Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, September 27, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-9-27 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of September 27, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting September 27, 2022 9:30 a.m. to 11:30 a.m. ET**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 9:33 a.m. EDT.**

Agenda slide deck [11-22/1660r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1660-00-00bh-agenda-tgbh-2022-sep-27.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)**
	+ September to November teleconferences: Tuesdays, 9:30-11:30 am ET (this time slot)
	+ Timeline reminder (slide 20)
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r11**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-11-00bh-cc41-comments-against-d0-2.xlsx)
	+ Continue discussion on resolutions of ones that are not on topics:
		- Opt-in, Pre/un-assoc, Non-AP STA-generated ID
	+ [11-22/1218r5](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) – Device ID synchronization and control (Kurt Lumbatis)
	+ [11-22/1329r6](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-06-00bh-cid-resolutoins-for-12-2-11.docx) – CID resolutions for 12.2.11 (Kurt Lumbatis)
	+ [11-22/1599r1](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-01-00bh-revisions-to-rsn-extension-element.docx) – Revisions to RSN Extension element (Kurt Lumbatis)
	+ [11-22/1620r2](https://mentor.ieee.org/802.11/dcn/22/11-22-1620-02-00bh-device-id-ladder-diagram.pptx) – Device ID ladder diagram (Kurt Lumbatis)
* **Walk-through CIDs status**
	+ **~1 hour**
* **Contributions (slide 16)**
	+ **~1 hour**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Revisions to RSN Extensions Element**

Kurt Lumbatis (ARRIS/CommScope) presented [11-22/1599r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-02-00bh-revisions-to-rsn-extension-element.docx). It would change the bit name “Device ID Support” to “Device ID Active” and update the definition of the bit. Corresponding text is also added to Annex C.3.

C- The Annex text doesn’t need to get into that level of detail. That should be left to Section 9.

C- I’m fine with removing that. I based my entry off a previous MIB entry.

C- We haven’t looked at the MIB descriptions all that much.

C- I can make that change.

Q- Is this MIB variable within the BSS block? I think we agreed in the meeting to have an activation in each of the BSSes.

A- I set it in the dot11StationConfigEntry.

C- I think we need to make it per BSS as we discussed during the interim meeting.

Q- Does the non-AP STA make updates via the SME to say which BSS it should be sent to?

A- Yes.

C- Then it seems like it’s fine here.

C- What I had in mind in having it in the BSS block with the default value of True. And then after joining, it can be removed or not used.

C- If we want to put it in the BSS entry, I can move it there, if that’s our decision.

C- I’m not sure we have a per-BSS entry.

C- I looked but couldn’t find one.

C- Let’s consider this a start and then determine that later.

C- I think this location is fine. The default value should be here, but it should be false not true.

C- I don’t have a default value set.

C- I have some doubts regarding that. If you set that default to false, then to any AP you know, you won’t hide your privacy.

C- This is confusing. This variable says whether you are sending the value. So, I believe it should default to false on a non-AP STA. And I’m not aware of default values that are different between non-AP STA and AP in other variables. You would need two variables for that. I’ve submitted text in the chat for how to set the default value to false. [DEFVAL { false }]

An updated version of the text will be posted and then readied for a motion.

1. **Device ID Synchronization and Control [Updated]**

Lumbatis then presented [11-22/1218r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx). He described updates to the truth tables in the presentation.

C- [In reference to Slide 8] I thought we weren’t going to do the empty ID field. We would just use the bit to indicate active or not.

Q- How is the AP going to know?

A- If the STA sets the capability bit, then the AP will send an ID. If not set, it won’t. That’s what we discussed at the last meeting. If the STA doesn’t have an identity, you can’t send one.

C- [In reference to Slide 10] I think you need another column for Device ID Active, one for non-AP STA and one for AP.

C- I was doing that through separate tables.

C- If that’s clear to everybody, I’m fine with it. I’ll withdraw the comment.

Q- I was going to say that this is extremely confusing. Are these slides for discussion or to get something into the draft?

A- This is for resolving CIDs, which will result in new text.

C- Then I agree that a new column is needed along with a way to indicate something is a reaction to what was received from the non-AP STA.

C- That can be done.

C- That might help to reduce confusion.

C- Changing the slide name also helps without requiring another column.

C- There are only four conditions. The STA and the AP indicate support or not plus the combinations thereof. I can’t see why we have so many slides.

C- Slide 11 [with modifications] might make that clearer. It lays out the cases for what the AP does when STA supplies an ID.

C- Is this a new ID being sent or the old one repeated?

