IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11Liaison statement from WBA on MAC Address Randomzation impacts |
| Date: 2018-09-11 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Dorothy Stanley | Hewlett Packard Enterprise | 3333 Scott BlvdSanta Clara, CA 95054 | +1 630 363 1389 | dstanley@ieee.org  |
|  |  |  |  |  |

**Abstract**

This document contains a liaison statement from the Wireless Broadband Alliance on the topic of MAC Address randomization impacts.

The liaison is embedded below and reproduced on the following pages.



|  |  |  |  |
| --- | --- | --- | --- |
| **Meeting Date**  | 4 September 2018  | **Meeting Time**  | 10.00-11.00 ET / 15.00-16.00 GMT  |
| **Project**  | Testing & Interoperability Workgroup  |
| **Project chaired by**  | Michael Sym (BSG Wireless), Luther Smith (CableLabs), Erinn Hall (AT&T), Mark Hamilton (Arris)  |
| **To**  | IEEE – 802.11 WG Chair  |
| **Subject**  | MAC randomization impacts  |
| **Action ID Prefix**  | N/A  |

Dear Dorothy Stanley, Chair, IEEE 802.11 WLAN Working Group,

Currently, iOS, Android, and Windows anonymize the MAC address during probe requests while still using the true MAC address when connecting to the network. Further addressing the need of user privacy, in Android P new development [(ref)](https://www.androidpolice.com/2018/03/08/android-p-feature-spotlight-per-network-mac-address-randomization-added-experimental-feature/), Android plans to create a unique, anonymous MAC for each SSID that the device connects to:

“*Connected mode randomization is a developer feature only and would be default off for Android P. Our main goal this year is to get a soak time in the industry and get feedback from partners such as yourself who depend on mac address identifier. It gives time for the ecosystem to adapt to new behavior once we roll out in subsequent releases as default behavior.*

*In O, we released Probe mode randomization, which randomized the mac address while scanning for new networks. For P, we are going to create a persistent mac address per SSID. So for enterprise use-case, you would see the device show up with the same mac address every time it connects to your network* “

One direct implication: If the user forgets the network, and then reconnects, a new MAC address is created for the SSID. The same thing happens if the user factory-resets their network settings. Thus, operators will no longer be able to use the MAC as a reliable unique identifier for the device.

Note: We believe MAC Address randomization, even for associations, is already in the field.

Also, IPv6 privacy features can result in a unique (“33-33”) MAC Address on individual links/connections.

802.11aq says:

* Note that 11aq requires setting the “Local” bit. (Clause 12.2.10 – use the locally administered address space)
* Only talks about pre-association randomization. So most (all?) of the discussion below is beyond 11aq features
* “MAC Address randomization provides MAC Address privacy and this is important. In 802.11aq-2018 it produces requirements for MAC Address privacy, and it is felt that interoperability would be improved if vendors adhered to the those requirements described in 802.11aq-2018.”
* Cf: 18/1032r4.

802.11-2016 says:

* (Clause 4?) Any MAC Address no matter how created, shall conform to IEEE 802 (by implication 802c).
* For the duration of an association to an ESS, the MAC Address should/shall? not change.

IEEE 1609.2 seems to have this facility (randomization) for OCB operation, and it has been working for years. Does it inform on how the list of issues raised here can be addressed?

In this context, WBA community identified a list of potential impacts of these changes to existing systems and solutions:

