IEEE P802.11  
Wireless LANs

|  |  |  |
| --- | --- | --- |
| Alternate edits to IEEE 802.11 Randomized And Changing MAC Addresses Topic Interest Group Report | | |
| Date: 2019-11-12 | | |
| Author: | | |
| Name | Affiliation | E-mail |
| Mark Hamilton | Ruckus/Commscope | [mark.hamilton2152@gmail.com](mailto:mark.hamilton2152@gmail.com) |
|  |  |  |

Abstract

Proposed edits to 11-19/1442r4, based on comments in 11-19/1789r0.

R1 – updated based on discussion in RCM TIG meeting during Waikoloa session, Tuesday PM1.

Table of contents

[1 Introduction 3](#__RefHeading___Toc5251_3726045101)

[2 Definitions and abbreviations 4](#__RefHeading___Toc5281_3726045101)

[3 Use-cases 4](#__RefHeading___Toc5285_3726045101)

[3.1 Initial infrastructure connection steering 4](#__RefHeading___Toc5667_264680990)

[3.1.1 Randomized MAC address impacts 5](#__RefHeading___Toc5669_264680990)

[3.1.2 Rapidly changing MAC address impacts 5](#__RefHeading___Toc5671_264680990)

[3.2 Access control and arrival detection in a home environment 5](#__RefHeading___Toc5673_264680990)

[3.2.1 Randomized MAC address impacts 5](#__RefHeading___Toc5675_264680990)

[3.2.2 Rapidly changing MAC address impacts 5](#__RefHeading___Toc5677_264680990)

[3.3 “Pairing” smartphone to a car (with 802.11/Wi-Fi) 6](#__RefHeading___Toc5679_264680990)

[3.3.1 Randomized MAC address impacts 6](#__RefHeading___Toc5681_264680990)

[3.3.2 Rapidly changing MAC address impacts 6](#__RefHeading___Toc5683_264680990)

[3.4 Airport security queue measurement 6](#__RefHeading___Toc5685_264680990)

[3.4.1 Randomized MAC address impacts 6](#__RefHeading___Toc5687_264680990)

[3.4.2 Rapidly changing MAC address impacts 6](#__RefHeading___Toc5689_264680990)

[3.5 Grocery store customer flow analysis 7](#__RefHeading___Toc5691_264680990)

[3.5.1 Randomized MAC address impacts 7](#__RefHeading___Toc5693_264680990)

[3.5.2 Rapidly changing MAC address impacts 7](#__RefHeading___Toc5695_264680990)

[3.6 Grocery store frequent shopper notifications 7](#__RefHeading___Toc5697_264680990)

[3.6.1 Randomized MAC address impacts 7](#__RefHeading___Toc5699_264680990)

[3.6.2 Rapidly changing MAC address impacts 8](#__RefHeading___Toc5701_264680990)

[3.7 Infrastructure (home or enterprise) with different SSIDs per band 8](#__RefHeading___Toc5703_264680990)

[3.7.1 Randomized MAC address impacts 8](#__RefHeading___Toc5705_264680990)

[3.7.2 Rapidly changing MAC address impacts 8](#__RefHeading___Toc5707_264680990)

[3.8 Infrastructure (home or enterprise): Probes are randomized, even to/with associated SSID 8](#__RefHeading___Toc5709_264680990)

[3.8.1 Randomized MAC address impacts 9](#__RefHeading___Toc5711_264680990)

[3.8.2 Rapidly changing MAC address impacts 9](#__RefHeading___Toc5713_264680990)

[3.9 Rogue containment in infrastructure networks 9](#__RefHeading___Toc5715_264680990)

[3.9.1 Randomized MAC address impacts 9](#__RefHeading___Toc5717_264680990)

[3.9.2 Rapidly changing MAC address impacts 9](#__RefHeading___Toc5719_264680990)

[3.10 Customer Support and Troubleshooting 9](#__RefHeading___Toc22750_2140853016)

[3.10.1 Randomized MAC address impacts 9](#__RefHeading___Toc22744_2140853016)

[3.10.2 Rapidly changing MAC address impacts 10](#__RefHeading___Toc5707_2646809901)

[3.11 Residential Wireless Gateway with Hotspot 10](#__RefHeading___Toc22752_2140853016)