C- The AP can choose to send a new ID if it recognizes the old one that the STA sent.

Q- Does the fourth box say that the AP can assign a new ID at any time?

A- Yes.

C- Then the second box should say that if the identity is recognized, then the AP will use it.

C- I don’t think the AP will ever send the same ID back in the “not recognized case”. That element is present only if a new one is being assigned.

C- We had a request for a handshake so that the non-AP STA knew that the value was accepted.

C- In that case, then it should be signaled in both the recognized and not recognized cases.

Q- Why is the ID sent back in the not recognized case?

A- That was requested during a previous meeting.

C- I think the STA has no way of differentiating between recognized vs. not recognized in that case.

C- If we want explicit identification that the AP recognizes the ID and is willing to use it, then we probably need a new bit in the element to signal that. And separately, the AP can signal “here’s a new identity”. If all of that’s wanted. I’m not sure it’s needed.

C- I don’t think the AP needs to insert an ID in message 3 unless it is assigning a new ID.

Q- Does anyone think the ID needs to be sent back to indicate the AP is still using it?

A- [Crickets.] Then we probably don’t need that.

C- I don’t think we need such an indication. I don’t know what the STA would do with it.

C- So we need to talk about what the AP is going to indicate and plan for that discussion. The AP is going to complete this negotiation and end up with an idea of the relationship. What does it communicate out, to the SME, the upper layer, the application?

C- Row 3 is out of scope. If the AP doesn’t recognize the identity, why would it allow it to be use?

Q- In the second row, what does utilize the identity mean? And the third row, the AP doesn’t deliver notification of the non-recognition to the STA.

A- The third row is to allow use of stale IDs, like if the AP has aged out an entry in its database. It can then decide to allow the ID to be used to identify the device or it can assign a new identifier.

C- The STA doesn’t know whether the AP recognized the ID in that scheme. There should be some information sent to the STA.

C- A new STA sends no identity to say it is new.

C- That’s a different case. Sending an unrecognized ID to an AP is not the same case.

C- That AP may allow this unrecognized ID to be utilized can’t be understood by the STA as being any different from the AP recognizing the ID. We would need a bit to signal that.

C- We don’t have one defined.

C- If the group agrees to, we can create a new bit to signal that.

Q- We had a term for a network-generated ID or is that a different thing?

A- I believe they are supposed to be the same.

C- If we say the term “identity”, we should be clear if it is network-generated. I don’t think it should be.

C- We only have network-generated IDs in the draft. We don’t have an agreement for other kinds.

C- We don’t have agreement on how the network generates the ID and what network means here. We have a BSS in IEEE 802.11, but no definition of network.

C- Aren’t we just trying to say how the ID is propagated, not how it is generated.

C- Let’s not go down the “network” rathole at this time. Let’s just try to get this table straight. Let’s assume the ID was somehow on the AP/infrastructure/network side. We can return to the term later when we generate text.

Q- To clarify the NACK bit to indicate that the AP didn’t recognize the ID. What does the STA do when it gets it?

A- That’s the confusing part – I’m not sure.

C- It sounds like an error to me.

C- The STA decides to provide its ID or not, signaling it wants to be identified. The AP may have lost that information and then send the NACK bit. Then the STA will know that it needs to act as a new STA and establish a new ID.

C- I’m not clear of the steps be taken in that state.

Q- The ID is used to say, “I’ve been here before”. It’s not for iterating until the AP says, “Yes, that’s a valid one.”

A- I think if the ID is not recognized, the network generates a new one and sends it back.

Q- Then why signal that it wasn’t recognized? It opens holes. Just send one back. Maybe always send one and the STA always uses that next time.

C- I can’t tell the difference between “I didn’t recognize you” and “I want you to use this new ID [for whatever reason]”. The STA can’t tell why it got a new identity.

C- Some of the comments in the chat indicate we need a flow table, not a chart here to clear up things. Then we invent things to solve the cases.

Q- We are forgetting the purpose of the ID. If you come in with a false ID and the AP gives you a new one, that’s a bit strange. You recognize an ID by things that happened before. There are privileges associated with the ID. If you come in with a false ID, what privileges are assigned along with the new ID? Or am I overthinking this? I’m finding this confusing.

A- I’m getting a bit concerned that handling this all in the 4-way handshake or the association process will not give enough time to get things done. What’s the timeout of a message 3, for example?

C- Let’s save that for when we understand the problem. And now we are getting back into the use cases in the tracking document and the type of state information that might be preserved about each STA that has previously visited an AP. We have a whole bunch of use cases for what that information might be and why. We need to think of the use cases.

