Ongoing developments in IEEE 802.11 WLAN standardization

A study group on randomized and changing MAC addresses

Amelia Andersdotter (RCM TIG Chair)
ARTICLE19

1. DEVELOPMENT OF WLAN STANDARDS IN THE IEEE

The IEEE 802 LMSC is one of the most successful network standardization bodies in the world. Responsible for standards such as Ethernet, it is present in virtually all networked environments. The IEEE 802.11, one of its working groups, standardizes 802.11 wireless local area networks (WLAN). The IEEE 802.11 WLAN standard underlies the globally famous Wi-Fi brand, which is developed and maintained by the Wi-Fi Alliance.

The work of IEEE 802.11 is organized into task groups, study groups and topic interest groups, each with their own function in the standardization landscape.

A task group works on developing an amendment to the main IEEE 802.11 standard. A study groups work to prepare the work of a task group. A topic interest group dives deeper into some issue where the working group has not yet determined whether it might need to develop standards amendments.

In the IEEE 802 Plenary meeting in Vancouver, Canada, the 802.11 working group decided that it should establish a topic interest group to look closer into effects of randomized and changing MAC addresses. It has been dubbed the Randomized and changing MAC addresses Topic Interest Group (RCM TIG).[1]

The establishment of the TIG follows the adoption of MAC randomization techniques in the .11aq amendmentto the main standard in June, 2018. The TIG will seek to understand existing MAC randomization schemes, and their impact on networking environments, as well as establish whether any further work - such as the establishment of a study group or eventual task group for futher additions to the standard, are necessary.

All proceedings of RCM TIG, including presentations made to the group, agendas and meeting updates, are available on the IEEE 802.11 mentor system.[2] The work of the topic interest group is expected to conclude in November 2019, and all interested parties are invited to contribute.

The views expressed in this document are those of its author, and should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE or any other individual participating in the IEEE-SA standardization work.

[1] http://www.ieee802.org/11/Reports/rcmtig_update.htm
[2] https://mentor.ieee.org/802.11/documents?is_group=0rcm

2. RANDOMIZED AND CHANGING MAC ADDRESSES

Non-consensual geolocational tracking of individuals in wireless networks is a long-standing concern. Especially the use of clear-text, permanent identifiers, such as MAC addresses, to track individuals who have not even associated to a wireless network has been identified as a serious privacy threat, since end-user clients in practise have few means of protecting themselves against inherent features of their technologies.

At the same time, MAC addresses come encoded with information that are used by network operators in practical situations. A part of the MAC address is, for instance, dedicated to information about which vendor is responsible for the device. This information can be used by network operators to seamlessly compensate for implementation errors in end-client devices, to the benefit of a consumer.

MAC randomization is intended to solve the privacy problem by changing the MAC address of a device at irregular intervals, thereby making it more difficult to tie an identifier to a particular device.

2.1 Different ways to randomize a MAC

Two distinct situations are recognized which have different impacts on network operations:

1. Pre-association: MAC-addresses which are randomized when a client device is not connected to any WLAN, but which revert back to the vendor-given device MAC whenever the client associates.

2. Post-association: MAC-addresses which are randomized when a client device is not connected to any WLAN, and which do not revert back to the vendor-given device MAC when the client associates.

In the first case, a network operator would have a stable, permanent identifier once a device is actually connected to a network. In the second case, a network operator would not have such an identifier.

The two cases present different problems from the perspectives of privacy and network operation.

Using the first method of randomization would allow a network operator to track a connected device across sessions (for instance a returning user). While it takes care of the trivial situation wherein which a consumer walks through a public space without associating to the network, *pre-association tracking*, it could be argued not to sufficiently protect the consumer from the network operators.

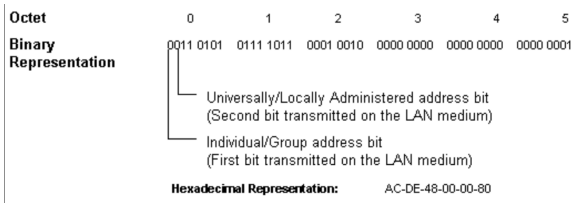

Figure 1: An example of a 48-bit LAN MAC address in both Binary and Hexadecimal Representations. Source: IEEE-SA RAC, Standard Group MAC Addresses: A Tutorial Guide.

