Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, August 16, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-8-16 |
| 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 August 16, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting August 16, 2022 6:30 a.m. to 8:30 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 [11-22/1345r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1345-00-00bh-agenda-tgbh-2022-aug-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:**
* **Organization topics (see Backup slides)**
	+ July to Sept 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:** [**11-22/0973r7**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-07-00bh-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
	+ [11-22/1069r1](https://mentor.ieee.org/802.11/dcn/22/11-22-1069-01-00bh-resolution-of-a-few-comments.docx) – Resolution of a few comments (Dan Harkins)
	+ [11-22/1078r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx) – Device ID indication (Jouni Malinen)
	+ [11-22/1082r4](https://mentor.ieee.org/802.11/dcn/22/11-22-1082-04-00bh-cr-for-device-id-generated-by-network.docx) – CR for Device ID generated by network (Jay Yang) - updated
	+ Walk-through CIDs
* **Contributions (slide 16)**
* **WBA liaison response**

Any comments? None

Any objections to agenda? None

With the additional of an additional presentation by Kurt Lumbatis (ARRIS/CommScope) to the lineup,, the agenda ([11-22/1345r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1345-01-00bh-agenda-tgbh-2022-aug-16.pptx)) was accepted unanimously. There is an understanding that Dan Harkins’ (HPE) and Jouni Malinen’s (Qualcomm) presentations will not be given as neither was able to make the teleconference.

1. **Organization topics**

The timeline, as amended during the previous meeting, was displayed. Most dates from July 2022 onward have been pushed out by one meeting (*i.e.*, two months).

1. **11bh D0.2 CR for device ID generated by the network**

Jay Yang (Nokia) presented [11-22/1082r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1082-04-00bh-cr-for-device-id-generated-by-network.docx). The update includes an editorial update for CID 3 that rearranges section 12.2.11 based on email input from Mark Rison (Samsung).

C- There’s some impact from stations that have or have not opted in, so perhaps that should be mentioned in this document.

C- My understanding of opting in to use MAY/SHOULD language and use the MIB to indicate the opt-in status. I’d prefer not to put opt-in language here.

C- Maybe we can note the MIB variables.

C- Sure, once we have the presentations and the language with the right spellings.

C- I don’t see why we should start with this unexplained sentence in this section without prior explanation of identifiers.

C- This was my suggestion. I wouldn’t mind adding more text in this clause. It was pointed out that Malinen and others have done some rewrites of this text, so the text isn’t quite done. We don’t seem to have an introduction, but this was supposed to make it so we didn’t jump into FILS and FT first.

C- I thought we had decided two weeks ago to use this sort of language. I would say that when a non-AP STA joins an ESS and has agreed to be identified, it MAY send the identifier most recently received.

C- This CID that we are resolving asked that we clarify what identifier was being discussed (the one from an AP in this ESS). Other comments will build on this. So, if we can stay focused on the scope of this comment, other comments can come in later and modify it.

C- I sympathize, however the language still needs clarification. Putting this text up front about the non-AP STA sending the identifier is confusing because it should indicate how the identifier is first obtained. I’ve thought about rewriting this text, and I suggest we wait until there’s more input from other comments before satisfying this comment.

C- I’ll note that all of the sentences that were there talk about the non-AP STA sending the identifier without mentioning the source of the identifier. The remaining text then discusses more about the identifier.

C- This text is still based on the following paragraphs. I hope we can close this CID. If your proposal is not accepted, then I hope we can use this text.

C- I sympathize. The whole of 12.2.11 is being torn up by competing proposals. This does make it difficult to resolve the CIDs. I guess I’m fine with accepting the text now and then perhaps we accept further resolutions that change the text here.

C- If we talk about more about the language on the origin of the identifier, that would be good progress, even if it gets rewritten later.

C- I agree. We have several people assigned to different parts of the text in 12.2.11. Let’s try to get something cohesive, but let’s get this off Jay’s plate and move on.

