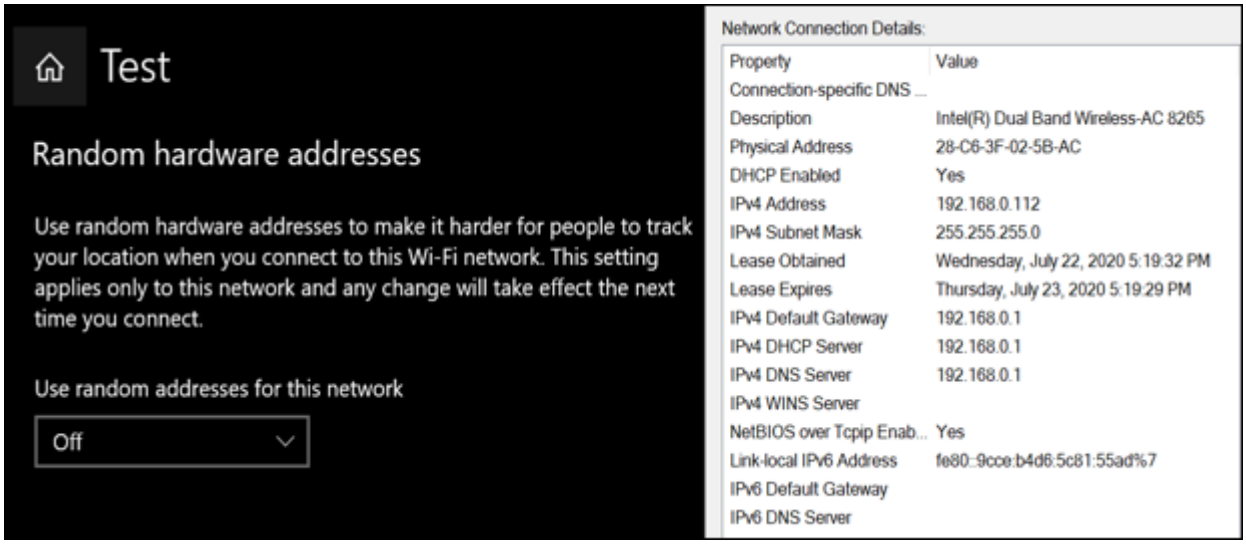
Step 1

- Connect a new SSID (for which there is no existing SSID profile)
  - The client gets connected to the SSID with a random MAC address (MAC randomization is automatically enabled for the SSID).



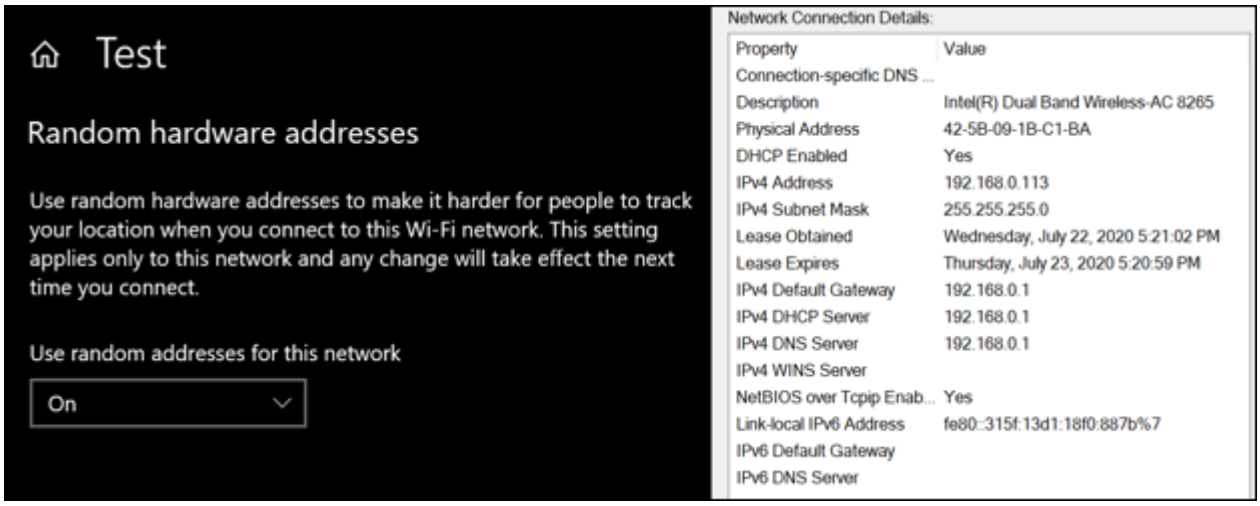
Step 2

- Disable SSID-specific MAC randomization while the device is still connected to the Wi-Fi network
  - Wi-Fi connection does not break down.
- Disconnect and reconnect manually to the same SSID
  - Hardware MAC is used for the new association even though the global MAC randomization option remains enabled.



