Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, December 13, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-12-13 |
| 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 December 13, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting December 13, 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. EST.**

Agenda slide deck [11-22/2127r02](https://mentor.ieee.org/802.11/dcn/22/11-22-2127-02-00bh-agenda-tgbh-2022-dec-13.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)**
	+ Timeline discussion (slide 24)
	+ Teleconference plan, going forward (slide 17)
* **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:** [**11-22/0973r13**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record:** [**11-22/0651r9**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **Contributions (slide 16)**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Timeline**

The next major milestone is the initial WG letter ballot (on D1.0). That might have been possible for January 2023, but that’s rather tight. Plus, there are two major letter ballots going out in January that would have competed for attention with our ballot. Thus, it probably makes sense to target March 2023 for the initial ballot. All other milestones ripple from there, giving us an end date of April 2024. [There were no comments on this updated timeline.]

1. **Teleconference time discussion**

Thursday calls have a lower number of attendees overall, but some can participate on Thursdays and not Tuesdays, and vice versa. It seems like Thursday evenings are of limited benefit. This topic will be discussed during the next Thursday meeting before any decisions on future meetings times and days.

1. **CID resolutions for 12.2.11**

Kurt Lumbatis (ARRIS/CommScope) presented updated CID resolutions for 12.2.11 ([11-22/1329r11](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-11-00bh-cid-resolutoins-for-12-2-11.docx)). This version has inputs captured by Mark Hamilton that have revised resolutions properly marked as such and cleaned up instructions to the editor. It also has textual changes.

C- CID 65 needs to be changed to revised as well. And instead of using conditional clauses that are based on Device ID being active, we should just use the MIB variable value.

C- I disagree – the MIB setting changes the field value, so it’s a valid indicator of the Device ID activation state.

C- Understood. But you have occurrences where Device ID activation state is not based off of checking the field value. Some of those might be MIB variable checks, right?

C- At the cited sentence, this is the peer’s Device ID activation status, so no MIB variable would indicate that. Let’s leave the sentence alone.

Q- When did we decide that the identifier should be capitalized?

A- I’ve capitalized it until we decide what we are actually going to call it.

C- I’d prefer italics or quotes as capitalization rings all sorts of bells to me. Also, there’s a lot of embedded explanation in clause 12. I don’t think that’s necessary. That kind of text would be appropriate for clause 4 but shouldn’t be repeated in clause 12. The text could be tightened up by doing that.

C- We need specific details of what text would be moved.

C- Things like “upon an association” is unnecessary. I’ll provide some specific feedback offline to Kurt. If others disagree, perhaps we reach a different conclusion.

C- We need to focus on the last paragraph on page 7 of the contribution and the following paragraph on page 8. There were comments on the last paragraph. Now, when the AP receives an unrecognized identifier, it can either fail the association or assign a new identifier.

C- The AP can do whatever it wants. If both the STA and AP advertise they are supporting Device ID and then sends an unknown identifier, that’s the same as not sending one. Also, I don’t like the ordering of options as the first one appears to be our preference.

C- I don’t understand the note [at the bottom of page 7] at all. If the AP doesn’t recognize the ID, how can it supply an ID previously used by the STA. This is confusing.

C- This is previously suggested note text. It could be removed or changed.

C- There are comments in the chat in favor of note removal.

Q- The AP may fail the association. We should go deeper into how that works. Should we specify that the AP doesn’t send message 3 [of the 4-way handshake]. In this case, it might work, but it’s ambiguous. Not sending message 3 to fail the association doesn’t seem the way. Sending the Authentication frame with a status code of unknown Device ID would seem sensible.

A- I do think we need to define a status code as to why the association failed. I’m not sure it needs to be spelled out in this paragraph unless we give the exact code. This paragraph was added in November, where there was a desire for the AP to fail the association and the ESS wants to ensure the association is recognized before allowing the STA onto the ESS. Is it proper to lay out the failure mechanism in section 12? If so, new text is needed.

Q- I’m wondering if we won’t get ourselves in a loop if a non-AP STA attempts association and is being rejected due to the fact that the identifier (like one the STA remembers, and the AP has forgotten) isn’t recognized. Are we failing the association without a true cause?

A- I think this came out of comments in the November meeting.