C- Any objection to that direction? [None heard.] This CID is agreed by the group, knowing that future updates will amend it, and it’s still subject to motions to approve it.

1. **Device ID Synchronization and Control**

Kurt Lumbatis (ARRIS/CommScope) presented 11-22/1218r02. He noted that we have to come to agreement on how these device IDs are synchronized and controlled. He’s proposing a high-level control mechanism. We can then agree if this is acceptable. He envisions two MIB variables, one for the device ID feature being implemented and one for the device ID being activated.

Q- Did you describe where these implemented and activated things show up, or are these just a generic concept?

A- As discussed last week, we talked about implementing MIB variables for these ideas. Actual specification text is needed to implement these concepts.

C- My takeaway from that agreement was that device ID activated applied to a specific SSID and I wanted to be clear that that concept is covered in your text.

C- I have “in the network” to mean that.

C- I believe we agreed to use “SSID” in place of “network” so that there’s never confusion on what we are talking about.

C- I can change that. I note that we use BSS/ESS in other contexts.

C- BSS doesn’t substitute for SSID and the equivalency of ESS is being debated in ARC.

Regarding slide 5, 2nd row. This is the crux of the concept. No bits need to be sent. If the non-AP STA does not want to be identified, it just doesn’t put the device ID in whichever frame is being sent (based on FILS, FT, etc.)

C- I’d like to clarify that we are referring to the non-AP STA sending the device ID.

C- Yes, that’s the case.

Q- For FILS, did you mean the Association Request, or did you mean the FILS Authentication?

A- I thought it was Association Request as given in Section 9.

C- I admit, I’m fuzzy how FILS does it.

C- Tables 9-62 and 9-63 would seem to indicate in the Association Request.

C- I’ll hold off, I might be wrong.

Q- Could it be clarified why RSNXE capability is being used here? The benefit of using it is that it is protected to prevent thinking a device supports a capability when it doesn’t. But here, you’re only using it to indicate that you are going to send something in Message 2, which is already protected, so why are you using RSNXE capability.

A- I didn’t write that text; it was existing.

Q- Why do we need a separate capability indication at all?

A- To allow the devices to prepare themselves for these fields being in EAPOL frames later.

Q- I could see that from the AP’s perspective, but I don’t see why the non-AP STA needs to advertise this.

A- I don’t have an answer to that since I didn’t write that section.

C- In my view, the only thing the AP has to tell is that it has device ID implemented. Non-AP STAs only need to say whether they have activated device ID. Implementation status does not need to be transmitted on both ends.

C- I would agree with that. Only the non-AP STA needs to decide whether it wants to be identified on the network. I can update the table to show activated applying to the non-AP STA only.

C- I know we have used “ID blob” as a term, but we really need to do something to find better language for that.

C- I’m using “identifier”.

C- We need to be clear on what kind of identifier is being discussed.

C- Sure. This presentation is more about the control signaling. The truth table needs to be broken out more clearly about what the AP and non-AP STA do.

C- I think this is complicating a simple idea. There are too many bits. If we are talking about a non-AP STA that wants to be identified, it tells the AP so. If it doesn’t, it can indicate that too. This presentation seems to complicate things.

C- What I’m trying to say is that if the non-AP STA wants to be identified and it’s using FILS, it does this. If doing FT, it does that. The logic is simple.

C- But the presentation seems to complicate it. If the STA advertises that it supports using an ID, the AP will give it an ID. The next time the STA associates and it wants a new one, it doesn’t send the old ID. This signaling can save the AP from generating and running out of IDs, which isn’t unreasonable. You really need to say where these bits are, where activated and supported bits are sent. I think the how part is clear, but I’m not sure the use of the bits is clear.

C- I think we have to allow on a per-network basis for a STA to say, “I want to be identified”.

C- I agree. But once it says that, things are straight as it says in the existing text. The important thing is where these two bits come in and are they the same as the support bit? You have it implemented as a ‘1’ on slide 6 and activated set as a ‘1’. Then you have a support bit in the extension.

