

2020-11 Advisory: Implications of MAC address randomisation on eduroam(UK) members

Introduction

With the introduction of iOS 14 and Android 11, MAC address randomisation will become more prevalent and will have some implications for our eduroam(UK) members.

History

Starting with iOS 8 and Android 8 mobile device operating system vendors started using randomised MAC addresses while scanning for wireless networks. These pre-association MAC addresses were random at every sweep. This was a step towards ensuring user devices could scan for wireless networks without being tracked.

In an enhancement to what the vendors billed as a privacy feature, Android 10 and iOS 14 introduced the ability to use random MAC addresses for actual Wi-Fi connections in that a connection to a new SSID would randomise its address once and then keep it the same for any subsequent connections. This is similar to existing behaviour of not using a randomised address at all on a per-network basis. However, as different SSIDs receive different device MAC addresses as part of the connection process, wireless networks cannot collude with each other to track the same device across their networks.

Android 11 introduces a feature identical to Windows 10 that initiates MAC address randomisation every 24 hours per SSID; this is identical to the experience with early iOS 14 development releases before Apple chose its more conservative regime upon release. On Windows 10 this feature is available, but disabled by default.

In an effort to ensure users are aware of this feature, iOS 14.2 and later will flag up a privacy risk with networks currently not using MAC address randomisation.

Implications

Research by eduroam(UK) based on devices seen across the national roaming servers has shown that the share of randomised device MAC addresses has grown from 2.1% to 10.5% in the last six months, and the share will grow more rapidly as newer versions of operating systems are adopted.

Therefore the implications for eduroam(UK) member organisations providing eduroam wireless network service include (but are not limited to) the following:

1. DHCP leases for IP addresses may be negatively affected and IP address pool exhaustion may occur, especially once randomisation on a 24-hour basis becomes prevalent.
2. Tracking specific devices on your wireless networks for error or abuse resolution may become more difficult, as newer devices with these operating systems pre-installed will automatically use MAC address randomisation.?
3. With newer operating system versions (such as Android 11) introducing randomisation on a 24-hour basis, the level of difficulty above will become more pronounced.?
4. Users of upgraded devices connecting to eduroam may request helpdesk assistance with the flagging of privacy risk on the eduroam network. This may require updated documentation to assuage fears of privacy compromise.?
5. Network traffic analysis for capacity planning may become inaccurate, as it may appear that more unique devices are connecting per day than is actually the case.?
6. MAC address-based mobile device control for home users (students/staff) with member organisation-issued devices may have unexpected consequences. For example, using registered MAC addresses to drive VLAN assignment for non-BYOD devices may suddenly no longer place staff devices into the correct privileged VLAN.?

Mitigations

Randomised MAC addresses can be recognised by checking the second hexadecimal character of the *Calling-Station-Id* RADIUS attribute for the values 2, 6, A, or E.

For organisation-issued devices, device policies and device management profiles allow the control of this feature. This may be useful for corporate Apple or Windows devices. eduroam CAT does **not** allow control of this feature as part of an organisation's CAT profile.

eduroam(UK) advises its members to engage with their network hardware vendors sooner rather than later to inform themselves on what effects MAC address randomisation may have on their access points and other network devices, and consider which effects of the above (or others that are not listed) may have on their provision of eduroam.

Useful links

Apple: <https://support.apple.com/en-gb/HT211227> [1]

Microsoft: <https://support.microsoft.com/en-us/help/4027925/windows-how-and-why-to-userandom-hardware-addresses> [2]

Android: <https://source.android.com/devices/tech/connect/wifi-mac-randomization> [3]

The Register: https://www.theregister.com/2017/03/10/mac_address_randomization/ [4]

PET Symposium: <https://www.petsymposium.org/2017/papers/issue4/paper82-2017-4-source.pdf> [5]

IETF: <https://www.ietf.org/proceedings/93/slides/slides-93-intarea-5.pdf> [6]

Vendor links

Meraki: https://documentation.meraki.com/zGeneral_Administration/Cross-Platform_Content/Meraki_and_iOS_14_MAC_Address_Randomization [7]

Cisco: <https://www.cisco.com/c/en/us/support/docs/field-notices/706/fn70610.html> [8]

Eleven Software: <https://blog.elevensoftware.com/how-mac-address-randomization-can-affect-thewifi-experience> [9]

Boingo: <https://support.boingo.com/s/article/Private-Address-Feature-for-iPhone-iPadand-Apple-Watch> [10]

Source URL: <https://community.jisc.ac.uk/library/network-and-technology-service-docs/2020-11-advisory-implications-mac-address-randomisation>

Links

[1] <https://support.apple.com/en-gb/HT211227>

[2] <https://support.microsoft.com/en-us/help/4027925/windows-how-and-why-to-userandom-hardware-addresses>

[3] <https://source.android.com/devices/tech/connect/wifi-mac-randomization>

[4] https://www.theregister.com/2017/03/10/mac_address_randomization/

[5] <https://www.petsymposium.org/2017/papers/issue4/paper82-2017-4-source.pdf>

[6] <https://www.ietf.org/proceedings/93/slides/slides-93-intarea-5.pdf>

[7] https://documentation.meraki.com/zGeneral_Administration/Cross-Platform_Content/Meraki_and_iOS_14_MAC_Address_Randomization

[8] <https://www.cisco.com/c/en/us/support/docs/field-notices/706/fn70610.html>

[9] <https://blog.elevensoftware.com/how-mac-address-randomization-can-affect-thewifi-experience>

[10] <https://support.boingo.com/s/article/Private-Address-Feature-for-iPhone-iPadand-Apple-Watch>