IEEE P802.11
Wireless LANs

|  |
| --- |
| Issues Tracking |
| Date: 2021-07-13 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA | +1 303 818 8472 | mark.hamilton2152@gmail.com  |
|  |  |  |  |  |

Abstract

Issues Tracking sheet for P802.11bh - Operation with Randomized and Changing MAC Addresses.

R0 – Initial discussion document.

R1 – With modifications/updates/notes from still-in-progress discussion of the Terminology section, from March 9 meeting.

R2 – Removed other “example” material in sections 3, 4 and 5. Task group will insert this material as it is reviewed and agreed.

R3 – Updates in sections 3 and 4, from March 29 teleconference.

R4 – Editorial clean-up/organization, which moved clause numbers. Prep for April 12 teleconference.

R5 – Added text/notes in section 4 (and a little in section 5)

R6 – Added explicit acknowledgement that some use cases may not result in text changes to Std 802.11, but will be noted as having solutions that are out of 802.11’s scope or already exist in 802.11 features.

R7 – Updated discussion on “Parental controls” (post-association access control) and added Airport security and Grocery store (flow analysis and frequent shopper notifications) use cases with discussion. All discussed during May session; all pending specific text contributions to capture that discussion and agreements.

R8 – Updated during June 14 call, use cases: Infrastructure (home or enterprise) with different SSIDs per band; and Infrastructure (home or enterprise): Probes are randomized, even to/heard by associated AP.

R9 – Updated during June 28 call, use cases: Rogue detection in infrastructure network; Rogue APs; Soft AP; Onboarding a “known” MAC address; Customer Support and Troubleshooting.

R10 – Updated during July 13 meeting of July plenary, use cases: Residential Wireless Gateway with Hotspot, Pervasive surveillance, Emergency services (pre- or post-association), Public Wi-Fi hotspot and roaming (AP to AP); TBC: WBA liaison use cases.

**Table of Contents**

[1 Introduction 3](#_Toc77075805)

[2 Terminology 3](#_Toc77075806)

[3 Brainstorming ideas/discussion 4](#_Toc77075807)

[4 Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used 4](#_Toc77075808)

[4.1 Pre-association client steering (AP steering, band steering, network steering) 4](#_Toc77075809)

[4.2 Post-association access control (Parental controls, etc.) 5](#_Toc77075810)

[4.3 Post-association home automation (including arrival detection) 5](#_Toc77075811)

[4.4 Airport Security Queue 5](#_Toc77075812)

[4.5 Grocery store customer flow analysis 6](#_Toc77075813)

[4.6 Grocery store frequent shopper notifications 6](#_Toc77075814)

[4.7 Infrastructure (home or enterprise) with different SSIDs per band 6](#_Toc77075815)

[4.8 Infrastructure (home or enterprise): Probes are randomized, even to/heard by ~~with~~ associated AP ~~SSID~~ 7](#_Toc77075816)

[4.9 Rogue detection in infrastructure network 7](#_Toc77075817)

[4.10 Rogue APs 8](#_Toc77075818)

[4.11 Soft AP 8](#_Toc77075819)

[4.12 Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address? 8](#_Toc77075820)

[4.13 Customer Support and Troubleshooting 8](#_Toc77075821)

[4.14 Residential Wireless Gateway with Hotspot 9](#_Toc77075822)

[4.15 Pervasive surveillance 9](#_Toc77075823)

[4.16 Emergency services (pre- or post-association) 10](#_Toc77075824)

[4.17 Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??) 10](#_Toc77075825)

[4.18 WBA liaison use cases…. Graham Smith doc: 11-21/1141 10](#_Toc77075826)

[5 Issues and analyses – discussion of 802.11 features/actions, per se 10](#_Toc77075827)

[5.1 Keep in mind, MAC address policy from the infrastructure 10](#_Toc77075828)

[5.2 Pre-association “steering” 10](#_Toc77075829)

[6 Proposed Solutions 10](#_Toc77075830)

[6.1 … 10](#_Toc77075831)

[6.2 … 10](#_Toc77075832)

# Introduction

This document serves as a tracking sheet for issues raised within the context of P802.11bh, Operation with Randomized and Changing MAC Addresses.