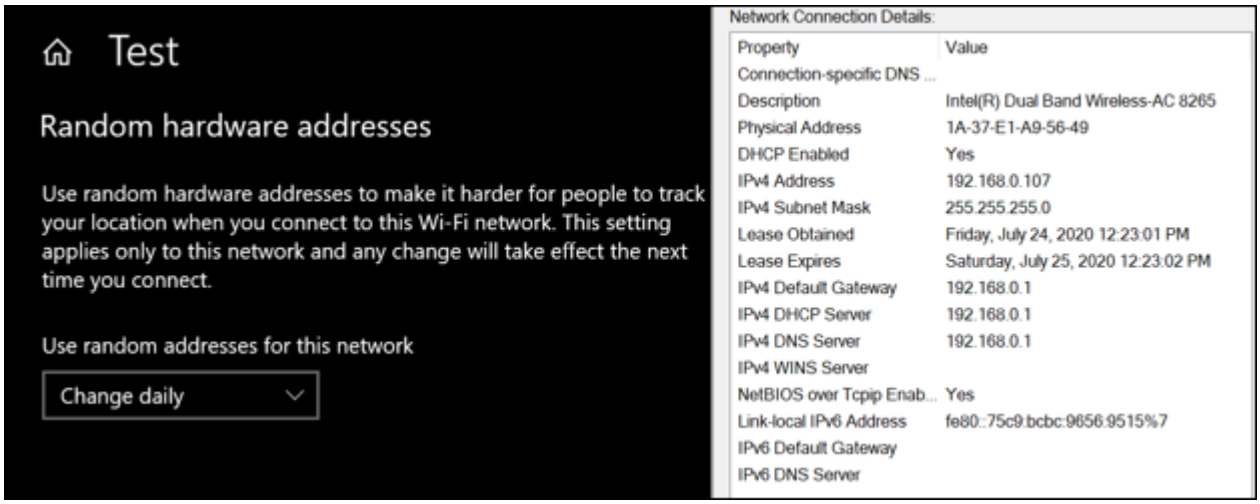
Step 3

- Enable the SSID specific MAC randomization
  - The ongoing association is not broken
- Disconnect and reconnect the client to the same SSID
  - MAC address is the same the one generated in Step 1 (42-5B-09-1B-C1-BA).



