IEEE P802.11
Wireless LANs

|  |
| --- |
| Issues Tracking |
| Date: 2021-05-04 |
| 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)

**Table of Contents**

[1 Introduction 3](#_Toc68691272)

[2 Terminology 3](#_Toc68691273)

[3 Brainstorming ideas/discussion 4](#_Toc68691274)

[4 Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used 4](#_Toc68691275)

[4.1 Pre-association client steering (AP steering, band steering, network steering) 4](#_Toc68691276)

[4.2 Post-association access control 4](#_Toc68691277)

[4.3 Post-association home automation (including arrival detection) 4](#_Toc68691278)

[4.4 Emergency services (pre- or post-association) 4](#_Toc68691279)

[4.5 Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??) 4](#_Toc68691280)

[5 Issues and analyses – discussion of 802.11 features/actions, per se 4](#_Toc68691281)

[5.1 … 4](#_Toc68691282)

[6 Proposed Solutions 5](#_Toc68691283)

[6.1 … 5](#_Toc68691284)

[6.2 … 5](#_Toc68691285)

# 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.

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 ~~Randomized~~ 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
* TGaz ranging, pre-association or post-association, TGaz’s security?
* TGbc features (pre-association/non-associated)
* Airport security queue is not a feature we need to make work

# 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

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??

## 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.

<Similar to hotel scenario?> Application function? Device-initiated Action frame (with crypto content) function?

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

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

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

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

## Pre-association “steering”

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

# Proposed Solutions

## …

## …