Section 3 is a “scratch pad” for brainstorming comments and ideas, and other discussion points to remember.

Section 4 has a set of use cases which provide real-world example contexts in which some issue(s) arise from randomized and/or changing MAC addresses. These include use cases that have been identified for which we believe either the solution is outside our scope, or the solution already exists, and we will so comment on the use case. (That is, the use cases list includes all the use cases that the task group has considered, even when the conclusion is that no changes are needed/appropriate in IEEE Std 802.11.)

Specific technical issue are then presented in Section 5, including a technical description of the scenario which raises the issue (and mapping back to relevant use case(s)), the technical details of the problem, and the impacts on the overall system including what users/components are impacted, what 802.11 features are

Section 6 provides proposed technical solutions to address the issues (including mapping back to the specific issue(s) addressed by each solution), and discussion of any trade-offs or shortcomings of the solution.

# Terminology

**Randomized 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 either not assigned as a globally unique or is not a permanent identifier (in what scope?).

NOTE: Such randomized MAC address should have the U/L bit set to indicate a local MAC addresses, per Std IEEE 802-2014. For the scope of this document, no compliance with 802c-2017 or P802.1CQ direction is assumed.

NOTE: 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.

Syn: Local MAC address (OR… do we say it is a special case of Local MAC address, and say something about how it is special?)

Something about 802c-2017??

When dot11MACPrivacyActivated??

P802.1CQ??

**Changing MAC address**: A MAC address which is also changed over time. Such changes may be periodic, event driven, 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 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—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.

# Brainstorming ideas/discussion

* Lawful intercept requirements and/or limitations
* Use cases where privacy is desired/expected
	+ Privacy from whom?
	+ Privacy of what information? MAC address, and/or other information. How is the information used?
	+ User consent?
* Use cases where RCM is causing issues
* Pre-association and/or post-association (to the ESS) use cases
* Network operator monitoring location of assets
* Duplicate MAC addresses and issues caused
* STA “doesn’t want to/care about maintaining state” with the network
* What does it mean (or multiple meanings) for “opt-in”
* What is the limit of our PAR scope on privacy concerns being created?
* TGaz ranging, pre-association or post-association, TGaz’s security?
* TGbc features (pre-association/non-associated)

# Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used

## Pre-association client steering (AP steering, band steering, network steering)

The user brings a phone within range of a multiple-AP infrastructure . Before connecting to the 802.11 network, the phone scans to discover the available APs, by sending Probe Requests, ANQP or other public action frames, etc.

* This is for infrastructure that can do multi-AP steering. A single AP multi-band might do that.
* Use case splits: previously visited network might imply re-use of same MAC address, or there might be a feature to change MAC address anyway
* Use case splits: device might have an SLA “agreement” with a previously visited network
* Use case splits: Device is probing specific SSID, or Broadcast SSID

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 avoiding requiringit scanning all supported channels 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.

## Post-association access control (Parental controls, etc.)

People want all their devices to be recognized when attaching to the 802.11 network and control access to Internet content based on the user of various devices, without launching an application or using a portal. And, this needs to use a method that isn’t easily hacked and circumvented. For a visiting device, the deviceshould be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the approved devices. For example, existing parental control offered in 802.11 routers is usually based on the MAC address of the device. Another example: pass/block list.

<Debate about this being within our scope.> Real-world example needed.

Hotel access (portal, pay, etc.) in here??

## Pending contribution with description, and analysis that solutions for this use case are beyond 802.11 scope.Post-association home automation (including arrival detection)

Similarly, two trends in home automation are converging: use of 802.11 technologies 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 the 802.11 network to detect the individual’s arrival, by detecting their personal 802.11 device (smartphone, etc.) is a highly desirable capability. Currently, this device recognition is usually done based on the MAC address.

Key point: the device (user) is voluntarily opting-in to this system. Also key that protection from third-party tracking is included. Pending contribution to specify that scope.

<Similar to hotel scenario?> Application function? Device-initiated Action frame (with crypto content, in mutual authentication RSN network) function?