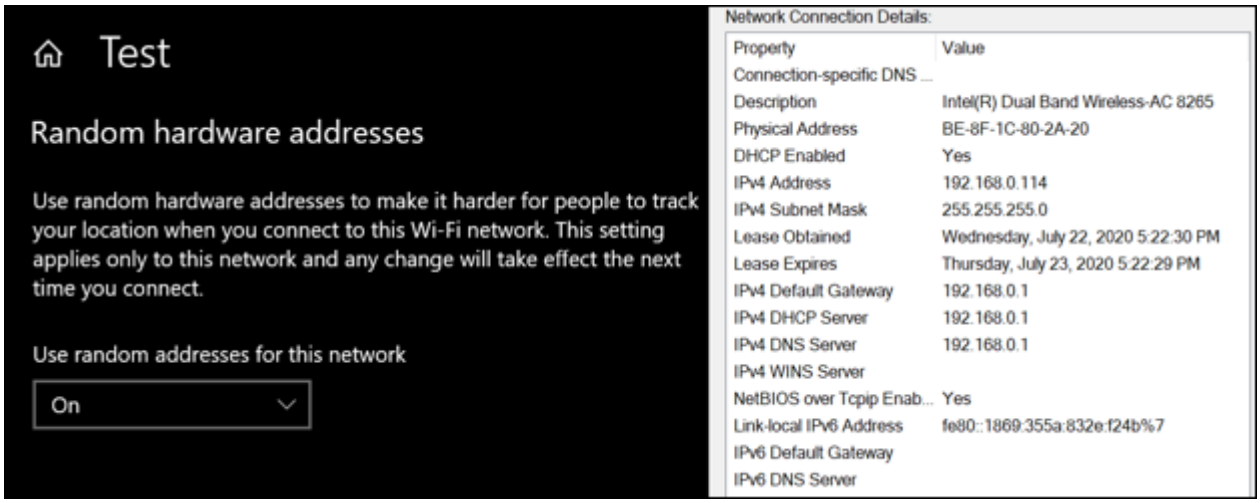
Step 4

- Enable the ‘ Change daily’ option for the SSID profile
  - New random MAC address is used the next day (Day 1 MAC address: 42-5B-09-1B-C1-BA and Day 2 MAC address: 1A-37-E1-A9-56-49).



Step 5

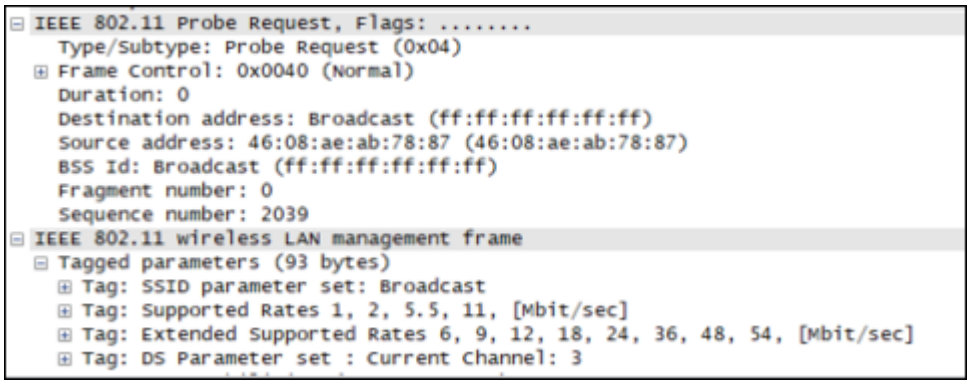
- Forget the SSID; the device gets disconnected from the Wi-Fi network.
- Reconnect to the same SSID
  - A new random MAC address is generated. The newly generated MAC address is different from the MAC address generated in Step 4 (1A-37-E1-A9-56-49).



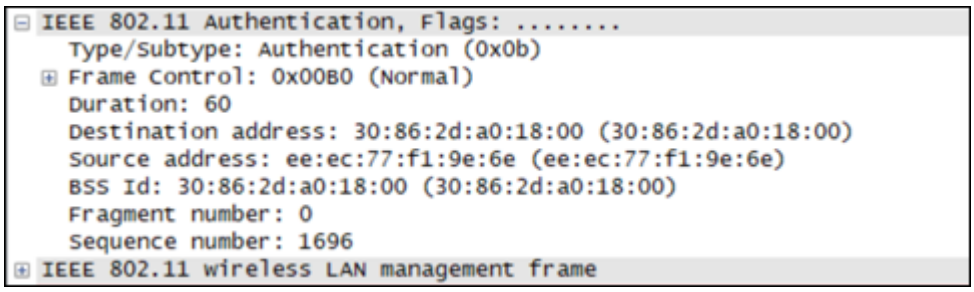
iOS 14

Step 1

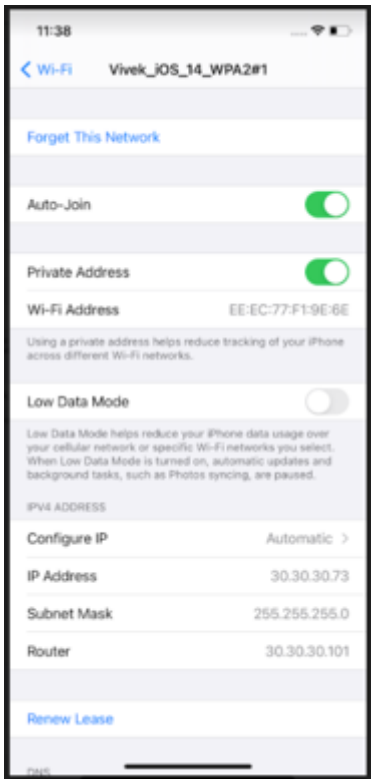
- Connect the iPhone to a new SSID
- A new random MAC address is generated for the connection and a totally different random MAC address is used in the Probe Request.
- The figure below shows the Probe Request frame generated from the iPhone.