C- We have discussed this issue many times before. But we don’t have to consider all use cases. And generally, there’s usually an acknowledgement of an identifier elsewhere in IEEE 802.11. For simplicity, we could just keep doing that without overthinking things.

C- That’s why I was returning the same identifier if it was recognized. However, I was asked to take that out. Let’s take this offline. And I’ll try to create a flow diagram.

C- That might help. Think about how those use cases apply to the diagram.

1. **CR for STA generated ID**

Jay Yang briefed the updated [11-22/1079r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1079-04-00bh-cr-for-sta-generated-id.docx). It covers comment IDs (CIDs) 7, 9, 19,20, 36, 40, 41, 42, 61, 64, and 65. There are two solutions for pre-association use cases, MAAD and RRCM. RRCM can be used alone or with MAAD.

C- Based on the previous discussion, I’m getting concerned with our security requirements. If we are using this for access control, the ID shouldn’t be easily observed and copied at will. There was some discussion of one-time use only, but I don’t see any text on that. I sympathize with getting something in and fixing it later, but I can’t support something that is used for access control. Attackers shouldn’t be able to get in by copying something easily. I’m not convinced a MAC-address based mechanism can be done safely.

Q- What happens when a device is not recognized?

A- I have no idea. My concern is a device being identified and allowed in with just a MAC address identifier.

C- This seems like it is making these mechanisms mandatory. This is a worrying direction. We have standards for the privacy of the device. This is not meeting those standards. But I don’t think we need access control here.

C- The current schemes are based on the MAC address. To keep that, out solution has to work in the Authentication frame. That’s the aim of this solution.

C- We shouldn’t invent new authentication mechanisms, especially if they might have security holes.

C- We can define rules to avoid copying problems. We can do that in a later revision. It’s not a big issue. We could make it a one-time identifier. I don’t think it’s a problem.

C- I’m seeing problems with this approach.

Q- We tried to work up to this via the issues tracking document to look at the problems caused and whether they needed to be solved. We need to go back to those specific points and specific use cases and specific security issues. Otherwise we will go in circles. I’m wondering if this STA-generated side is raising concerns about security because: 1) the ID is publicly available to third parties that might spoof it; and 2) whether the network could trust a STA-generated ID for access control. Would it make sense to say that when a STA-generated ID is use, the network makes its own decisions on whether to trust it and how much.

A- I think this topic was already discussed in previous teleconferences. Let’s not do that again. If we can do a STA-generated variant, we can avoid the issue.

C- That didn’t answer my question.

Q- If we can address the issue of identifier reuse, is that enough?

A- I have other concerns. And I would not like to accept a STA-generated proposal until everything is resolved.

C- We will look at how to address the concerns raised.

C- It would be good to also allow a true AP to be recognized instead of a false AP.

C- Even in the baseline, there’s this problem. This is a different requirement you are making.

C- I’m not sure if the Device ID is capable of solving that problem. But I think if we are doing access control, we should find a way to fix that. Otherwise, we may have a solution that’s good for device tracking by the network but not access control. This is a general issue for IEEE 802.11bh.

C- Yes, it’s not a problem specific to the STA-generated ID.

Q- To people who don’t support MAC-based identification, the current draft doesn’t talk about managing random MAC addresses at all. If we accept that draft, then aren’t we leaving it to the vendors to come up with their own solutions? Those addresses will be implementation not based on standards, right?

A- I think we have some proposals that use the MAC address as the signaling mechanism when the non-AP STA returns. The question is whether we are adding back in something to the draft that is causing you concern.

Q- The MAAD or IRMA or the RRCM all use the MAC address. Someone could listen to the frame and copy the address. How does the current draft solve that problem? The STA that uses the Device ID might do random addressing poorly. How are addresses managed?

A- It doesn’t talk about random addresses because they are out of scope. But at a high level, there are proposals that want to use the MAC address as an identity and use it for access control. Those are broken ideas and we should not bring them back. I don’t mind using the MAC address for identity where it doesn’t really matter. But I don’t want the network to perform actions based on a MAC address that is easily cloned. It really depends on the security needs of your use cases. We don’t have a clear statement about that. The MAC-address based thing could have an IE that has a nonce to prove a live operation or other things that make cloning more difficult. That might be enough to cover my main worries. I’m worried that these proposals will be used to enable things that were done in the past.

C- Opposition to MAC-based identification is philosophical for me. We have been trying to get away from that for a long time, so I don’t want to see it anymore.