C- My comment then was the behavior was the AP could do anything. That sort of text wasn’t helpful. The standard should describe an expected behavior in an error condition. We seemed to have narrowed down the text. That’s what my comment was about.

C- We had a bunch of discussion around this point and removed one option.

C- In terms of this idea of adding some sort of indication back about why the association failed, I’m nervous we get into the realm of denial of service attacks or sniffing out capabilities of devices that should or should not have security. It might give an idea of what the security stance of the AP is. I’m not sure if there’s a real problem here, but we should think about it.

C- I think I am agreeing with others. If the note in the text is valid, the AP should not fail the association, if the ID is not being used as a security thing but is just supplied to the upper layers to allow them to provide some sort of service. I find it difficult to see why the AP should fail that association. The note sort of says that APs don’t know what they are doing. That’s fine, but then it should be a reason why the AP doesn’t fail the association. The ID is used above Layer 2. There’s no danger of someone coming in. If you want to fail the association, the AP can do that. It always can. We don’t need to say that. I think we’re going down a slippery path putting that kind of text in. Let’s be simple and not too clever. I think it has to assign the identifier. You don’t just assign an ID. You find out from the upper layers why you are doing this. The reason for the ID is not at layer 2. I think if the ID is not recognized, assign one.

Q- Would that be a SHALL statement?

A- If we used SHALL before for no ID, then it should be a SHALL here too.

Q- Do we want to say it shall accept the identifier or keep the new one?

A- There are bigger questions to settle.

C- Right. We don’t know if we are going to allow STAs to generate IDs.

C- I understand the intention of keeping it simple, but at the same time we are trying to create a properly function scheme. If the ID is not recognized, it’s not super important. The STA is not recognized as a known STA. The whole point of IEEE 802.11bh collapses. We don’t have to think of all possibilities. It’s like a password ID. It’s not super critical. There is a feedback mechanism. The non-AP STA sends a password identifier. The network doesn’t recognize. So, the network sends back “invalid password identifier”. These sorts of mechanisms are already in the spec. Why not copy it here? Otherwise, from an implementation point of view, things will be messy.

C- I’m thinking this is an example of why this group thrashes. People have in mind their own use cases and think of solutions that work for those use cases. But those solutions don’t work for other use cases. It can’t be that the STA’s supplied ID is accepted always. Otherwise the IDs have little use. If we look at the grocery store returning shopper thing. Maybe someone else has used my telephone number for the frequent shopper program. Maybe that just means that I get some benefit from that other person’s spending. The binding isn’t tight. I don’t want to say we look at the issues tracking document again, but we need to look at more than our singular use cases.

C- Reflecting on why the group was created, it was to overcome problems when the MAC address was used in the upper layers by adding a new identifier for that purpose. While we are providing a mechanism to provide an identifier, we should not break what’s working. Failing the association breaks what’s currently working.

C- If I remember correctly, we already voted on different options in the last plenary meeting. We chose the two options. We don’t need to vote again. Let’s move forward.

C- It’s reading too much into it. In IEEE 802.11bh, we want to know that this is a station we have seen before. Initially, the AP gives the STA an ID. The STA supplies that on return. The AP could always give out an ID to the STA when it doesn’t recognize the STA. It’s that simple. We tried to put something concrete into the ID and that’s when we hit these problems. That’s the nice thing about Device ID. You tag the station and then you recognize it going forward (if it wants to be recognized).

C- The next paragraph covers a recognized ID. It can return the received ID as an acknowledgement. Or assign a new one for use going forward. Comments on this new text?

C- [Going back to previous paragraph] Aren’t there serious decisions that are made based on the ID? You can’t make those based on an unknown ID.

C- Those decisions are made at the higher layer.

C- If there’s an upper layer app that has to understand these IDs, then whether the AP recognizes the ID is meaningless. All of this behavior we are discussing is meaningless. It’s all opaque to the AP. The upper layer is making the decision.

Q- How did it work before? An unknown MAC address wasn’t just entered into the list of acceptable ones.

A- It was all done outside of IEEE 802.11 behavior. Go to some webpage, enter credentials, and have the MAC address added to the permission list. The text is improved, but I’m not happy with it.