<Is there any issue with associating to the home work, upon arrival?> The use case “problem” here is really the individual recognition.

## Airport Security Queue

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 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 802.11 network 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.

<Such tracking without “opt-in” by the user is considered a violation of privacy that MAC address randomization is designed to prevent. This can be accomplished in other ways, without 802.11 involvement. We do not need to address this issue. Pending contribution to indicate this was considered and dropped.>

## 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 address of public /non-associated frames from their 802.11 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. At reasonable/lower cost.

<But, this is a privacy concern – “crosses the line” for our PAR scope? Or, only do this with an “opt-in”? Pending contribution to indicate this was considered and dropped.>

## 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 text, perhaps, since the customer may not be associated to the store’s network) such as items that 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 802.11 device(s)' public/pre-associated frames.~~

<Pending contribution and further discussion: This is probably in scope, IFF limited to “opt-in” by the user. Could add the “opt in” step to the above use case description.>

## 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, under single network management, 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 Local-ID MAC 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 infrastructure band steering effectively impossible.

<Is this out of scope, because it is an “incorrect” deployment to use different SSIDs? Rather than band steering (different SSIDs means this is intentionally “manual band steering”, not infrastructure band steering), something about different IP addresses, depending on which SSID (and therefore MAC address) is used? Is BTM (for example) supported across ESSs, or across SSIDs (REVme question?)?

Other use case scenarios from more than one SSID for a given “network”? (Alternative for second paragraph above.) Device would end up not having a consistent MAC address, when connected to this network. CF: 802.11aq: if the client is expecting to have shared state with the AP (network) it must use the same MAC address for interactions with that AP/network.

More than one SSID for a given “network” (ESS?) is not legitimate for 802.11. But what about more than one ESS that are inconnected in a “network”? (That’s beyond TGbh scope to address.) So, impacts from MAC address results are not in our scope. >

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

A client that is using Local-ID MAC addresses could easily have an implementation that generates a new Local-ID 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.

<11aq: “The non-AP STA connecting to an infrastructure BSS shall retain a single MAC address for the duration of its connection across an ESS.” -- should that be also “in the scope of its connection”?

Is this “hidden” state information the infrastructure (might be) keeping about the client? So, the infrastructure desires the “11aq rule” of not changing MAC address, to keep this state. But, is this out of scope, and potentially broken by passive scanning, etc.?

Note: Current text seems to require the AP to send Probe Response. But, can also use steering mechansisms, and information in the response can be varied (if the response is directed?). >

## Rogue detection in infrastructure network

A managed WLAN network may desire to detect rogue, un-authorised access points and/or client stations operating in its service area. One such rogue detection mechanism entails monitoring for users associated to access points which are not known to be part of the managed network. The MAC addresses of the known APs are kept in a database, and the medium is monitored for Beacons or other broadcast traffic from, or non-AP STAs’ traffic to, APs not on the known AP list.

Non-AP STAs could also be listed on a known client list, by MAC address, and thereby unexpected/unwanted client devices in the service area can be detected, by detecting unknown MAC addresses.

When a rogue AP or STA is detected, appropriate action (such as contacting the owner) can be taken to resolve any issues such as interference with the operation of the managed WLAN.

<Rogue non-AP STA? In a (physically) controlled/secured environment, should know all the clients. Couldn’t an attacker spoof a known client’s address? WIPS will detect this and alarm. For authorized clients, is this the same as other post-association authorization cases? What about an authorized device before it associates/as it is probing? Will an RCM device use a “known” MAC address for probing a known SSID (only after detecting the SSID is present, just before associating)? Maybe, but not for broadcast probes. Authorized devices may need a specific policy (when we get to solutions)?

## Rogue APs

Soft AP problem: In enterprise (controlled environment). Beyond/not really a RCM problem, but some higher agreement problem?

Off-the-shelf systems/solutions (that use Wi-Fi):

Not a use case affected by RCM. Might be another policy controlled situation, to retain MAC address.

## Soft AP

Causing connectivity issues if BSSID changes. Maybe okay, if only used for short time. Shall not change while clients are connected. Shall not change while beaconing (and do tear down after a timeout if no clients are attached)? Might make recommendations; but note that 802.11 doesn’t have “soft AP” concept (yet).

## Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address?

Policy can handle secure environment. But, doesn’t solve onboarding.

Device count, of active devices (per credential), for BYOD environment. What about PSK/Passphrase networks (non-unique credentials)?

## 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 802.11 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. Or, one of the devices in the residence is violating a policy, is detected by the ISP, and gets the entire residential service turned-off. 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.

Broaden to cover enterprise case…

<RCM makes the technician identifying a problematic device difficult.

RCM complicates identifying the device type from OUI.

Diagnosing actors: SP, AP vendor, WLAN admin. >

## 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 802.11 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.

<Should the client device make this decision, connecting to the correct network? Or, should the public hotspot side of the gateway steer clients that connect to the “wrong” side? Agreed the client should handle this. Note that solutions for other use cases *might* happen to apply/help with this, but we will not target this use case. Perhaps not even a valid use case – we should not prevent clients from attaching to either network.

Bigger issue (beyond TGbh scope?) to do ESS steering of clients? >

## Pervasive surveillance

Some organizations, both public and private, have a strong desire to monitor people in their behavior and habits. Having a device constantly emitting a unique identifier can help such these organizations surveil people. When people move around, sensors that passively detect these unique identifier emissions can make note of the identifier. Time and location of the sensor can combine with this datum to create a large database of information that can enable tracking of people. Habits can be recorded and observed and deviations from an established baseline can result in an alert regarding the person’s behavior. Artificial intelligence and big data analytics can use this database of information to facilitate this effort. A database of who is where and when can be used for a multitude of purposes, some benign and some nefarious. Records in the database can be used as evidence in a government’s case against a citizen, and personal, and private information about people can be sold without their knowledge or approval.

802.11 is an obvious technology to build such a surveillance apparatus. Fixed MAC addresses will be used in mobile devices even when SIM cards are swapped out or removed. Laptops typically do not have a method of network access that is not bound to a MAC address. The tendency of unconnected devices to find a network results in active probing which can be passively detected, thereby enabling the surveillance apparatus. Indeed, the very nature of 802.11 network discovery and connection establishment compels exposure of MAC addresses and there is no way to disable their use. Using 802.11 to construct a surveillance database is an obvious choice.

<Privacy protection laws come into play. Governments, however, may sometimes override such laws (legally), to protect citizenry against criminals and terrorists for example. How do we support equipment that can comply with local regulations (both privacy, and legal tracking regulations) – but still protect privacy as required by our PAR? Balancing act, versus profiling, etc.

Opt-in or not (how this is different from a store/mall knowing a customer is present)? Document reference for legal intercept scenario? Are there legal intercept requirements for such tracking (or is it “if available”, not “compelled” – on the user, or on the provider)? IEEE 1609 might be an example, to help understand any requirement on 802.11.

Direction: we don’t believe we need to fix this use case; it would be good to have some evidence/support that we don’t have to fix it. “Happy accident” that this worked, ever – criminals know to not own/use such devices, anyway (?). This can be solved at another layer/another solution. Believe that any ‘fix’ would violate privacy, and therefore violate the PAR. We are not aware of any legal requirements that we solve this in the Standard.>

## Emergency services (pre- or post-association)

GAS and following association assumption of consistent MAC address, perhaps. Emergency alerts are done via AP advertisement, not dependent on knowledge of clients. “E911” scenario to require location, and MAC address(?), of caller.

The GAS/association problem is probably just a bad assumption, and not something we need to fix. E911 is TBD.

## Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??)

Non-AP STA: If this is a different ESS, you cannot Reassociate, so nothing is broken. (Same ESS is covered by 802.11aq requirement for stable MAC address.) PAR investigation …

Network side: Covered by use cases above.

## WBA liaison use cases…. Graham Smith doc: 11-21/1141

# Issues and analyses – discussion of 802.11 features/actions, per se

## Keep in mind, MAC address policy from the infrastructure

## Pre-association “steering”

What is currently done, within the Spec? (Explicitly supported by the Spec, or allowed by the Spec?)

# Proposed Solutions

## …

## …