[3.11.1 Randomized MAC address impacts 10](#__RefHeading___Toc22746_2140853016)

[3.11.2 Rapidly changing MAC address impacts 10](#__RefHeading___Toc22748_2140853016)

[4 Required .11 features for enabling use-cases 10](#__RefHeading___Toc5303_3726045101)

[4.1 MAC address change timing 11](#__RefHeading___Toc5721_264680990)

[4.2 Alternative identifiers 11](#__RefHeading___Toc5723_264680990)

[4.3 Issue recommendations on SSID assignments 11](#__RefHeading___Toc5725_264680990)

[4.4 Correlation of information elements 11](#__RefHeading___Toc5727_264680990)

[5 Recommendations to .11 leadership team 12](#__RefHeading___Toc5311_3726045101)

[5.1 Title TBD 12](#__RefHeading___Toc5313_3726045101)

[5.2 Broader work on privacy 12](#__RefHeading___Toc5315_3726045101)

[6 References 12](#__RefHeading___Toc5319_3726045101)

# Introduction

MAC randomization has been visible in IEEE 802 LMSC since 2014. The future expected prevalence av MAC randomization techniques was, for instance, raised by commenters in the draft 0.3 ballot of what is now IEEE 802C.

The privacy threat mitigation potential of MAC randomization was also studied by 802 LMSC members at the Privacy ECSG in 2014 ([privecsg-14-0026-01-0000](https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0026-01-0000-secure-moderated-random-mac-addresses.ppt), [privecsg-14-0025-01-0000](https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0025-01-0000-wifi-privacy-network-experiment-at-ietf91.pptx)) and 2015 ([privecsg-15-0028-00-0000](https://mentor.ieee.org/privecsg/dcn/15/privecsg-15-0028-00-0000-wifi-privacy-network-experiment-at-ieee-802-may-plenary-and-ietf91-meetings.pptx)).

Together with the assessment of software-driven MAC randomization referenced above, this work lead to the inclusion of MAC randomization as a privacy enhancing feature in the .11aq Pre-Association Service Discovery Task Group amendment to the 802.11-2016. This work can be revisited at the "TGaq (inactive)" repository of the 802.11 mentor website. The .11aq amendment was approved by the IEEE Standards Association Standards Board in June 2018.

In September 2018, three months after the publication of the official 802.11aq amendment, the IEEE 802.11 WG received a liaison statement from the Wireless Broadband Alliance (WBA) detailing network operator concerns with the disappearance of clear-text sufficiently-permanent unique device identifiers ([11-18-1579-00-0000](https://mentor.ieee.org/802.11/dcn/18/11-18-1579-00-0000-2018-09-liaison-from-wba-re-mac-randomization-impacts.docx)).

The ARC SC made efforts to address the concerns raised by the WBA in a response approved by the 802.11 Working Group in November 2018 ([11-18-1988-02-0arc](https://mentor.ieee.org/802.11/dcn/18/11-18-1988-02-0arc-proposed-response-to-liaison-from-wba-on-mac-address-randomization-impcats.docx)). In this response, the Working Group noted that some issues raised by WBA merit further consideration.

While it is recognized that MAC address randomization supports user privacy, changing MAC addresses can have a wide range of repercussions impacting not only 802.11 networks, but also many related services.  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. 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”.

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.

# Terminology

Within this document, the following terms are used for differing aspects of MAC address usage. Note, these terms are not mutually exclusive, but form a hierarchical structure of concepts.

**~~Randomized~~ Local-ID MAC address:** An individual MAC address (layer-2 MAC/PHY entity identification, or more specifically a MAC SAP identification) used by a MAC entity as its identification, but that is not assigned as a globally unique and permanent identifier. Such randomized MAC address should have the U/L bit set to indicate a local MAC addresses, per Std IEEE 802. ~~The duration of use of the randomized address could be permanent or only for a shorter duration.~~  Such a randomized address can obscure the real identification of the device and/or its user, for purposes of privacy, for example.

**Changing MAC address**: A subset of Local-ID ~~Randomized~~ MAC addresses which are ~~also~~ changed over time. Such changes may be periodic, event driven, context-dependent (such as SSID-based), or triggered by other inputs. Note that IEEE 802.11 requires that a device’s MAC address not change during the lifetime of an association to an ESS. However, the time bounds of such an ESS association are not always clearly specified or signalled in 802.11, and the interpretation of this requirement is varying across implementations.

