Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, November 4, 2021Randomized and Changing MAC addresses (RCM) |
| Date: 2021-12-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter YEE | NSA-CSD | Mountain View, California |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecom Interim meeting December 16, 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Dec 16, 2021 7.00 to 9.00 pm ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**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 7.03 hrs. EDT,**

Agenda slide deck [11-21/1996r01](https://mentor.ieee.org/802.11/dcn/21/11-21-1996-01-00bh-agenda-tgbh-2021-december-16.pptx)

1. **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 Backup slides)
* Issues Tracking updates/status: [11-21/0332r26](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-26-00bh-issues-tracking.docx)
* Evaluation of proposed solutions
* Next meetings: Jan 5, Jan 11

Nothing submitted on the WBA Liaison response

No objections, Agenda accepted.

Any comments on the latest Issue Document revision? – None

Q- Have any of the proposals been updated?

ACTION Mark Hamilton: Reach out to all authors of proposals to see where things stand

A- Liuming Lu (OPPO) said he was preparing a new version of his proposal for the next meeting

**11-21/0332r26: Issues Tracking document**

Q- Can we change “post-association” to indicate after security complete?

Q- Does that also include the case of PMK caching?

A- We haven’t gotten into that level of detail in the document.

C- There might be holes associated with cached PMKs.

Q-Then what about after association and when security is complete?

A- That would work.

Q- This is RSNA?

A- That sounds right.

Looking at table 1 in Section 5, which covers use cases and group agreement on whether they are in scope. Then at Table 2, which indicates if each of the three proposals supports that use case.

4.13 was agreed to be describing a mobile AP.

C- The general agreement was to just offer recommendations, but would consider solutions if one is presented.

Q- Comments? New attribute ideas? Anything to capture?

Q- Does this also cover when a device that is also a mobile AP changes its MAC address or are we talking about the STAs using the mobile AP?

A- This should be about the mobile AP itself, not the STAs using the mobile AP. And automotive APs are pretty much the same thing in different packaging. APs don’t generally change MAC addresses because they are wired into a fixed network, but that’s not true of a mobile AP. Any AP, as long as it has clients attached to it can’t change its address. That was the direction we were heading.

Q- Can you mark the definition of the use case in the text as you just stated?

A- Yes. (Immediately added text about lack of terminology in IEEE 802.11).

4.14 How to onboard a “known” MAC address. This can be solved with IEEE 802.1X security or SAE passwords, or other identity mechanism. We can recommend that that should be the case.

Q- Did anyone discuss Wi-Fi Easy Connect?

A- That did come up.

C- Wi-Fi Easy Connect solves that problem, both in enterprise and home environments, via multiple methods. So can IETF BRSKI from the ANIMA working group.

A- That can be added to the use case table.

Q- If you allow Easy Connect, then you can allow many other methods. The sky’s the limit once you use out-of-band methods.

A- Let’s make it support other out-of-band methods.

4.15 Customer support and troubleshooting

C- This is for residential support via a remote service provider. Pre-association troubleshooting is still a problem, even if we expanded to an enterprise level.

C- If you look at both residential and enterprise use cases, the enterprise is easier to solve. Enterprise environments tend to have some sort of app or mechanism to uniquely identify the user in question, which allows them to achieve any sort of troubleshooting they need to. That’s not true of the residential case where there’s no asset tracking. If the user could temporarily turn of randomizing MAC, that might be a workaround. There would need to be user consent involved.

Q- Yes, we would need to have a user opt in to the process. There’s a different solution for turning off a random MAC, but what if there’s a world in which RCM is the default and becomes more aggressively so, where it can no longer be easily be turned off by a normal residential user?

C- The other mechanism is that the service provider could request that an app on the device be used to assist in mapping the MAC to a device identifier.

C- The enterprise doesn’t have good device tracking pre-association.

Q- We are putting in the idea that there is customer support at the MAC layer, but isn’t it true that the upper layers are using some interface to allow the MAC change. It’s not like there’s a universal method to reach into the MAC even when it would be something done through the management SAP. Doesn’t it seem like that’s outside of 802.11’s control? Maybe we only define an interface to make it possible.

