Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, 10 August 2021Randomized and Changing MAC addresses (RCM) |
| Date: 2021-08-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11 bh telecom Interim meeting 28 June 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting August 10, 2021 9.00 to 11.00 am ET**

**Chair: Mark Hamilton**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 9.03 hrs. EDT,**

Agenda slide deck 11-21/1295r3

**Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
* Attendance, noises/recording, meeting protocol reminders
* Policies, duty to inform, participation rules
* Organization topics (see also Backup slides):
	+ PAR/CSD: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html); [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
	+ Timeline estimate
* Issues Tracking/Contributions
* Next meetings: Aug 19 19:00 ET, Aug 31 9:00 ET

The Chair reviewed the agenda.

Chair expressed opinion that Issues Tracking Document is now largely done and will go through the latest revision at this meeting.

Chair displayed the Timescales slide 20

Any comments? None.

The proposed agenda was adopted without objection.

Attendance is listed at end of the Minutes.

1. **TGbh Issues Tracking document: 11-21/0332r13**

Chair presented latest version of the Tracking Document 12/0332r13.

Presented updates to Use cases. TG Needs to decide which Use Cases we need to track.

4.1. Pre-association client steering (AP steering, band steering, network steering)

*“previously visited network might imply re-use of same MAC address, or there might be a feature to change MAC address anyway”*

C –Certain devices re-use same MAC address when re-joining an SSID.

C – If same MAC address then that solves problem.

C – If using same MAC within same ESS then that solves most of these issues. Does probe with the random MAC however.

C – Heard that some devices will use random MAC until finding wanted network. Then does one more directed probe and switches to the saved MAC for that network.

C – That hinders privacy – but if intended to join, MAC is displayed anyway.

C – Before RCM we had a product that passively scanned all the time, but once selected network, if we did not send an active scan before association could not associate.

Q – Steering is all after association, so what is pre-association? There is no spec for pre-association so what can we change?

A – Need to check BTM query and maybe ANQP etc. – don’t think there is a public action frame here.

C – Most pre-association steering just simply do not let STA associate if not wanted. Also do not send probe response.

C – Mechanism is hit and miss. Never defined before is period of time after STA selects and connects, the join part, a period where the STA established state with network similar to roaming, but could define that state in more detail. Device is not associated, but has selected the network.

A – May be outside of our spec. Note that agile multiband Wi-Fi Alliance and WBA talk about network selection procedures.

C – This state could give recommendations on behavior.

C – Mechanism of not replying to the probes can be used but appears to violate the spec.

C – Are we talking about AP pre-association transmissions to the STA?

C – Client may have several networks configured. Problem is that on infrastructure side no way to know intent of the STA when receiving probes. Better to let the STA associate then steer it.

Chair – Steering when client is just probing is not in spec and hence would be outside our scope.

Our scope is to address a feature that is already in spec and may now be broken.

*“device might have an SLA “agreement” with a previously visited network”*

C – Covered if post association.

C – SLA has nothing to do with steering, more analytics.

C – Need to get device to associate with correct network, private vs public for home routers, or hotel where some clients pay for better service, for example. Other organizations may be looking at this.

*“Device is probing specific SSID, or Broadcast SSID”*

C- Think thas is covered.

Chair – Any objection if we write this up as ‘outside our scope’?

Q - is this because pre-association steering is not addressed in the spec?

A - Yes

No Objection

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

Chair proposed the following conclusion
“This scenario can be handled with an “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established). Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh”

C – Can we elaborate more on “opt-in”?

A – “Opt-in” concept is something that requires explicit user action or agreement. Client has to indicate it wants to do this and human user involved.

Generally Accepted.

## 4.3. Post-association home automation (including arrival detection)

Chair proposed following conclusion, similar to 4.2:

“This scenario can be handled with an “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established). Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh.”

Generally Accepted.

## 4.4 Airport Security Queue

Chair proposed following conclusion:

“Upon analysis of this scenario, it has been agreed that such tracking of individuals without their consent is considered a violation of their privacy – exactly what MAC randomization is trying to prevent. Since the fundamental purpose of this tracking can be accomplished in other ways without 802.11 involvement, this scenario is considered out of scope for 802.11bh to provide a solution.”

Generally Accepted.

4.5. Grocery store customer flow analysis

Similar to 4.4.

“Upon analysis of this scenario, it has been agreed that such tracking of individuals without their consent is considered a violation of their privacy – exactly what MAC randomization is trying to prevent. Since the fundamental purpose of this tracking can be accomplished in other ways without 802.11 involvement, this scenario is considered out of scope for 802.11bh to provide a solution”

Generally Accepted.