C- One of the problems is that we don’t have a clear view of the pre-association use cases. I think I agree with the simple solution. The fact that the STA was recognized, if it meets the needs, that’s fine. The upper layer stuff is out of scope. If you connect to the ESS the first time, you get an ID. On return, the AP can provide the ID to the upper layers for a decision. This can work like the globally unique MAC addresses that were used before. It would be simpler if we could agree on not trying to bind other information into the identifier. That’s in the current draft for the post association case. The same level of functionality can be agreed for the pre-association cases, if we can agree on that. I’m not sure the group is willing to do that. If we do, it would make it easier for the group to agree on what language should be in the specification.

C- I think I mostly agree with the previous comment. Given that we currently have the sentence above the last paragraph on page 7, if we treat a STA with an unrecognized ID as being one that needs a new ID, that could also serve as indication to the STA that it wasn’t recognized and it should use the newly assigned ID going forward. But then we need a status code to indicate why an identifier was assigned because we allow the AP to assign a new one even if the old was recognized. [See first paragraph on page 8.]

C- In some cases, the MAC address is passed up to the upper layers. In others, like the grocery store, it’s an identifier for an account, not a device itself. If we get into the captive portal thing, you register a device, it uses something other than an app-assigned ID. That process would identify the device. That used to be a MAC address. It should now be the ID that is passed up to the upper layers. If the device is returning and the AP understands that, it could pass the ID up. If the AP updates the ID and passes that up, it would be similar to passing up a randomized MAC address, that is an ID that has not been seen before.

C- Let’s think about what that implies.

C- I agree that the passing up of the ID if it is a random ID is meaningless. The purpose is to allow the AP, when the MAC address is randomized, to pass up an ID to the upper layer instead of the MAC address. Just because the ID is random does not mean that what’s passed to the upper layers has to be randomized. It’s a mapping. The ID within the ESS and the higher layers can be constant. It can assume security context and previous security associations to a portal in a hotel. That’s what we are talking about with this ID. The over-the-air ID is not the actual ID that’s provided to the higher layers. That’s my understanding. I like the change Kurt made to the sentence above the last paragraph on page 7. That seems to solve the issue. Obviously, if the ID is not recognized, then there’s nothing to pass to the upper layer. It’s just bookkeeping for the AP to say, “I don’t recognize you, here’s a new ID for when you return.” It’s just as if it came in fresh. I don’t see security issues if it’s not identified. It’s just how we do the bookkeeping.

C- I should point out that this ID is protected from 3rd parties. The exchanges of the identifier are. It’s not going in the clear [in the 4-way handshake]. Not everyone is going to recognize it. But I’m fine to add it to the text.

C- That’s post association.

C- Right.

Q- What are people’s thoughts on the current text? If the AP doesn’t recognize the STA it assigns a new ID.

A- The problem is the non-AP STA side, it has to opt in. It decides if it wants to be identified. If the AP says, “I don’t recognize you” and the STA hadn’t opted in, then there’s no feedback to the user if we remove the last paragraph on page 7.

C- The paragraph doesn’t apply if the STA has not opted in. If the STA has opted in, then the paragraph does. Is the question what happens if the STA is recognized?

C- That new paragraph on page 8 doesn’t cover the opt-out.

C- Yes, we need to add signaling to distinguish between sending a new identifier when the old identifier was recognized and when it was not.

C- Offline, please say which comments are not being addressed.

C- We are nearly at closure, so let’s finish this topic. Other than the signaling text that needs to be written, are there concerns in going in this direction.

Q- What do you mean by this direction?

A- Do we agree with the sentence above the last paragraph on page 7 [as modified] and the first [new] paragraph on page 8.

C- It’s still not complete. The sentence doesn’t deal with the non-recognized case.

C- No, it’s in the modified sentence above the last paragraph on page 7.

Q- For clarification. The STA provides the ID in message 2. The AP provides a new one in message 3. Or repeats it. Message 3 always has an ID? Is that correct? A new KDE?

A- Yes, we would have to make protocol changes. Maybe the “I recognize you” status code doesn’t require sending the identifier back.

C- The status code would indicate why the identifier was assigned.

C- At a high level, I agree with the direction, but the return-the-identifier language is protocol and needs to be fleshed out. I would be happier if we didn’t say anything about the protocol here and keep things non-specific. So, in the last paragraph on page 7, the first option would be to indicate that the supplied identifier will continue to be used.

