Liaison Statement from IEEE 802.11 Working Group to Wireless Broadband Alliance (WBA)

Source:	IEEE 802.11 Working Group[1] November 2018	
To:	Bruno Tomas	Senior Manager, PMO, Wireless Broadband Alliance bruno@wballiance.com
	Michael Sym	Chair, WBA Testing & Interoperability Workgroup michael.sym@bsgclearing.com
CC:	Konstantinos Karachalios	Secretary, IEEE-SA Standards Board Secretary, IEEE-SA Board of Governors sasecretary@ieee.org
	Paul Nikolich	Chair, IEEE 802 LMSC p.nikolich@ieee.org
	Jon Rosdahl	Vice-chair, IEEE 802.11 WLAN Working Group jrosdahl@ieee.org
	Robert Stacey	Vice-chair, IEEE 802.11 WLAN Working Group robert.stacey@intel.com
	Mark Hamilton	Chair, IEEE 802.11 ARC Standing Committee mark.hamilton@arris.com
	Tiago Rodrigues	General Manager, Wireless Broadband Alliance tiago@wballiance.com
	Edgar Figueroa	CEO, Wi-Fi Alliance efigueroa@wi-fi.org
From:	Dorothy Stanley	Chair, IEEE 802.11 WLAN Working Group dstanley@ieee.org
Subject:	**Liaison communication reply to *WBA Liaison Statement – MAC Randomization Impacts***	

Dear Bruno and Michael,

The IEEE 802.11 Working Group is pleased to have received your liaison on September 11, 2018, regarding concerns expressed by the WBA community on impacts of client devices anonymizing (randomizing) their MAC address.

Some general comments and specific responses on the detailed liaison bullet points are included below.

In general:

[1] This document represents the views of the IEEE 802.11 Working Group, and does not necessarily represent a position of the IEEE, the IEEE Standards Association, or IEEE 802.

1) Certain generally available devices already use a randomized MAC address for 802.11 association, extending use of random MAC addresses beyond the address used for probe frames and other pre-association frame exchanges.
2) IEEE 802.11 has standardized MAC address randomization to enhance user privacy in the recently published IEEE Std 802.11aq™-2018 amendment.

The IEEE 802.11 WG strongly recommends **against** using any specific MAC address as an identifier for a user or device outside the scope of layer 2 communication. Most of the examples/scenarios provided in the liaison are examples of misuse of the MAC address as such an identifier, and our opinion is that the system or application should be modified to use a more appropriate identifier, preferably one that can be protected from eavesdropping to keep the user's identity private.

The IEEE 802.11 WG understands that for automotive use cases (Intelligent Transportation System), implementations of IEEE 1609.3 and SAE J2945/1 have deployed MAC address randomization ("re-addressing") when out of the context of a BSS, and this has been working for years. It seems possible that methods of client device identification used in that context could be adapted for use within an infrastructure network, and might provide a starting point for such work.

With respect to the specific bullet points listed in the received liaison, the IEEE 802.11 WG offers the following responses:

- MAC-based identification (such as MAC Authentication, etc.):
    - Device or user identification needs to use a specific mechanism that is permanently and privately connected to the device or user. MAC addresses are not private and should not be assumed to be permanent.
    - The IEEE 802 community built its standards based on the assumption that such uses would not occur beyond layer 2.
    - We recognize this assumption may not have been understood by other organizations. Hence, appropriate organizations should be brought in to the discussion (as WBA are doing) to solve the problem within their specific domains.
- A single device using a combination of more than one SSID and more than one MAC address:
    - These scenarios are outside the scope of the IEEE 802.11 standard, as the interaction of Passpoint profiles and ESSs ("SSID"s) is beyond 802.11's scope. Since Passpoint behavior is defined by Wi-Fi Alliance, Wi-Fi Alliance may be better positioned to address this point.
        - We note that multiple, distinct scenarios may be covered by this bullet:
            1. A single device which connects to the same SSID using more than one Passpoint profile, over time.

               We assume an example of this is a device that has multiple subscriptions configured, which are all valid for use on a given SSID (for example, a "neutral host" hotspot)
            2. A single device which connects using the same Passpoint profile across multiple SSIDs.