The figure below shows the Association Request frame generated from the iPhone.

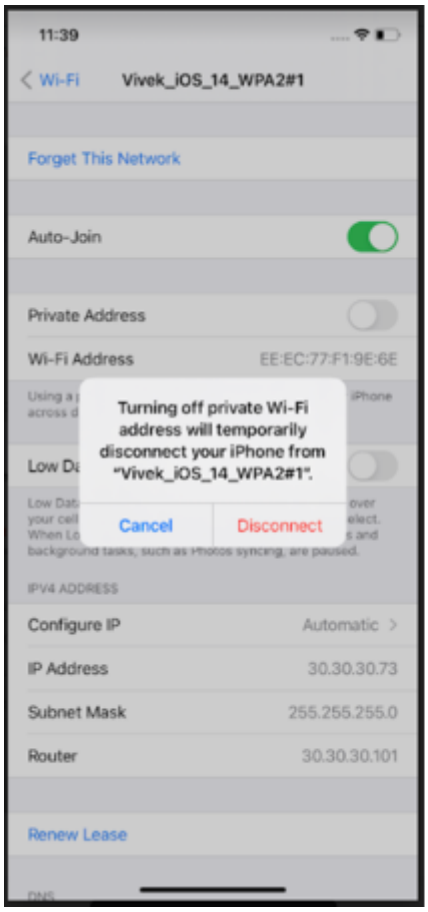


- The profile of the newly connected SSID has MAC randomization automatically enabled (referred to as 'Private Address' in the figure below).



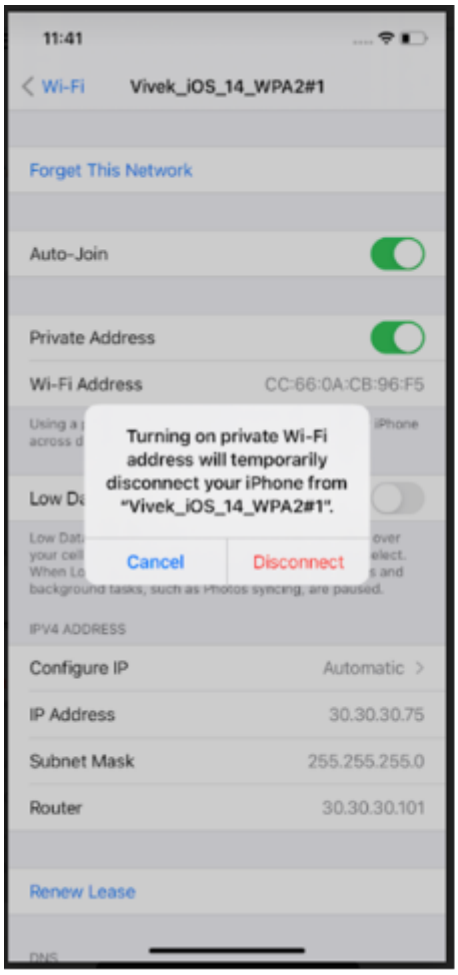
Step 2

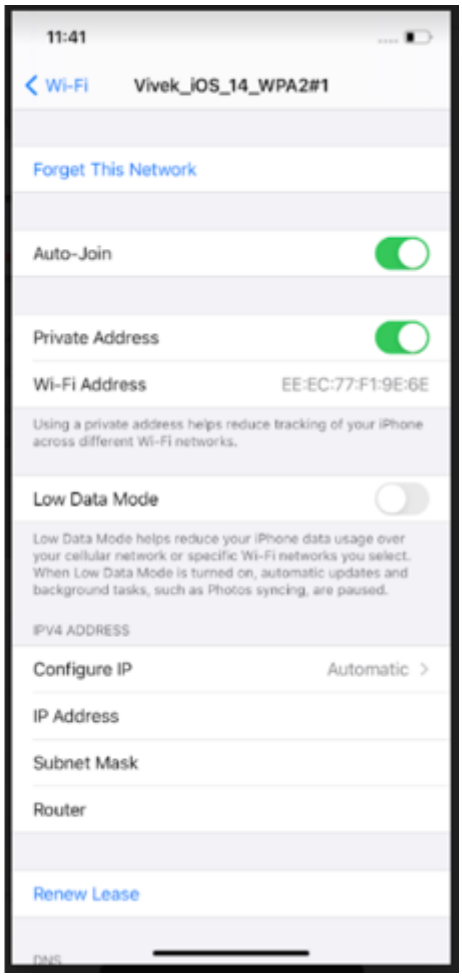
- Disable MAC randomization in the SSID profile; a confirmation message pops up.
- On selecting the 'Disconnect' option, the iPhone automatically disconnects and reconnects to the same SSID.
- The client gets reconnected to the SSID with its Hardware MAC address.