C- Recognizing that we need to specify the protocol later, are we agreement that this is the right direction?

Q- We will define signaling in the next round?

A- Now, or on the next call, or at some point. This is about direction, not process.

Q- This is assuming that the identifier is only passed encrypted, this is not a new random MAC address replacement visible to someone externally?

A- The first paragraph in 12.2.11 indicates that the exchanges of the identifier are protected from 3rd parties.

Q- So, if the non-AP STA wants a new identifier, can it force the assignment?

A- Yes, by not sending an identifier or by sending one that is not recognized. If the non-AP STA doesn’t provide one, the AP will assign one.

C- That satisfies my concerns.

Q- Is this text we can live with? Any more concerns? We will work on the protocol in clause 9 later.

Q- Returning the identifier if it was recognized would require signaling. Does the STA need to know why?

A- We have comments to that effect. It could be policy to rotate identifiers. It could be the STA-supplied identifier was not recognized. We could reject that comment.

Q- Why does it need to change?

A- I don’t know, but we have comments that want that. Maybe it needs to rotate frequently for pre-association cases. But that’s getting ahead of ourselves.

Q- Do we have consensus of the behavioral aspects written in clause 12.2.11?

A- I agree the direction is okay, but it’s not adequate for the clause it is in and the actions that need to happen. We need to be more specific. Are flags used? Is the same ID returned? Some other mechanism outside the 4-way handshake to update the ID at a later time. There are many things that can be done. I don’t think the text is adequate as it now stands. We need to be specific what the AP does when it receives an identifier it recognizes, either setting a bit in the response or returning the identifier.

Q- I agree we need to flesh that out as the next thing we do. Do we need to reorder the paragraphs in this clause to assist in understanding? Maybe we discuss that offline. Conceptually, the concern raised needs to be addresses. Can we agree that this text is an acceptable starting point? [No concerns noted.]

Q- Do we need a straw poll and then motion to put this text into the draft?

A- I’m not sure we need that at this time. Let’s just treat it as consensus for now.

Q- Do you want the text re-arranged now?

A- That’s probably okay and then there will be changes based on how the protocol discussion goes.

C- I would say that will a separate submission since this is a comment resolution.

C- Fair enough.

C- The paragraph for does not provide an identifier or provides an identifier that is not recognized has the AP providing a new identifier. That eliminates the association failure case. The AP always assigns an identifier if it is not recognized or present. The following paragraph talks about the success case (the identifier is recognized).

C- Right. We need a status code for that case too.

C- The Device ID KDE or something else will need to be modified to indicate status.

Q- When you saying status code, are you talking about a status code field or just a general indication?

A- From a protocol point of view, I would use a status code, even in the recognition case. The success case only says that behaviorally, not explicitly.

Q- I understand that. Is this a message 3 status code?

A- It’s not there now, but we might need it.

Q- Is someone proposing to add the two octets for the field into the EAPOL exchange?

A- Yes. We don’t have that now. I’m not sure exactly if it goes here. Or some sort of indication.

C- We haven’t gotten to level of calling it a status in the KDE or the EAPOL exchange. There seem to be multiple possibilities that we haven’t explored.

C- I would assume anything we do would be inside of the KDE, not a change to message 3.

C- Understood, not defining a status code in the EAPOL frames. It’s just something that is transported within the 4-way handshake.

Q- If we make a change in the Device ID element or the Device ID KDE, that would suffice. I’ll take a stab at that as a new submission to see if we can get agreement. Does that need to be reflected in clause 12.2.11? [Kurt Lumbatis to generate this text.]

A- Eventually. It will need to be in clause 9 and referenced in clause 12 (in the protocol part).

Q- Do we have consensus on this direction for these CIDs?

A- [No objections.]

Q- Do we need to mark the Identifier some other way?

A- I’m okay the way it is, but it’s fine as long as we don’t forget about revising it.

Q- So, these CIDs are on hold until we finish the clause 9 and clause 12 work?

A- Yes.

C- Okay. Cross references in the table above [with the CIDs] will need to be made.