**Rapidly changing MAC address**: A Changing MAC address which is generally changed within a time-frame that is approximately equal or less than the time constants for an 802.11 feature, usually impacting the feature’s correct operation.

NOTE – common usage of “randomized MAC address” appears to apply to any (or all) the terms above.

NOTE—the interval that defines whether a changing MAC is rapidly changing varies with the feature and use case being considered, but is generally on the order of several minutes or less. For instance, changing MAC address in each probe request, or changing MAC address between each new association to the same ESS.

# Use-cases

RCM TIG has explored different use-cases that are impacted by the expected future prevalence of randomized and changing MAC addresses in 802.11 networks.

## Initial infrastructure connection steering

A ~~Wi-Fi~~802.11 enabled smartphone is configured to prefer 802.11/Wi-Fi over cellular connection, to save the owner costs for their cellular plan. The users bring the phone within range of a multiple-AP infrastructure to which it has attached previously and has a stored configuration, for example at the user’s work or church. Before connecting to the Wi-Fi, the phone scans to discover the available APs, by sending Probe Requests, ANQP or other public action frames, etc.

During this scanning, the infrastructure monitors the signal levels received from the smartphone at multiple APs and bands on those APs, determines which AP and band will provide the best service, and steers the client to that AP. This saves the client power by directing its scans to shorten its scan and AP selection procedure and lower the requirement for the client to thorough scan all APs and bands, and also saves the infrastructure from needing to steer the client after attachment which saves time, connection disruption and bandwidth for management frames.

### Randomized MAC address impacts

None.

### Rapidly changing MAC address impacts

If the connecting device changes its MAC address frequently while scanning, in extreme with every Probe Request, for example, the infrastructure does not have a way to correlate the different Probe Requests to make correct steering decisions.

## Access control and arrival detection in a home environment

Consider a parent with children of ages 10 and 7 years. The parent wants to block access to the home 802.11/Wi-Fi and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the Wi-Fi, without launching an application or using a portal. And, this needs to use a method that the kids can’t hack and circumvent. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the Wi-Fi and Internet; thus unknown devices need to be distinguishable from one of the family’s devices. Parental control offered in Wi-Fi routers is usually based on the MAC address of the device.

Similarly, two trends in home automation are converging: use of 802.11/Wi-Fi as the ‘backbone’ of the automation system; and a feature of the automation system which allows it to recognize when one of the residents arrives and “welcoming” them home by turning on lights, music, etc., tailored to the individual. This convergence means that using Wi-Fi to detect the individual’s arrival, by detecting their personal Wi-Fi device (smartphone, etc.) is a highly desirable capability. Currently, this device recognition is usually done based on the MAC address.

### Randomized or Changing MAC address impacts

The home Wi-Fi network itself has little value in changing its MAC address with any frequency, since there is little privacy loss in knowing that a MAC address associated with the home is detected in the home. However, the phones and laptops using a randomized MAC address means that the home network cannot recognize or determine when a “authorized” phone is in range and should be allowed on the network, or what permissions should be granted once it is associated. If the randomized address is static, this can be resolved by providing the user easy and clear access to the address actually in use, to configure this address into the home system. However, a changing MAC address will defeat this ability.

### Rapidly changing MAC address impacts

Interactions between the phones and laptops and the home network will be done within the context of an association, so the MAC addresses should not be changing. However, the privacy aspects of whether there is a concern with being to identify when a particular individual is home (or at least their device is) could be explored. This is outside the scope of the random/changing MAC address study, however, and better belongs in a more advanced privacy study.

## Discovery and association between smartphone and a car (with 802.11)

Many modern cars have Wi-Fi capabilities. A common facility also available for some time is the ability to “pair” the smartphone to the car to access messages, calendar, contacts, etc, and make phone calls. This has largely been done with Bluetooth, but since the car has Wi-Fi already, a Wi-Fi based solution could be preferable.

For security reasons, to accomplish discovery once having done this pairing, likely an association is created (infrastructure or peer-to-peer) based on either the car recognizing the phone and querying it with a security validation, or the phone needs to recognize car and initiate the security validation. However, both devices are likely to change their MAC addresses for privacy reasons, which can make their ability to recognize each other difficult.