Using the second method of randomization would, on the other hand, potentially make it more difficult for network operators to do troubleshooting. This is especially the case if randomization occurs over a large proportion of the MAC address bits, thereby precluding the use of the MAC address to establish device manufacturer identity. Network operators argue that they are the parties most likely to receive customer complaints when a network association does not work, and that post-association randomization therefore risks creating difficulties for them.

At the same time, randomizing over an insufficient number of bits brings other concerns. IEEE 802 networks currently assume that MAC addresses are unique per device once associated to the network. In order for the network to correctly transmit information between parties, such MAC address uniqueness is required. If randomization occurs, it has to be over a sufficiently large space that the risk of MAC address collisions remains sufficiently low.

2.2 MAC randomization in IEEE 802.11

The potential of MAC randomization has been discussed in IEEE 802 LMSC since 2014, both during the development of 802C (a new way of managing MAC identifier allocation), in the proceedings of the P802E Privacy Recommendations Group, and in the creation of the .11aq Pre-Association Discovery amendment.[3]

The lengthiest treatment of MAC randomization in the IEEE 802 LMSC to date was during the adoption of the .11aq amendment.[4] It put to the forefront issues relating to the degree of randomization (the number of bits over which randomization occurs), and whether randomization should happen only during pre-association or whether it can or should have effects post-association.

A standard group MAC address has 48 bits, out of which 2 are pre-allocated for signalling purposes (Fig. 1). It was argued in 2017 that .11aq MAC Privacy Enhancements should cover the all the 46 bits that are not currently used for signalling purposes. However, recent addressing developments in the IEEE 802C standard to accommodate for use-cases in industrial settings require the allocation of two additional bits for signalling. This would bring down the effective number of bits over which randomization could work to 44.[5] The purpose of these two additional signalling bits would to be enable a *structured local address plan* (SLAP), that can assist in separating networks intended for different uses (for instance, separating factory sensors from personal devices).

An Organizationally Unique Identifier (OUI) would typically require 24 bits, and be allocated on the first three octets of a MAC address. If network operators were taken into account, the number of bits over which to randomize would be dramatically decreased.

Whether privacy-enhancing MAC randomization should accommodate for the SLAP, or even for network operator troubleshooting purposes, is in the understanding of this author not yet definitely decided within the IEEE 802. The author further understands that it is within the scope of RCM TIG to bring clarity to some of these issues.

2.3 Lack of data on practical effects of MAC randomization

One challenge for the RCM TIG is that there is relatively little data on practical concerns with randomized and changing MAC addresses.

MAC randomization has been an optional feature of mobile operating systems for a number of years, but research shows that the level of voluntary activation by end-users is low.[6] While Android Q seeks to turn MAC randomization on by default,[7] this version of Android is not yet rolled out and so it is unknown whether network operators will be faced with the challenges they fear.

Re-addressing strategies for MAC addresses were introduced early in vehicular networking standards as far back as 2012[8], but real-life pilot deployments have only been started as recently as 2019.[9] It is not yet known whether re-addressing of MAC addresses bring practical issues for network deployment and maintenance in these scenarios.

The lack of data on practical effects of MAC randomization for network operators makes problem solving difficult.

3. CONCLUSION

The 802.11 RCM TIG is set up to clarify the implications of MAC randomization for network operation. It will looks at ways in which other standards (for instance IEEE 1609.4 or Bluetooth) have reconciled privacy and troubleshooting needs. It may determine a need for new identifiers to compensate for some of the use-cases that were previously covered by MAC addresses, while preserving the privacy-preserving properties of MAC randomization. The group is set to conclude its work with a report, if necessary, in November 2019.

Interested parties are invited to collaborate with the IEEE 802.11 on the work of the topic interest group. Please reach out to `amelia@article19.org` to find out more about the group's work.

[3] https://mentor.ieee.org/802.11/dcn/19/11-19-0588-01-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt

[4] See meeting minutes from 2017 and 2018 at https://mentor.ieee.org/802.11/documents?is_group=00aq

[5] https://mentor.ieee.org/802.11/dcn/19/11-19-0884-00-0rcm-temporary-addresses.pptx

[6] C. Matte, M. Cunche, Spread of MAC address randomization studied using locally administered MAC addresses use historic. [Research Report] RR-9142, Inria Grenoble Rhône-Alpes. 2018. <hal-01682363>

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

[8] IEEE 1609.4 WAVE, 2012.

[9] https://www.its.dot.gov/pilots/