C- Last week, we discussed that we needed two MIB variables, one for implemented and one for used.

C- Are there two bits for implemented and support, or are they one bit?

C- Well, now you have a problem. If it’s set in the extension element and not set in the other place where these bits are used, then we have a problem.

C- You need two, one to say I implemented this and then one to say whether the STA wants to use it.

C- These variables aren’t transmitted.

C- This discussion is going in circles. Can you discuss the bottom of slide 5 and why we need to different rows and whether that’s useful?

C- This seems similar to an earlier presentation from a few weeks ago in which there was a separate bit signaling if there would be a device ID in the FILS or 4-way handshake. I’m surprised that if you look at the KDE in message 2 of the 4-way handshake, I’m not sure it’s encrypted.

C- It’s encrypted by the PMK of the 4-way handshake.

C- I don’t think that occurs until message 3.

C- Irrespective of what we are doing in TGbh, I’m not sure the KDE can be encrypted.

C- It’s an optional feature of message 2 and we agreed that if it is in message 2, it is encrypted.

Q- Could someone point me to the spec where message 2 encryption is implemented?

The current 12.7.3 [?? Is this reference right?] states that encrypted key data == 1 if the device KDE is included.

C- I’m not sure I’ve heard an answer to why we want to indicate both implementation and activation? Why not just signal whether the STA wants to use it?

C- I guess that would be for a per-network basis. One is a user control, one is an activation of the feature.

Q- Why does the network need to know that it has been implemented but not switched on.

A- We could say that we won’t say that we set the bit in RSNXE.

Q- I’m trying to understand why you would say that you have the software but aren’t using it.

A- This goes back to the earlier point about the significance of the bottom row of slide 5.

A- This could prevent the AP from expending resources on generating an ID when the STA is just going to throw it away. It lets the AP know that this is a STA that wants to maintain its privacy. If it’s using an out-of-band mechanism to signal it is a returning STA, it can do so.

C- I’m not sure I buy that. The AP doesn’t need to know why the STA doesn’t want to use device ID. I think the semantics of the second row on slide 5 is being overloaded. I’m happy to continue this discussion on the reflector.

C- Do we need all these bits? If the non-AP STA knows that it is keeping a BSSID/ESSID list, then it’s just a matter of setting the activation bit in the RSNXE. You can have the two MIB variables to determine that one bit in the RSNXE.

C- Let’s continue the presentation, which may clear up this up, starting slide 7.

If a non-AP STA does not indicate that device ID is activated, then ID blob is meaningless. If it does indicate activation, then an empty value for ID blob is indicative of the STA’s desire to obtain such a blob.

C- The first time the non-AP STA comes to the AP, it has to indicate whether it wants an ID blob.

C- That’s what the second row on slide 7 means.

C- This is a major change, but I understand that row now.

C- That second row means, “I don’t have an ID, but I want one.”

C- One of the things of having the separation between activated and implemented is it gives flexibility. You can connect to a network and then choose whether you want to be identified or not. That’s helpful in the captive portal case. The decision of when to be identified by the network is an important one. After I’ve read the terms and conditions and what it’s going to cost me, then I can decide if I want to be identified on this network. So, it’s not just the choice of being identified, it’s also the timing. Lumbatis’ work allows that.

On to slide 8, this shows that the STA use of device ID is activated and here’s the ID it wants to use. On slide 9, this is the AP side. Nothing happens if the device ID activation is not indicated. If the indication is there and the ID blob is empty, then it the AP knows it needs to generate an ID blob and send it to the device. Where that ID blob is placed depends on what’s being done (FILS, FT).

C- I don’t see why we need an empty KDE to signal on top of the device ID activated bit.

C- We would need to discuss that and consider whether we want to change the logic in the presentation. Should we discuss it offline and see about bringing it back as a group consensus? And add some straw polls then.