Step 3

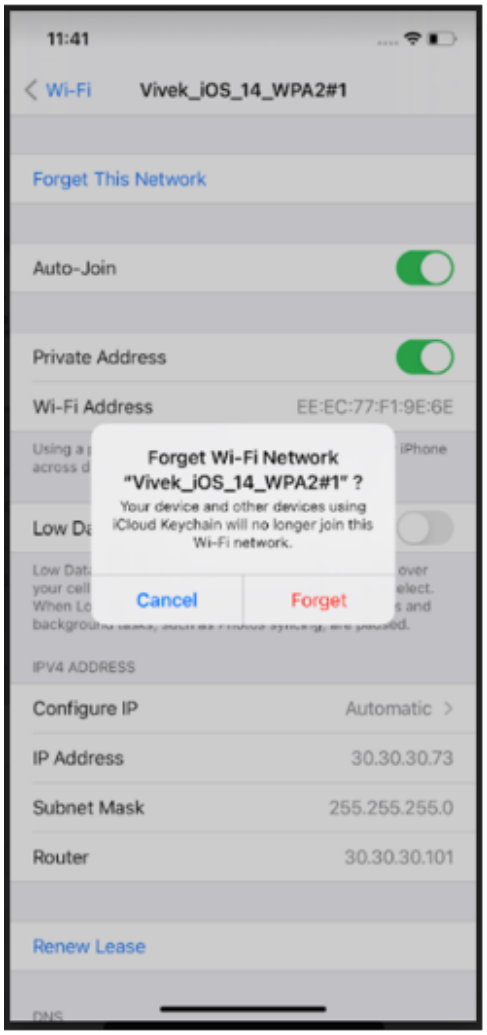
- Enable MAC randomization in the SSID profile; a confirmation message pops up
- On selecting the 'Disconnect' option, the device automatically disconnects and reconnects to the same SSID with a random MAC address
- The random MAC address is the same as in Step 1 (EE-EC-77-F1-9E-6E).





Step 4

- Forget the SSID profile while the device is connected to the Wi-Fi network; it is observed that the user gets disconnected from the network.
- Reconnect to the same SSID; the same random MAC address that was generated in Step 1 (EE-EC-77-F1-9E-6E) is used for reconnecting to the SSID.



Note: On upgrade to iOS 14, even though MAC randomization is ON by default, the MAC address corresponding to known networks (SSID) remains the same as Hardware MAC address for more than 24 hours and it changes to random MAC after that which remains constant.

Summary

	Android 11	Windows 10	iOS 14
Default Behavior	MAC randomization is default ON and users cannot change it.	MAC randomization is turned OFF by default. Users have the option to turn ON/OFF MAC randomization.	MAC randomization is default ON and users cannot change it.

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.	1. – 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	On connecting for the first time to an SSID, a new random MAC is generated for the connection.
Connection to existing SSID	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.	On disconnecting and reconnecting to the same SSID, the same random MAC is used for the connection.
Disable MAC randomization for an SSID	On disabling MAC randomization, the device is automatically reconnected to the SSID with Hardware Wi-Fi MAC address.	– MAC Randomization is OFF On disabling MAC randomization, the user has to manually reconnect to the same SSID (Hardware MAC address is used) – MAC Randomization is ON On disabling MAC randomization, the user has to manually reconnect to the same SSID (Hardware MAC address is used)	On disabling MAC randomization, the device is automatically reconnected to the SSID with Hardware Wi-Fi MAC address.
MAC randomization Disable for all SSID	NA	On disabling MAC randomization for all SSIDs, the device uses Hardware MAC address for reconnection.	NA
SSID Profile Forget and Reconnection	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.	On forgetting the SSID and reconnecting to it, the same SSID specific random MAC is used for the connection.

For details on how MAC randomization impacts Arista Wi-Fi features, see the whitepaper.