               We assume an example of this is a single provider network that is available via more than one SSID.
- A single device using different MAC addresses in different bands and/or different SSIDs:

    - Refer to general statement above; the 802.11 WG recommendation is to not use a MAC address as a device identifier.
    - We agree that band steering in this scenario is likely an issue. The 802.11 WG may consider further investigation in this area and collaborate with Wi-Fi Alliance as appropriate.
- Even if the MAC address is "stable" for a given SSID, many client devices will use the broadcast SSID in probe request frames with different MAC addresses
    - Refer to the general statement above; the 802.11 WG recommendation is to not use a MAC address as a device identifier.
    - In this case, we agree that client steering is likely an issue. The 802.11 WG may consider further investigation in this area and collaborate with Wi-Fi Alliance as appropriate.
- Pay per use (PPU), short-term complimentary services, accounting and billing systems, device or user blacklisting, and parental controls that rely on MAC address for identification of user or device:
    - Refer to the general statement above; the 802.11 WG recommendation is to not use a MAC address as device or user identifier.
    - We recommend that all such services and controls use a different method to identify a device, which allows persistent and globally unique identification of the device user without introducing eavesdropping concerns for privacy. Or, even more importantly in these use cases, it is actually the user that should be identified, for convenience and a feature of opt-in/pay-in services, and to control/prohibit the actions of the user correctly for lock-out services.
- Collision of a random address with another randomized, or "real" (globally unique, assigned) MAC address: Collision of MAC addresses will confuse DHCP servers.
    - We refer to specifications IEEE Std 802.11aq™-2018 and IEEE Std 802™-2014 that require a randomly generated address to set the "Local" bit. Such addresses cannot collide with a globally unique, assigned address.
    - As for collisions between two random (or any other "Local") addresses, we refer to the mathematics of the "Birthday paradox". First, note that MAC addresses are only visible within the domain of a single bridged LAN – that is, they are not seen beyond a router, if their use is restricted to layer 2 purposes as recommended. We believe the maximum reasonable "flat" network (bridged LAN) would have an estimated 20,000 users randomizing MAC addresses. An example of such an installation would be to cover an entire sporting arena with a single bridged LAN. Even in this extreme case, the odds against a collision are astronomical.
    - We also would like to point out that work is underway within IEEE 802 in project P802.1CQ, to provide support for centralized control methods that can guarantee address uniqueness, when other constraints limit the size of the address pool.
    - As for DHCP server collisions, this is certainly one side-effect of a duplicated MAC address within a bridged LAN. However, this is only one of many problems such a collision would cause. See the discussion above about the probability of such a collision and methods to avoid it.
- Analytics may rely on MAC addresses for identification.
    - This is another example scenario of the more general statement that services should not rely on MAC address for device or user identification.

    - We realize, however, that some types of network analytics and troubleshooting are done at the low layers of the network stack, and don't have access to high-level concepts for identification. The 802.11 WG may consider further investigation in this area.

- Legal intercept and other legal requirements:
    - For legal requirements such as device ownership and tracking, warrantees, contracts, etc., we refer to the general statements about using a different method for device (and user) identification.
    - For legal intercept, our understanding is that the legal requirements (in layman's terms) are to provide the information that a provider/operator has available.
- Identification of manufacturer, based on OUI portion of the MAC address:
    - We agree, this identification will not work for devices with a randomized MAC address. Again, we refer to the recommendation to use other methods to identify a device, including the device type or manufacturer. We also note that there are "finger-printing" methods that are generally well-known and reasonably effective, that can be used for this purpose.

There are a number of concerns raised in the received WBA liaison which need to be addressed at a "higher layer" by the specific service, system, or purpose which is currently using MAC addresses for identification. These services and systems are generally outside the scope of IEEE 802.11 or even IEEE 802. We recommend that the WBA work directly with appropriate organizations to change to identification methods that will address these issues. The IEEE 802.11 WG is happy to support that effort.

We have identified some issues that might be addressed within the IEEE 802.11 community, in conjunction with Wi-Fi Alliance or IEEE 802. We invite WBA members to join us to further this activity. In particular:

- Client steering and band steering methods rooted in 802.11 features, and further developed or enhanced by IEEE 802 and Wi-Fi Alliance specifications should be investigated.
- Network analytics and troubleshooting
- Device manufacturer identification

We look forward to continued collaboration between the IEEE 802.11 WLAN Working Group and the WBA.

Sincerely,

Dorothy Stanley

Chair, IEEE 802.11 WLAN Working Group