### Changing MAC address impacts

Due to the car changing its MAC address frequently enough to prevent tracking, the phone no longer can detect which car it should pair to. Similarly, the phone changing its MAC address frequently enough, also for the same privacy/anti-tracking reasons, means the car cannot recognize or determine when a “paired” phone is in range and appropriate to initiate the security negotiation.

### Rapidly changing MAC address impacts

In this situation, both the car and phone need to maintain their MAC addresses during their association to allow ongoing interaction. However, this creates potential privacy concerns, as the car and phone are now easily tracked for the duration of the phone-car pairing/association. Rapidly changing MAC addresses to prevent tracking will also have the side-effect of breaking the connection and thereby the ability to share the desired information and applications.

## Airport security queue measurement

Airport security (and immigration) line wait times can reach times of an hour or more. It has become a feature of airports to offer information about lines’ wait times to passengers, which requires the ability for an automated system to measure the “average” time individuals are spending in these lines.

A common idea for such measurement is to “track” the 802.11/Wi-Fi devices carried by people in the lines through their exposed MAC addresses, and detect how long the devices are, effectively, stationary in the area of the queue.

Such tracking generally needs to be effective on devices that are not connected to any network, especially, for example, in an airport where the Wi-Fi is a fee-based service, so few people are attached. Further, the tracking needs to be effective across time spans of an hour or more for worst-case busy hours, when the information is most critically needed and needs to be accurate.

### Randomized MAC address impacts

None. The airport has no need for identification of the specific device or user.

### Rapidly changing MAC address impacts

If the device’s change their MAC address frequently while in line, it will be difficult or impossible for the infrastructure to make a determination of time spent in the immediate area.

## Grocery store customer flow analysis

It is now common for a grocery store (or similar retail spaces) to do considerable analysis of the “traffic flow” of their customers. Doing this lets the store recognize the areas that are frequented by most/many customers and also the common pairings or patterns of multiple areas that are frequented in the same visit by many customers. This could be reasons that help the customer (putting frequent items near the front of the store, putting common combinations near each other), or that help the store despite the customer (putting frequent items or frequent combinations far apart, to force the customer to walk through the rest of the store), but either way, someone is benefiting and expects to be able to gather the information to implement their policy.

However, the store does not need to have any information about the actual identity of the people being tracked. Further, the store needs to track people that have no relationship with the store, and are not associating to the store’s network, e.g. through tracking the MAC addresses of public/non-associated frames from their Wi-Fi devices.

To discover useful patterns, the store needs to track individuals for a reasonable period of time – say, roughly a half hour at a minimum.

### Randomized MAC address impacts

None. The store has no need for identification of the specific device or user.

### Rapidly changing MAC address impacts

If the devices change their MAC address frequently while in the store, it will be difficult or impossible for the infrastructure to make a determination of the foot traffic patterns.

## Grocery store frequent shopper notifications

A very different use case from the grocery store foot traffic analysis, is a grocery store that wants to recognize and reward frequent shoppers. This is likely to be an “opt-in” service, where the shoppers that are interested in participating with the store indicate that they are willing to have the store know some identity that the store can use (possibly not their true or complete identity, however). For maximum effectiveness, such programs need to recognize when the customer enters (or approaches) the store, and provide information (such as daily specials for frequent shoppers) without any action on the user’s part. Additionally, the store could be able to build a profile of the user, and push content (with a cellular txt, perhaps, since the customer may not be associated to the store’s network) such as items of likely interest to the customer and are on sale/special, when the customer is near those items in the store. It is likely all this is accomplished by detecting the pre-known MAC address of the customer’s Wi-Fi device(s)’ public/non-associated frames.

### Randomized or Changing MAC address impacts

Very different from the foot traffic analysis use case, the frequent shopper use case does need a stable identification of the customer (or their commonly carried device), without requiring any user action nor an association with the store’s network.

In many ways, this use case is similar to the home automation and parental controls use cases. One important difference is that the user may not want to divulge true identity information to the store. But, even if a method is proposed for a pseudonym identity, such an identity needs to have a very long lifetime (months or years), and needs a method to still protect the user’s privacy from third parties (but not from the store itself).