A- Most implementations have a hardware-programmed MAC address that they are hiding to do RCM. Essentially, we are allowing the user to hide that MAC address. If there’s an upper layer application that could map to the hardware-programmed MAC address without compromising the randomization process. The details of that need to be worked out, but the thought isn’t fully bake in my head.

C- I don’t think we want to go into this level of detail, but I’m wondering with respect to the question if there’s information we can provide from the SME to an application that’s doing customer troubleshooting. I’m not sure what that information is or if we have to control the random MAC, but it would be worth looking into.

C- It sounds like there are somethings worth looking at, even if not providing a full-on solution. Maybe a technique to manage this particular scenario.

C- It could be more MIB entries.

C- Or counters.

C- We could see what the intent was.

4.16 Residential gateway with public hotspot (and private network access for homeowner).

C- Previously determined to be out of scope.

4.17 Lawful surveillance.

C- Allowing Law Enforcement to track people or glean information. As far as we know, law enforcement can use whatever the technology supports, but we aren’t attempting to allow greater access than the technology supports, including any loss of tracking functionality from RCM.

4.18 Emergency service.

C- Identification of an emergency services caller via MAC address. Out of scope and a different solution is needed.

4.19 Public Wi-Fi hotspot roaming (between multiple APs that are not directly connected to the same backend network).

C- This is either covered by an existing use case if the backend is common, otherwise it is out of scope – it’s like jumping between different networks.

4.20 MAC address collisions (WBA use case). Seems to be out of scope, but we could add recommendations on ways to help avoid the problem. (Shout out to Graham Smith for winnowing the WBA’s list of use cases.) This doesn’t seem like our problem to fix.

4.21 Account and billing issues (WBA use case). Seems to be the same as use case 4.2, which is in scope, even if MAC addresses don’t make highly reliable billing identifiers.

Q- Aren’t there similarities between 4.21 and 4.15 as well?

A- Maybe, but not as clearly as between 4.21 and 4.2.

C- Both are trying to support a customer, one for troubleshooting, the other for billing. Both require knowing the customer.

C- If you don’t pay, you don’t get (customer) service and support.

A- If so, that could point back to 4.15, but I think the WBA was talking about basic access and service, not support. Do we agree that if we cover the other use cases we are good?

A- I think this use case is out of scope and not related to 4.2 and 4.15. We should discourage billing based on a spoofable identifier.

C- I should clarify about the mapping between an upper-layer identifier and a low-layer identifier. The mechanism used to convey the identifier would be out of scope for us to solve. The communication of the identifier should be out of band.

C- I agree with previous speakers, however there are systems in use today that use the MAC address for billing. The scope of the TG is to solve things RCM broke. Yes, it’s a misuse of the MAC address, but it’s how things are done.

C- Yes, it breaks that, but it was something that was sort of broken before randomized MAC addresses happened. Randomization just exposed the breakage more. I don’t think we need to fix this. It was twice broke.

C- This is about money. There’s way more that needs to be done to bring this into scope. Is it possible we can even convince them to use our (more secure) mechanism (whatever that will be) for billing?

C- We should educate them not to do billing this way.

Q- Could we revisit our decision about 4.2?

C- 4.2 is in scope, though all of the criteria need to be considered. I think captive portal drove this discussion.

Q- The reason I’m asking is that I wasn’t present for that call, but if 4.15 and 4.21 are out of scope, then what happens to 4.2?

A- We said parts of 4.15 are in scope.

C- Some of the discussion in 4.21 also applies to 4.15. Things can be done out of band.

A- Maybe we need to revisit 4.15, although I don’t necessarily agree with where you are going.

C- You still don’t do anything outside of the device. You just potentially provide additional info from the MAC that can be used outside of the device for customer support and troubleshooting. If it goes off device, I’m not advocating it.

Q- What is done with the identifier then? Out of band, it could be sent off device.

A- I don’t know about 4.21. There are probably ways in 802.11 to solve it. In 4.15, such an interface might have uses.

C- An AAA server can already do 4.21 without a MAC address, so we don’t need to do anything.

A- Yes, if you’re using that sort of mechanism.