## 4.6 Grocery store frequent shopper notifications

Similar to 4.5 but here the user wants to opt-in

Chair proposed following conclusion:

“If this scenario is limited to opt-in uses, and it can be assumed that the device will have been configured to associate to the grocery store infrastructure when in range, then the scenario can be handled with an “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established).

Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh.”

C- Can have apps that ask STA for information. Hence not clear what opt-in means here? What are you opting-in?

C – User has agreed that they want to be tracked when in store.

Q – Is this pre or post-association? If client has to associate, then no real problem if we assume same MAC.

A – Case when device does associate. If pre-association, then can’t address it. Trend is to use different MAC addresses with time for example.

C – If spec allows MAC to periodically change then this brings the Use Cases back into scope.

C – If the STA has a state established with that network then it keeps same MAC address. If not, then it may change.

C – Carefully worded the 11aq clause, were thinking more of security, PMKSA.

C – 11aq description is pretty general?

A – Yes, written in general way to avoid describing every specific state. At the time battling with RAC comments and not breaking rules in IEEE 802. Note that we cannot address IP addresses. We could provide recommendations on the requirements we have written.

C – If it makes sense to create a layer 2 feature that allows a layer 3 facility is something we could do.

C – Could make clarity in 11aq statement. But when do we bang up against 11bi.

A – For 11bh, it has to be something that used to work, stopped working because of RCM, and we think we have a solution that does not hinder user privacy.

C – Hence if “opt-in”, user has given up some of his privacy.

C – Yes, when device is connected. What about when multiple networks available?

A - Hence added words about intention to association, but does get murky.

C – Need to add “and associated”.

Generally accepted.

4.7. Infrastructure (home or enterprise) with different SSIDs per band

Chair proposed following conclusion:

“This scenario is considered out of scope for an 802.11bh solution. Deploying an intended single ESS with more than one SSID is beyond the scope or correct operation for 802.11. If a given single “network” (802 access domain) is deployed with multiple ESSs providing access, the device would not be able to maintain any shared state across the ESSs, unless it uses a consistent MAC address (see: 802.11aq). While a solution to indicate to the client that these ESSs are in fact a single network might be possible, it appears to be solving a problem caused by incorrect deployment, not by MAC address randomization.”

Generally accepted.

This was the end of the Chair’s editing of the document.

Discussion on possible re-visiting and spec support of multi band networks.

1. **Presentation**

[11-21/1247r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1247-00-00bh-mac-features-impacted-by-rcm.pptx) (**MAC features impacted discussion**)

Presented by Chaoming Luo, OPPO.

This contribution recaps some features in IEEE Std 802.11 that identify a STA by its MAC address, and draws the group’s attention to solve the related issue when using random MAC address.

Proposal: We should consider a mechanism (e.g., signature method mentioned in 21/1083r0) to assist the AP to identify the non-AP STA when the STA uses a randomized MAC address or changes its MAC address.

C – After association 11aq wants you to go back to previous MAC. So what is new here?

A – There may be cases where MAC may change. Not sure if group wants to keep this or allow MA to change.

C – Are ARP services within our scope of 802.11? Proxy ARP are. How do we solve within ARP service if MAC address changes?

A – Yes will be problem.

C –Is Straw Poll is a general question in looking for a mechanism to ID STAs other than MAC address, or looking at specific solution as proposed in 1083?

A – Yes, General question

C – On Straw Poll need to add “while not exposing any new privacy concern”.

Q – Talk about STA changing MAC, is this also when associated? 11aq says cannot change MAC while associated.

Added “whether the non-AP STA is associated or unassociated”

Straw Poll

“Do you agree that TGbh should consider a mechanism to assist the AP to identify the non-AP STA when the STA uses a randomized MAC address or changes its MAC address while not exposing any new privacy concern.

Whether the non-AP STA is associated or unassociated TBD.”

C – If TBD, what is purpose of this SP?

A – Not sure if group would consider case of changing MAC address after association.

**Out of time**

**Next calls Aug 19 19:00 ET, Aug 31 9:00 ET**

**Meeting Adjoined at 11.01 ET.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 8/10 | Ansley, Carol | Cox Communications Inc. |
| TGbh | 8/10 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 8/10 | Henry, Jerome | Cisco Systems, Inc. |
| TGbh | 8/10 | Huang, Po-Kai | Intel Corporation |
| TGbh | 8/10 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 8/10 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 8/10 | Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| TGbh | 8/10 | Montemurro, Michael | Huawei Technologies Co., Ltd |
| TGbh | 8/10 | Ng, Boon Loong | Samsung Research America |
| TGbh | 8/10 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 8/10 | Petrick, Albert | InterDigital |
| TGbh | 8/10 | Shalom, Hai | Google |
| TGbh | 8/10 | Smith, Graham | SRT Wireless |
| TGbh | 8/10 | Yee, Peter | NSA-CSD |