* For MAC-based identification (e.g. MAC Authentication, MAC whitelisting, certain widelydeployed captive portal configurations) MAC is cached on first time usage and subsequent logins re-use it. The customer would have to re-sign in and register the device each time the SSID is forgotten. This would result in a long list of devices per customer.
	+ - Also, this would fill up the customer’s device limits.
		- The customer will subsequently find it difficult to identify their devices to specify which MAC addresses are the current ones that should be retained and which are invalid past identities that should be deleted.
		- MAC-based identification is BAD. Don’t do it. Device/user identification needs to use a specific mechanism that is permanently (and desirably privately) connected to the device/user. We recognize that this a potential change to current behaviour. Appropriate organizations should be brought in to the discussion (as you are doing) to solve the problem within their specific domains.
* When one device connects to a particular SSID using 2 (or more) different Passpoint profiles, we are not guaranteed the same randomized MAC address will be used on that same SSID.
	+ - Depending on device implementation, a single Passpoint profile may not use the same randomized MAC address every time it connects to the same SSID. Meaning, the device may have the same behavior as a device in which the SSID has been forgotten.
		- For Passpoint connectivity, maintaining the MAC address for a given SSID could be problematic, as multiple SSIDs will typically be used for a single service provider. It would be better if the MAC address randomization maintained the MAC address for all connections using the same Passpoint profile, not for connections to a specific SSID.
		- Agreed, this last point will help, and should be encouraged. IEEE 802.11 will consider the concept above (reference to the same address for the duration of an association to an ESS) to recommend it apply for any connection to the same Hotspot network. However, if this is probably not sufficient. Identification based on MAC Address is just a bad idea, even with this slight help.
* Different bands with different SSIDs (2.4GHz and 5GHz) – Operators may see devices reported twice on their networks. This breaks band steering with multiple SSIDs.
	+ Agreed. Recommend that 802.11 should look into this. Perhaps coordinate with WFA.
* Clients may use the broadcast SSID in probe requests, and therefore may use a different randomized MAC address than the ones used when associated to an AP.
	+ Client steering depends on the probes using the same MAC address as the associated MAC address. When different MAC addresses are used, client steering cannot determine that the device is the same client.
	+ Agreed. Recommend that 802.11 should look into this. Perhaps coordinate with WFA.
* Certain widely-used Pay per use (PPU) customers have their pass associated with a MAC, so if the MAC Address changes there is no way to transfer that pass to another MAC.
	+ - MAC-based identification is BAD. Don’t do it. Device/user identification needs to use a specific mechanism that is permanently (and desirably privately) connected to the device/user. We recognize that this a potential change to current behaviour. This is out of scope of 802.11 to address.
* Certain widely-used Short-term complimentary services could be accessed by customers repeatedly by getting a new MAC Address that will allow customers to create another account and get another free session / allowance, simply by forgetting the SSID.
	+ This may impair the ability of the Wi-Fi service to enforce policies tied to specific devices, such as parental controls. The user can forget the network and get a new MAC address, and network-based parental controls would no longer be applied appropriately.
		- MAC-based identification is BAD. Don’t do it. Device/user identification needs to use a specific mechanism that is permanently (and desirably privately) connected to the device/user. We recognize that this a potential change to current behaviour. This is out of scope of 802.11 to address.
* MAC randomization could result in duplication of another randomized (or real registered) MAC address, creating a duplicate MAC scenario (collision).
	+ This is unlikely (how unlikely?). But, if it happens it is BAD.
	+ 802.1CQ is considering centralized control methods to avoid this happening, that should be investigated.
	+ Maybe can leverage something from IPv6 neighbor methods, to dervice a method to help prevent this.
* Collision of MAC addresses under the same DHCP server would cause issues with the users accessing the network.
	+ Agreed, but this is the least of their problems.
	+ Further, per above points, a single client may appear as multiple addresses (on different bands, etc.) which will confuse DHCP assignment, and confuse upper layers.
* Analytics rely on the ability to identify a unique device and have that identifier remain consistent over time o Helpdesks need to be able to identify specific devices that the customer is calling about, and understand how they have behaved over time. If a user forgets the SSID because they are having connectivity problems, the service provider will lose traceability of the issue. It will also make it more difficult for the user to identify their device to the helpdesk advisor.
	+ If a device has an association failure on first attempting to connect, we are not guaranteed the same MAC Address be used subsequently. And so, the failure cannot be traced, obscuring device attribution.
	+ Access points / Service providers which track the history of devices that have connected will end up with bloated records which contain additional entries for devices where the user has forgotten the SSID and reconnected.
* Accounting and billing issues – MAC Address is tied to this in use cases where rates rely on a unique device identifier. This could be accomplished instead with proper support for Chargeable-User-Identity (CUI).
* Blacklisting of devices based on MAC Address becomes unreliable.
* We may not be able to handle Legal requirements for providing the type of information required for device traceability, device ownership, and legal intercept.
* We can no longer identify manufacturer from OUIs or CIDs in the IEEE registry for the purposes of troubleshooting, diagnostics, and analytics.

**Specific request**: WBA would like to recommend further discussion within the operator and vendor community to minimize the impact of implementing MAC randomization. The team may also approach device makers to propose revising certain aspects of randomization, which may help to resolve some concerns listed. Please let us know your thoughts on the impacts listed, any additional impacts we haven't noted, and any actions your organization recommends.

**Target date:** A response to this LS is requested by November 2, 2018.

For additional information and/or further questions please contact Bruno Tomas - WBA PMO (bruno@wballiance.com).

Next WBA F2F Meetings:

* 29-30 October, 2018, London, UK
* 29-31 January, 2019, Hong Kong