### Rapidly changing MAC address impacts

Interactions with the store could often be done without an association, yet the need for a long-lived identification still applies. So, whatever is used for this identification of the customer (MAC address or otherwise) needs to be stable and re-used within the area of the store, for months or years.

## Infrastructure (home or enterprise) with different SSIDs per band

This use case is in reaction to two situations: first is a network where (for whatever reason, perhaps incorrectly) the network (a single LAN, really) has been deployed with different SSIDs on different bands (“XYZ24G” and “XYZ5G”, for example); and second is considering a device that will use a consistent MAC address for a given SSID, but generates a new random address for each new SSID. These scenarios have both been seen, relatively commonly, in the field.

In combination, these two scenarios result in the network infrastructure being unable to correlate the device’s signals, location, and network interaction on the two bands, which makes band steering effectively impossible.

### Randomized MAC address impacts

It is not the randomization of the MAC address that is a direct impact in this use case, but the scope of that randomization. If the randomization is tied to the SSID, the problem will occur.

### Rapidly changing MAC address impacts

Not directly applicable. The duration of the two MAC addresses being used by the client is orthogonal to the problem in this use case. It is noted that even devices that keep a given MAC address (for a given SSID) permanently, will still have the issue.

## Infrastructure (home or enterprise): Probes are randomized, even to/with associated SSID

A client that is using randomized MAC addresses could easily have an implementation that generates a new random MAC address for every Probe Request. This could even apply to Probe Requests that are directed to the associated SSID, when the client would otherwise use a consistent MAC address for transmissions within an association.

If the client has this extreme (or approaching this extreme) an implementation of MAC address randomization, it will have a strong impact on the infrastructure’s ability to making steering decisions for that client.

When attached to a multiple-AP infrastructure, if the client uses the stable MAC address when probing, the infrastructure can help steer the client across both APs and bands, to give the entire network better experience. This could apply to both directed probes and broadcast probes, too.

### Randomized MAC address impacts

Similar to the Infrastructure with different SSIDs per band use case, it is not the randomization of the MAC address that is a direct impact in this use case, but the scope of that randomization. If the randomization applies to Probe Requests even when the device is associated, then the problem will occur.

### Rapidly changing MAC address impacts

Not directly applicable (or entirely the point, depending on how you look at it). The duration of the stable MAC address being used by the client while associated is orthogonal to the problem in this use case. It is a question of whether Probe Requests are treated as special traffic even while associated, and do not use the stable MAC address.

## Rogue containment in infrastructure networks

A managed WLAN network may consider the deployment of rogue containment measurements which prevent un-authorised access points and/or stations from operating in its service area. (Note that such prevention of third-party operation may be illegal in some contexts or jurisdictions.) One such rogue containment mechanism entails de-authenticating users associated to access points which have not been previously allow-listed. Part of the allow-listing information required for this to work, is the MAC addresses of the AP and STAs respectively.

In order to start an AP in the area, the AP and STAs connecting to it will need to be allow-listed by the infrastructure network. For STAs periodically randomizing MAC addresses, the absence of a permanent identifier will preclude white-listing by the rogue containment mechanisms.

### Randomized or Changing MAC address impacts

STAs will not be able to be allow-listed in the infrastructure, and will therefore not be able to connect to the newly deployed APs. Similarly, rogue STAs will be more difficult to discover and track.

### Rapidly changing MAC address impacts

The faster the speed of change the more difficult to detect, track and/or allow-/block-list STAs.

## Customer Support and Troubleshooting

Service providers are deploying wireless gateways in residential environments. With about two thirds of customer complaints related to WLAN, operators have to be able to provide top-notch technical support when a subscriber faces WLAN-related issues.

As an example, a subscriber has 16 devices connected to their Wi-Fi network. They have set-up different SSIDs for their guests, their kids, and their personal devices.  The subscriber is experiencing connectivity and low performance issue on their wireless network. When they call the technical customer center, the technician is able to identify the MAC address of the faulty device and ask the subscriber to reset its device and reconnect to the wireless network.

### Randomized MAC address impacts

The technician uses the MAC address OUI of the device to point out the device manufacturer to the subscriber. If the device uses a locally administered randomized MAC address, the subscriber must determine and check the randomized MAC address of each individual device to figure out the faulty device, increasing the troubleshooting time. Troubleshooting is also more difficult if the device uses a different MAC address per SSID.

