IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11Proposed Response to liaison from Wireless Broadband Alliance (WBA) to IEEE 802.11 Working Group on MAC address randomization impacts |
| Date: 2018-11-13 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Mark Hamilton | Ruckus/ARRIS | 350 W Java Dr,Sunnyvale, CA 94089 |  | mark.hamilton@arris.com  |
|  |  |  |  |  |

**Abstract**

This document contains the proposed response to the liaison statement from the Wireless Broadband Alliance (WBA) on MAC address randomization impacts (11-18/1579r1)

R0: Initial revision; incomplete – need to pick up from where this left off on Oct 11 teleconference.

IEEE 802.11 WLAN Working Group
DRAFT Liaison Communication

|  |  |
| --- | --- |
| Source: | IEEE 802.11 Working Group[[1]](#footnote-1) |
|  |  |  |
| To: | Bruno Tomas | Director – Programs / PMO, Wireless Broadband Alliancebruno@wballiance.com |
| Michael Sym | Chair, WBA Testing & Interoperability Workgroupmicheal.sym@bsgclearing.com  |
|  |  |  |
| CC: | [Konstantinos Karachalios | Secretary, IEEE-SA Standards BoardSecretary, IEEE-SA Board of Governorssasecretary@ieee.org ] |
| Paul Nikolich | Chair, IEEE 802 LMSCp.nikolich@ieee.org |
| Jon Rosdahl | Vice-chair, IEEE 802.11 WLAN Working Groupjrosdahl@ieee.org |
| Robert Stacey | Vice-chair, IEEE 802.11 WLAN Working Grouprobert.stacey@intel.com |
| Mark Hamilton | Chair, IEEE 802.11 ARC Standing Committeemark.hamilton@arris.com |
|  | Tiago Rodrigues | tiago@wballiance.com |
|  |  |  |
| From: | Dorothy Stanley | Chair, IEEE 802.11 WLAN Working Groupdorothy.stanley@hpe.com |
|  |  |  |
| Subject: | Liaison communication reply to *WBA Liaison Statement – MAC Randomization Impacts* |
| Approval: | Approved by the IEEE 802.11 Working Group at IEEE 802.11 [plenary | interim] meeting, [where], [date] |

Dear Bruno and Michael,

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

IEEE 802.11 WG would like to respond with some general comments, and also some specific responses on your detailed bullet points, further below.

In general, to enhance user privacy, IEEE 802.11 recommends against using any MAC address as an identifier for a user or device, ouside the scope of the layer 2 communication. Most of the examples/scenarios provided in the WBA 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 protect the user’s privacy of identity.

We also note that we have received reports that some generally available devices are already using a randomized MAC address for association, extending this behavior beyond the address used for probes and other pre-association interactions.

<are references from 802.11aq and 802.11-2016 needed/useful? It seems that WBA may already know this, perhaps?>

IEEE 802.11 WG believes that IEEE 1609.3 and SAE J2945/1 have deployed MAC address randomization when out of the context of a BSS, and this has been working for years. It seems possible that methods of client identification used in that context could be adapted for use within a infrastructure network, and might provide a starting point for such work.

Specific comments on bullet points:

* 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.
	+ We recognize that this a potential change to current behavior. Appropriate organizations should be brought in to the discussion (as you are doing) to solve the problem within their specific domains.
* Combinations of more than one SSID and more than on MAC address:
	+ We note that multiple, distinct scenarios are 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, that are all valid for use on this same 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’s network that is available via more than SSID.
		3. ??
	+ Both the above scenarios are outside the scope of 802.11, as the interaction of Passpoint profiles and ESSs (“SSID”s) is beyond 802.11’s scope. Since Passpoint behavior is defined by the Wi-Fi Alliance, they may be better positioned to address this point.
* Different bands with different SSIDs:
	+ Refer to general statement above, to not use a MAC address as a device identifier.
	+ Also, we agree that band steering in this scenario is likely an issue. We recommend that 802.11 should look into this, perhaps providing recommendations about SSID assignment, depending on network deployment and goals (there may be scenarios where different SSIDs are necessary/desirable). 802.11 should coordinate with WFA on this topic.
* Even if the MAC address is “stable” for a given SSID, many clients will use the broadcast SSID in probe requests, and hence there is again no stability in MAC address.
	+ Refer to the general statement above, to not use a MAC address as a device identifier.
	+ In this case, we agree that client steering is likely an issue. We recommend that 802.11 should look into this. 802.11 should perhaps coordinate with WFA on this topic, depending on our findings.
* 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, 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. 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. These services should change to a method that allows persistent and globally unique identification of the device user.
* Collision of a random address with a another randomized, or “real” (globally unique, assigned) MAC address: Collision of MAC addresses will confuse DHCP servers.
	+ We refer to the current specifications (IEEE Std 802.11aq, IEEE Std 802) 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 th e”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 (again, as recommended in the general section). We believe the maximum reasonable such “flat” network (bridged LAN) would have maybe 20,000 users – such an installation that decided to cover an entire sporting arena with a single bridged LAN. Even in this extreme case, if at least 44 bits of address are randomized, the odds of a collision are astronomical.
	+ We also would like to point out that work is underway within IEEE, in the P802.1CQ project, to provide support for centralized control methods that can guarantee address uniqueness, when other contraints 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 discuss 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. What do we say here?
* Legal intercept, and other legal requirements:
	+ For legal requirements such a 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, we believe that the legal requirements (in layman’s terms) are to provide the information that a provider/operator has available. If device/user tracking becomes unavailable/unreliable, it is not a legal requirement of the provider/oprator to solve that problem.
* Identification of manufacturer, based on OUI portion of the MAC address:
	+ We agree, this will no longer work. 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.

As can be seen from the above, there are a number of concerns raised by your liaison letter 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. IEEE 802.11 WG is happy to support that effort, if that would be helpful.

We have identified some issues that should be addressed within the IEEE 802.11 community, in conjunction with Wi-Fi Alliance or IEEE 802, perhaps. We will take such activities under advisement, and encourage our members to work on these areas and provide you periodic updates. 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.
* Anything about interaction of Passpoint and SSIDs – or is that entirely in Wi-Fi Alliance’s scope?
* Network analytics and troubleshooting?

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

Sincerely,

Dorothy Stanley

Chair, IEEE 802.11 WLAN Working Group

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. [↑](#footnote-ref-1)