1. **Update on ID encoding in pre-schemes**

C- There have been some emails on this topic. It seems to be moving to a common understanding. I don’t know what others think. I haven’t had time to look at [11-22/2150r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-00-00bh-clarification-of-requirements.pptx), but I’m not clear on what people are planning on using the pre-association ID for. My concern remains about using this for access control decisions. If we are making a STA recognizable and when it returns, leaving the rest to the upper layers, then we don’t need much more than a minimal exchange for the pre-association use cases. If we don’t agree with that point, then I would like to know what we are trying to do.

C- [11-22/2150r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-00-00bh-clarification-of-requirements.pptx) is asking what we are trying to solve. Do we need crypto or something simpler? This is a step back to the beginning. How far do we have to go? Do we have to solve spoof AP? We definitely have to solve tracking. The presentation is intended to focus on what we are trying to do. How much privacy is supposed to be in IEEE 802.11bh. Having made these decisions, we can decide on what schemes are needed.

C- That sounds reasonable, outside of the lack of the time. Those who can’t make the Thursday call will have to comment offline. Now, is something broken in the case that STAs use the same RMA when they return to the AP? That’s how things are done now. Is that sufficient for the use cases? Let’s discuss [11-22/2150r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-00-00bh-clarification-of-requirements.pptx) and determine if anything is really needed.

Q- It seems that pre-association use cases work in the field because devices generally use the same RMA when returning to the same ESS. Do we need to just document that behavior in the standard?

A- Remember we have discussed pre-schemes many times. Do we need to repeat which use cases we need to address? From the previous straw poll in November, most members agreed with schemes to address pre-association use cases. So, let’s move forward in that direction. Otherwise, we may not even make a ballot out of the next plenary meeting. In my previous contributions, there are a lot of use cases discussed. If we take a step back, the discussion will be even longer.

C- Fair enough. Pulling up previous conversations could take a lot of time. We will try to look at [11-22/2150r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-00-00bh-clarification-of-requirements.pptx) soon. And we will look at [11-22/1079r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1079-07-00bh-cr-for-sta-generated-id.docx) on the Thursday call.

C- Maybe Graham presents on the next Tuesday call.

C- We will have [11-22/1079r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1079-07-00bh-cr-for-sta-generated-id.docx) on Thursday, and maybe some of [11-22/2150r00](https://mentor.ieee.org/802.11/dcn/22/11-22-2150-00-00bh-clarification-of-requirements.pptx). To make a decision on that latter document will require time on a Tuesday call too.

C- Everyone: Think about if specifying that devices do what’s already done in the field with retaining an RMA on a per-ESS basis is sufficient and think of other schemes. The next call is Thursday evening followed by Tuesday morning.

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

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 12/13 | Ansley, Carol | Cox |
| TGbh | 12/13 | Baron, Stéphane | Canon |
| TGbh | 12/13 | De la Oliva, Antonio | InterDigital |
| TGbh | 12/13 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 12/13 | Harkins, Dan | HPE |
| TGbh | 12/13 | Henry, Jerome | Cisco |
| TGbh | 12/13 | Levy, Joseph | InterDigital |
| TGbh | 12/13 | Lumbatis, Kurt | ARRIS/CommScope |
| TGbh | 12/13 | Malinen, Jouni | Qualcomm |
| TGbh | 12/13 | Mutgan, Okan | Nokia |
| TGbh | 12/13 | Nezou, Patrice | Canon |
| TGbh | 12/13 | Orr, Stephen | Cisco |
| TGbh | 12/13 | Riegel, Max | Nokia |
| TGbh | 12/13 | Rison, Mark | Samsung |
| TGbh | 12/13 | Sam, Harvey | Broadcom Corporation |
| TGbh | 12/13 | Sevin, Julien | Canon |
| TGbh | 12/13 | Smith, Graham | SRT Wireless |
| TGbh | 12/13 | Smith, Luther | CableLabs |
| TGbh | 12/13 | -Sun, Li-Hsiang | Mediatek |
| TGbh | 12/13 | Thakore, Darshak | CableLabs |
| TGbh | 12/13 | Thakur, Sidharth | Apple |
| TGbh | 12/13 | Yang, Jay | Nokia |
| TGbh | 12/13 | Yee, Peter | NSA-CSD |
| TGbh | 12/13 | -Peng Yan | Wi-Fi Alliance |