### Rapidly changing MAC address impacts

A rapidly changing MAC address (i.e. every 24 hours or less) will impact the ability of troubleshooting the Wi-Fi network, especially when intermittent issues are observed over long period of time.

## Residential Wireless Gateway with Hotspot

Service providers are deploying residential wireless gateways with public hotspots to expand their network coverage and capacity. With millions of hotspots available, subscribers can enjoy the benefit of complementary and seamless Wi-Fi connectivity while on the go. When a subscriber is at home, however, their devices should connect to the wireless home network rather than the hotspot available on the residential gateway. If a device connects to the hotspot, the subscriber doesn’t have access to their local network, cannot print files or access storage attached to the network. Neither can they enjoy their gigabit subscription. The gateway can prevent “home devices” from connecting to the hotspot based on their expected unique MAC address~~es, by “blacklisting” those devices’ MAC addresses on the hotspot.~~

### Randomized MAC address impacts

When a device uses a different MAC address per SSID, the gateway cannot enforce the device connection to the home network rather than the hotspot. The subscriber has to manually connect their device to the home SSID.

### Rapidly changing MAC address impacts

The impact is similar the Randomized MAC address case.

# Required 802.11 features for enabling use-cases

Different methods can be used to enable each of the use-cases addressed in section 3. The group has considered remedial features in the following broad categories:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Possible enabling measures \  Use-case in section | 3.1 | 3.2 | 3.3 | 3.4 | 3.5 | 3.6 | 3.7 | 3.8 | 3.9 | 3.10 | 3.11 |
| A smallest interval between MAC address changes | X |  |  | X | X |  |  |  |  |  |  |
| Recommendations for naming of SSID |  |  |  |  |  |  | X |  |  |  |  |
| Introduction of alternative layer 2  identifiers and method for carrying this identifier without breaking privacy |  | X | X |  |  | X |  |  | X | X | X |
| Correlation of information elements | X |  |  | X | X |  |  | X |  |  |  |

## MAC address change timing

Infrastructure connection steering, and airport queue measurement and grocery store flow analysis use-cases are all possible as long as the MAC address does not change too often. Recommendations for, or mechanisms to control, the timing at which the client changes its MAC address while probing can manage the loss of correlation.

The current proposed defaults from a major deployer of accessible, default MAC address randomization for end-users duration of a MAC address pertaining to an un-associated device is 30 minutes. This is not expected to unduly interfere with these use-cases (although, at times, it may be too short for airport security queue measurement)

## Alternative identifiers

Access control and arrival detection in a home environment and grocery store frequent shopper notifications use-cases would be possible if there was a method for an infrastructure network to recognize a client device after they have been apart for a long time and the device has changed its MAC address.

This method must not introduce privacy concerns by exposing personal information about the presence of individuals at home (or decide that this is not a significant privacy concern). It must also not introduce privacy concerns by exposing trackable information about the individual to third-parties.

One such solution has been discussed in IEEE 802.11 ARC SC and IEEE 802.11 RCM TIG (see doc.: IEEE 802.11-19/179).

## Recommendations on SSID assignments

The Infrastructure with different SSIDs per band use-case would be mitigated if there were recommendations that infrastructure networks that are actually a single LAN be deployed using a single SSID across the entire network, including multiple APs and multiple bands.

Such recommendations could be issued by those bodies that influence network operators, and may not need to be issued by the IEEE 802.11 WG. They could also be placed in an annex to the 802.11 standard.

## Correlation of information elements

An alternative way of enabling the Infrastructure connection steering, and airport queue measurement and grocery store flow analysis use-cases is to provide another method of recognizing when traffic from a device while not associated is from the same device (probing across channels and bands). This could be a method for an infrastructure network to correlate a client device’s traffic, despite its use of more than one MAC address in that traffic.

# Recommendations to 802.11 leadership team

## Title TBD

## Broader work on privacy

Throughout the work of RCM TIG, it has been evident that there is a desire in IEEE 802.11 to discuss broader privacy topics relating to 802.11 technologies. RCM TIG therefore recommends the formation of a Privacy TIG with a mandate to explore a broader range of privacy issues relating to 802.11 networks.

The Privacy TIG should be tasked with identifying privacy and security failures relating to 802.11 technologies, as well as the need for future work by the WG to address such pitfalls.

# References