C- We can do straw polls now, if desired. Does the group want to discuss the topic more?

C- This was supposed to be a simplification of the logic in the STA. It doesn’t have to think. It just has to put in whatever it has, empty or an ID.

C- We should combine that with slide 6 (implemented and activated on).

C- Maybe I missed a point in the logic.

Q- The second row in 7 is you have implemented it and activated it. Does the empty blob and the activated bit signal the same thing?

A- The empty blob can’t be distinguished.

Q- If you have set the bit in the RSNXE, is that sufficient to not need the empty blob? Or do we use the empty blob and not use the bit in the RSNXE.

A- I’ll need to think about that.

C- The point was made that the options are no blob, empty blob, or some blob included. These three options are trying to indicate the same thing as the activated bit. I’m not seeing how this all works together, but perhaps we come up with a setup to how they are used.

C- Perhaps the tables should be combined to show things are used all together.

C- Slides 7, 8, 9, and 10 all assume the activated bit is set.

C- I think what is missing is how you deal with these two MIB variables. How you indicate your status to the AP. If you associate without a KDE in message 2, it’s clear the AP is going to give you an ID. The only case that’s not clear is when it doesn’t want to be identified. The STA should indicate that it doesn’t support identification. What the AP sees is what we are struggling with.

C- I’m proposing to the use the device ID element or device ID KDE as the indication that the STA wants to be identified. I can make the RSNXE logic work as well.

C- You need to make a proposal of how to do this from the outside looking in. The logic is fine, it’s how the STA tells the AP, how many bits it needs, and where you put them.

C- This goes back to why it needs to be seen in one table to understand all of the scenario.

C- In general, anything that goes into the RSNXE should be static for the duration of the association. I don’t see the use case for a STA saying it implements a feature that it doesn’t activate for the association. A STA not initially using an identifier until after it fully identifies the network, other approaches could be used, by including a KDE or using an Action frame. I’m not sure if we didn’t have an RSNXE indication and just relied on the KDE in message 2, do we have downgrade protection? Is frame modification detectable? I’m not sure, but this should be checked. Downgrade protection is important.

C- I don’t have an answer for that at the moment as to whether a spoofed message 2 is identifiable and action can be taking. As for the STA associates and then later decides to be identified, the only way to do that is in the initial security handshake. The Action frame concept was rejected by the group.

C- But that first conversation about detecting frames that have been modified sounds like it should be part of the offline discussion.

Q- Device ID activated and implemented will be done at the MIB level, right?

A- Yes. They will be signaled up through the device to activate or deactivate features.

Q- There are no control bits in the frames that indicate anything?

A- Right. Revision 1 of the presentation had control bits, but they have been rethought and removed.

C- On slide 7, second row, procedurally, the current draft signaling flow is a little confusing. In the first association, there’s only one KDE from the AP to the STA. I think this row is what’s confusing people. They are ignoring the empty blob happening during the initial association when the STA wants to be identified.

C- Yes, that’s the signal to the AP that the STA needs to have an ID assigned.

Returning to the presentation at slide 10, the AP’s response if the device ID is activated and the ID blob contains an actual ID comes down to whether the ID blob is recognized. If it is, the AP doesn’t need to send an ID again. If the AP does not recognize the ID, the AP has to decide if it wants to allow the use of this ID by the device.

C- That logic about what the AP does if it doesn’t recognize the ID blob is a change. How quickly can the AP determine what to do between message 2 and message 3 based on that unrecognized ID blob.

C- I was just trying to say what the AP response was in all cases.

C- Yes, but if the ID blob is not recognized is a bigger question and covered in other CIDs.

Q- Why does the AP not insert a device ID if it recognizes the existing ID? That rules out an ID update capability.

A- You’re right, I shouldn’t rule that out.

Q- If the ID is not recognized by the AP, the logic doesn’t indicate what the STA should do after receiving message 3 and not being given a fresh device ID.