C- If you aren’t using AAA, then you’re screwed. And the global MAC could be spoofed too.

Q- I’m trying to understand that on-device/off-device aspect of troubleshooting. Lots backend systems look at MAC addresses for many purposes. Please clarify 4.15.

A- I don’t know what would be exposed through such an interface, but it would be worth looking into an interface that can be exposed to upper layers in the device that can assist in troubleshooting and support. I don’t have details, but it’s worth looking into.

Q- That’s outside of current troubleshooting flows, something new added to the upper layer to help with troubleshooting?

A- Right. It doesn’t go outside of the device.

Q- What does not going off the device mean?

A- That’s from the MAC point of view. An application could communicate an identifier off the device. It’s just not a MAC-to-MAC communication of an identifier. And I won’t sign up to do primitive work if that’s what’s involved.

Q- Does that mean 4.21 does not have anything new beyond 4.2 and 4.15?

A- I would say we punt that one. It implies that the MAC address is some sort of an identity. I don’t think there’s any useful work we can do with that. We have done lots of useful work in the last 20 years that allows solutions that require MAC addresses as identities.

Q- So, this use case is out of scope?

A- We might have a terminology problem. When we are saying something is out of scope, that means that it is beyond the scope of 802.11 or 11bh or 11bi to deal with. It doesn’t mean we don’t think this is a problem that should be solved. It’s just not for us to solve.

C- If it’s out of scope for 802.11, it’s out of scope for 11bh and 11bi. It doesn’t matter how far out of scope it is.

C- We can point to how mutual authentication is done on wireless networks and that such mechanisms could be used for identification.

C- Then we can say the use case is in scope if such mechanisms are in use and that the security mechanism identifier is the solution.

C- But then a PMKID can change and wouldn’t be a useful long-term identifier.

C- We consider 802.1X behavior within our network scope. So, if it is used, then the 802.1X identifier would be one solution. Use that and not a MAC address for billing.

Q- Does such a statement belong in 802.11?

A- I think it would be permissible. We would have to determine if we actually wanted to do so.

C- I am concerned that there would be a statement in 802.11 that deals with accounting and billing.

C- There may be other good reasons for not saying it, but that has nothing to do with scope.

C- There are mentions of AAA servers in the specification. AAA servers are used for accounting and billing. There’s an RFC that uses MAC addresses this way. It shouldn’t be handled by 11bh. Maybe it should be done in 11bi, but not here.

Q- So, we can call this use case out of scope?

A- [Crickets.]

C- I have no problem with replying to them that they should not use MAC addresses this way if that’s what we think.

C- We could say that the MAC address was never an appropriate or reliable identifier.

4..22 Qos and QoE (WBA use case)

Q- Aren’t these service-based and done at a higher layer? Done per connection, not per MAC address?

A- Could be. It’s not clear if it’s per network.

Q- So they are identifying devices from MAC addresses – my game console vs. some other MAC address using the network? And applying a uniform level of service for any connection from that device?

A- It could be based on the owner of the device.

C- If it’s per user and service, doesn’t that go back to accounting and billing. In which case, it’s out of scope because they are using the MAC address it wasn’t meant to be used for. Don’t identify devices types based on the MAC address and then set a service level.

C- That’s not a service if you haven’t gone through a captive portal to get that level of service. How that service identifies me is up to the service, it should not be via the MAC address.

A- Is that a level of service? In the extreme, “no service” vs. “yes service” is some sort of level of service. But if you’ve gone through the captive portal, you get some higher level of service for that.

C- Home users set up QoS to prioritize their devices.

A- There are solutions if you want to prioritize a particular device. Wi-Fi Easy Connect can provide this.

C- We could point to that list of other ways to identify devices, à la 4.14.

C- We could put some of this in an annex somewhere that describes this.

C- That would help the WBA not to make bad decisions to use MAC addresses once they better understand the alternatives.

Q- Are we okay copying 4.14’s answer into to 4.22?

A- (seems fine)

4.23 DHCP Pool Exhaustion (WBA use case)

Q- Shorter DHCP lease times could help here, right? And a device can request a particular DHCP address instead of getting a new address from the lease pool. And some DHCP servers will ping the previous device that held an IP address to see if it’s still on the network prior to re-assigning it.