C- We are getting confused. All of a sudden, the MAC addresses have gone from tracking and privacy to access control. Cloning a MAC address doesn’t give you the keys to associate and get into the network. The idea that we have a MAC address that’s recognized is enough to get in is wrong. It just gets you to the next step. You still have to associate. And we do have proposals that change the MAC address continuously, but they were shot down because they required computation. Even then, if you pretend to be someone, you have to possess the keys to get into the network.

C- Personally, I think the MAC address is a problem in general. It’s a unique identity. It was designed that way. So unfortunately, we can’t get rid of MAC addresses. We would have to do something like IEEE 802.11bi and encrypt the header. Also, regarding the device ID, it’s being treated like a magical ID. It’s just signaled once in the 4-way handshake. The MAC address is the main identifier and is used all over again. So, I see the device ID as mapping your current MAC to your previous MAC. So, the MAC address is the unique identifier. For device ID, to make it more general to get rid of MAC address, we could extend the device ID somehow, putting it in an IE and protecting it.

C- I do not agree with that. The MAC address is not identifier. A MAC address should not identify a STA. Now, we have different use cases. For the captive portal, with a device ID, you’ll be locked in without further authentication. Trying multiple device IDs until one works is a possible attack there.

C- Privacy and security are not the same thing. Often there are overlapping solution, but not always. Privacy is relevant to the individual using the device. That’s why we started doing random MAC addresses. Getting into a network using credentials is a security mechanism. We should not use an over-the-air clear identifier to get into a network. We should provide services to the user when the user agrees to be identified, whether that’s by a lower layer or upper layer element. Identification should not be tightly coupled to the lower layers. We want to preserve the services to the user so that there’s a better experience. I don’t think we need to revisit the MAC address being used as an identifier.

Q- How do you want to proceed, Jay? We have comments on your proposal that need to be addressed to make progress.

A- I don’t care which solution is adopted. I hope we have a solution for pre-association use cases. WBA and WFA have such use cases. If we don’t agree to work on solutions using MAC addresses, I hope the task group will find another solution to those use cases.

C- We have to try again to identify the pre-association use cases and find solutions.

Q- WBA asked us to fix these broken use cases. If we don’t, then why do we have this group?

C- I’m stuck in the same spot.

C- I’m not fully convinced which pre-association use cases are the key ones. My current thinking is that probe requests are out of scope. This is mainly the about the AP recognizing returning non-AP STAs. I’d like someone to describe the process for a particular use cases in some detail. That would be helpful. I’m not sure what we are trying to address. If we can have a detailed description, almost to the flowchart level, that would be helpful.

C- We talked about several use cases on the reflector already.

C- I heard you say Neighbor Report and client steering. Access control I don’t understand. Measuring is probe request frames. That’s interesting.

C- I did two presentations on these topics: [11-22/1230r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1230-00-00bh-background-use-cases-par-privacy-etc.pptx) and [11-22/1650r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-00-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx).

C- I want TGbh to address the fake AP issue, even though it was noted as being out of scope.

C- Let’s hear those two presentations during the next call. And then we will try to get to the non-controversial topics as well. It would help to have discussions on the reflector to save time on the calls. Our next call is in two-weeks’ time.

**Meeting adjoined at 11:29 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 9/27 | De la Oliva, Antonio | InterDigital |
| TGbh | 9/27 | Halasz, Dave | Morse Micro |
| TGbh | 9/27 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 9/27 | Henry, Jerome | Cisco |
| TGbh | 9/27 | Kneckt, Jarkko | Apple |
| TGbh | 9/27 | Lu, Liuming | OPPO |
| TGbh | 9/27 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 9/27 | Malinen, Jouni | Qualcomm |
| TGbh | 9/27 | McCann, Stephen | Huawei |
| TGbh | 9/27 | Mutgan, Okan | Nokia |
| TGbh | 9/27 | Nezou, Patrice | Canon |
| TGbh | 9/27 | Orr, Stephen | Cisco |
| TGbh | 9/27 | Riegel, Max | Nokia |
| TGbh | 9/27 | Rison, Mark | Samsung |
| TGbh | 9/27 | Sam, Harvey | Broadcom Corporation |
| TGbh | 9/27 | Smith, Graham | SRT Wireless |
| TGbh | 9/27 | Smith, Luther | CableLabs |
| TGbh | 9/27 | Sun, Bo | Sanechips |
| TGbh | 9/27 | Thakur, Sidharth | Apple |
| TGbh | 9/27 | Yang, Jay | Nokia |
| TGbh | 9/27 | Yee, Peter | NSA-CSD |
| TGbh | 9/27 | Zuniga, Juan Carlos | Cisco |