A- In that case, the STA goes on believing that the AP is satisfied with the ID the STA presented, and it keeps using it. In the last part of the slide, the AP supplies a new ID because it didn’t recognize the presented ID.

C- If the AP doesn’t send a new ID when it doesn’t recognize the presented ID, the STA will keep using it, but the AP still won’t recognize it. It would be better to simplify things and let the AP signal whether it recognizes the STA or not.

C- That’s what returning or not returning message 3 means.

C- You mean don’t return a device ID in message 3, not return message 3.

C- Correct. I was just trying to do things simply without defining new bits.

C- You need to think how the logic works.

C- The important thing is what the device ID is. If the STA gives something the AP doesn’t recognize (due to ID age, arbitrary deletion), if the AP receives the ID, it presumably provides a service. If the STA gives the ID and doesn’t get the service, it should know what to do. This is probably part of a higher layer application that has the logic that means it doesn’t have to all be done at layer 2.

C- We need layer 2 signaling back and forth to let both sides know everything is okay.

C- I don’t see any reason to worry about any of this. If the AP wants to maintain the existing ID, it just sends it again. If device ID activated is set, the AP should always send the ID, whether it is the one the STA presented and the AP understood, or a new one if the AP didn’t recognize it. Having a blank thing mean something makes me uncomfortable. We don’t need a bunch of bits either. The ID value suffices along with upper layer logic.

C- I think this is where things get messy. If the messy is not recognized, we might have a problem. In scenario 1, a legitimate user deleted the ID, or the ID blob was corrupted by the channel. But there’s a scenario in which a 3rd party mounts an attack by using a random ID blob that is then not recognized. More consideration is needed for when the ID is not recognized.

C- We should take the CIDs one at a time, but we should look at where security issues can arise in each step.

Q- Isn’t there text needed in section 11 (of the base specification) around this.

A- It is surprising that we haven’t gotten into that section yet. Let’s continue that discussion offline.

C- Given that, then we should defer going through the text submission that goes along with this presentation, since the text goes along with the logic in the presentation.

C- A flow chart would be helpful.

1. **Upcoming motion**

A motion on pre-association identification will be run on August 30th based on text that is being batted around on the reflector, assuming no one has any immediate concerns. [None noted.]

**Meeting adjoined at 11:27 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 8/16 | Ansley, Carol | Cox |
| TGbh | 8/16 | Dash, Debashis | Apple |
| TGbh | 8/16 | Derham, Thomas | Broadcom |
| TGbh | 8/16 | Halasz, Dave | Morse Micro |
| TGbh | 8/16 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 8/16 | Henry, Jerome | Cisco |
| TGbh | 8/16 | Kang, Sugbong | Apple |
| TGbh | 8/16 | Kneckt, Jarkko | Apple |
| TGbh | 8/16 | Lan, Zhou | Apple |
| TGbh | 8/16 | Levy, Joseph | InterDigital |
| TGbh | 8/16 | Liu, Yong | Apple |
| TGbh | 8/16 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 8/16 | Montemurro, Mike | Huawei |
| TGbh | 8/16 | Mutgan, Okan | Nokia |
| TGbh | 8/16 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 8/16 | Petrick, Al | InterDigital |
| TGbh | 8/16 | Rison, Mark | Samsung |
| TGbh | 8/16 | Sam, Harvey | Broadcom Corporation |
| TGbh | 8/16 | Smith, Graham | SRT Wireless |
| TGbh | 8/16 | Smith, Luther | CableLabs |
| TGbh | 8/16 | Thakore, Darshak | CableLabs |
| TGbh | 8/16 | Thakur, Sidharth | Apple |
| TGbh | 8/16 | Wu, Tianyu | Apple |
| TGbh | 8/16 | Yang, Bo | Huawei |
| TGbh | 8/16 | Yang, Jay | Nokia |
| TGbh | 8/16 | Yee, Peter | NSA-CSD |