A- We seemed to be previously not wanting to suggest short leases, although the DHCP client identifier might help. We were going to capture that in a recommendation.

Q- I think this is not a question of scope for this use case. We can choose to make a recommendation or not. If we choose to do so, would it be in the 802.11 spec or in some form of response to the WBA?

A- I will try to get into a response to the WBA for anything we capture from this discussion. All of these are going to get a response. The question is if we put something in 802.11 to head off these questions coming to us again in the future.

Q- There was mention of an IPv6 issue previously. What was that?

A- There’s a way of generating your IPv6 address from your MAC address, which means your IPv6 address changes with your MAC address.

Q- You don’t have to do that, right?

A- Correct.

C- Seems like we just make recommendations.

4.24 Inconsistent DHCP address assignment (WBA use case)

C- This is a related to the previous use case. If there’s supposed to be a static allocation in the DHCP server for a device, an RCM causes problem with that. A short lease doesn’t solve this problem.

C- If I am a device communicating with an RCM node, doesn’t the ARP cache need to be updated?

A- That’s what I’m thinking. But if you haven’t seen the MAC address change, you might send a frame to the wrong device because your ARP cache is stale.

C- That’s the same thing as going away and coming back with a different MAC address. You aren’t supposed to change your MAC address while associated. And probably not your IP address.

C- But some devices want to change their MAC addresses periodically. That will require them to re-associate. That’s how it should be.

C- When you come back, you’ll have to re-instantiate your ARP cache. And devices you ARP will ARP you back and figure out who you are.

C- That works for you, but other devices that don’t know about your change of MAC address will not be able to communicate with you.

C- Spanning trees in large networks have similar problems.

C- This is just a problem that takes some time before the network sorts it out.

C- Which is why if you want a continuous service, you don’t go around changing your MAC address a lot.

C- Changing the MAC address leads to a new IP address in most cases today. If that’s not what’s desired, don’t use RCM (excessively).

C- The only issue for DHCP seems to be pool exhaustion.

C- Inconsistent DHCP address assignment seems to be out of scope. We might use the same recommendations as 4.23.

4.25 ACLs/firewalls (WBA use case).

C- This seems to be the same as 4.2. If you use IP-based ACLs, then it is out of scope for us.

C- The reason we went through this list (Table 1) was to narrow down what we discuss in Table 2 (analysis against features/attributes/criteria). My recommendation is to have the authors of solutions that are being proposed to comment on how the proposals work (or not) with the attributes/criteria.

C- This mapping will be part of the email that will be sent to the authors to see where their proposals are. We will pick that up after the break.

Q- We didn’t discuss 11-21/1634r00 (Private Identifier Requirements). Where should we go with that?

A- We could do it during the next meeting, although it’s rather incomplete.

Q- How does it compare with what is in section 6?

A- Let’s discuss that offline.

C- That’s the only contribution we haven’t gotten to at all. The other contributions are updates or extra information on the existing proposals. That seems like plenty to do in the interim.

**Next meeting: 6 January 2022, followed by 11 January 2022.**

**Adjourned at 9:00 p.m. EST.**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout |  | Name | Affiliation |
| TGbh | 12/16 | Ansley, Carol | Cox |
| TGbh | 12/16 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 12/16 | Huang, Po-Kai | Intel Corporation |
| TGbh | 12/16 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 12/16 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 12/16 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 12/16 | Montemurro, Mike | Huawei |
| TGbh | 12/16 | Petrick, Albert | InterDigital |
| TGbh | 12/16 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGbh | 12/16 | Sevin, Julien | Canon Research Centre France |
| TGbh | 12/16 | Shalom, Hai | Google |
| TGbh | 12/16 | Sun, Bo | ZTE |
| TGbh | 12/16 | Thakur, Sid | Apple |
| TGbh | 12/16 | Torab, Payam | Meta |
| TGbh | 12/16 | Yang, Jay | Nokia |
| TGbh | 12/16 | Yee, Peter | NSA-CSD |