IEEE P802.11
Wireless LANs

|  |
| --- |
| Issues Tracking |
| Date: 2021-03-09 |
| 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.

**Table of Contents**

[1 Introduction 3](#_Toc65167137)

[2 Terminology 3](#_Toc65167138)

[3 Use cases 3](#_Toc65167139)

[3.1 Initial infrastructure connection steering 3](#_Toc65167140)

[3.2 Residential AP with “home” network, and public access network 4](#_Toc65167141)

[3.3 Airport security queue measurement 4](#_Toc65167142)

[3.4 Customer Support and Troubleshooting 4](#_Toc65167143)

[3.5 <Disruption of ongoing activities?> Mark H added this one (not in 11-19/1442) 4](#_Toc65167144)

[3.6 … 5](#_Toc65167145)

[4 Issues and analyses 5](#_Toc65167146)

[4.1 Rapidly changing MAC address, when not associated 5](#_Toc65167147)

[4.2 Periodically changing MAC address, associated 5](#_Toc65167148)

[4.3 … 5](#_Toc65167149)

[5 Proposed Solutions 5](#_Toc65167150)

[5.1 MAC address change timing 5](#_Toc65167151)

[5.2 Alternative identifiers 6](#_Toc65167152)

[5.3 Issue recommendations on SSID assignments 6](#_Toc65167153)

[5.4 Correlation of information elements 6](#_Toc65167154)

[5.5 … 6](#_Toc65167155)

# 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 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 4, 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 5 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.

Note – text in the remaining sections is just a placeholder for now, based on (an incomplete list of) discussion/topics in 11-19/1442r9, just as an example and a starting point for discussion. This list is not meant to be complete, nor necessarily are all items appropriate/correct.

# Use cases

## Initial infrastructure connection steering

An 802.11 enabled smartphone is configured to prefer 802.11 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 802.11 network, 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.

## Residential AP with “home” network, and public access network

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. It is preferred that the gateway prevent “home devices” from connecting to the public hotspot.

## 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 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.

**Use Cases:**

## 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.

The network/provider needs to be able to “track” devices across extended periods, to determine the cause of complaints of intermittent connectivity or performance issues.

## <Disruption of ongoing activities?> Mark H added this one (not in 11-19/1442)

<Is it accepted/expected that these devices will lose all active state if/when the address is changed while associated, and the device needs to re-attach to the network and re-establish any higher layer services?>

## …

# Issues and analyses

## Rapidly changing MAC address, when not associated

Rapidly changing MAC addresses can affect operation of 802.11 features that assume some correlation of a device’s behavior over time. These rapidly changing address can appear in Probe Request, Public Action, and Self-protected Action frames, etc.

Recommendations for, or mechanisms to control, the timing at which the client changes its MAC address while probing and other non-associated actions can manage the loss of correlation between device and MAC address. For example, the current proposed defaults from a major deployer of accessible, default MAC address randomization 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 some behaviors/operations).

Example use cases include:

* 3.1 Initial infrastructure connection steering
* 3.2 Residential AP with “home” network, and public access network
* 3.3 Airport security queue measurement

## Periodically changing MAC address, associated

As randomized MAC addresses are becoming more popular in consumer products, some such products are adding the capability to “re-randomize” the address even while associated, on a time basis, usually user selectable, often on the order of 24 hours for example. IEEE Std 802.11 currently calls for the MAC address to remain constant for the duration of any association (to an ESS), but it’s not clear if this is being followed by such devices.

Example use cases include:

* 3.4 Customer Support and Troubleshooting
* 3.5 <Disruption of ongoing activities?> Mark H added this one (not in 11-19/1442)

## …

# Proposed Solutions

## 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).

…

<Explicit text changes…>

## Alternative identifiers

Access control and arrival detection in a home environment, grocery store frequent shopper notifications and pervasive surveillance 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).

…

<Explicit text changes…>

## Issue 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.

…

<Explicit text changes…>

## Correlation of information elements

An alternative way of enabling the Infrastructure connection steering, pervasive surveillance 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.

…

<Explicit text changes…>

## …