IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Randomized or Changing MAC address Recommendation | | | | |
| Date: 2019-09-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Lili Hervieu | CableLabs |  |  | l.hervieu@cablelabs.com |

Abstract

This submission contains some suggested recommendations for the RCM TIG consideration. Given the scale of the 802.11 networks deployed by service providers, issues related to the use of random MAC address beyond the layer 2 should be addressed by the IEEE 802.11. In particular, methods to uniquely identify a device on trusted 802.11 networks without compromising the user privacy should be investigated.

This material (or part of it) may be integrated into the RCM TIG’s report to the Working Group.

R0 – initial version

**Recommendation**

While it is often recognized that MAC address randomization supports user privacy, it can have a wide range of repercussions impacting not only the 802.11 networks, but also many other related services.  The MAC address being a Layer 2 identifier, its usage was not intended for beyond L2 networking. The IEEE 802.11 Working Group “strongly recommends against using any specific MAC address as an identifier for a user or device, outside the scope of the layer 2 communication”.

However, due to its ubiquity and, so far, expected uniqueness, the MAC address is widely used by Internet Service Providers, Multiple Service Operators, and Wi-Fi network operators for additional purposes including security and access control.  The following are examples of such uses:

* MAC-based access which admits or denies wireless association based on the connecting device MAC addresses (e.g. wireless gateway providing public hotspot services).
* MAC address filtering is often used to add an extra layer of protection on the network (white/blacklist) and enforce policies such as parental control.
* Monitoring, troubleshooting, and analytics of Wi-Fi deployments, including helpdesks, often rely on MAC addresses as part of the client identity.
* Lawful interception makes use MAC address.

Although no recent public data are available, the use of randomization is expected to increase in the near future as more OSs are implementing it. Given the scale of the 802.11 networks deployed by service providers, issues related to the use of random MAC address beyond the layer 2 should be addressed by the IEEE 802.11. In particular, methods to uniquely identify a device on trusted (e.g. service provider) 802.11 networks without compromising the user privacy should be investigated.