Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Interim Meeting Minutes, September 2022  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2022-09 | | | | |
| 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 September 2022 Interim meeting.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting September 12, 2022, 10:30 a.m. to 12:30 p.m. HST**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the meeting to order at 10:33 a.m. HST.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/1282r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1282-02-00bh-agenda-tgbh-2022-sept-interim.pptx) (updated over the course of the week to [11-22/1282r06](https://mentor.ieee.org/802.11/dcn/22/11-22-1282-06-00bh-agenda-tgbh-2022-sept-interim.pptx)). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
  + September Interim meetings: Monday, 10:30-12:30; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00
  + Approve July plenary and July/Aug/Sept teleconference minutes
  + Timeline update review
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [11-22/0651r5](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-05-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [11-22/0973r9](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-09-00bh-cc41-comments-against-d0-2.xlsx)
* **Contributions (slide 22)**
* **Way forward to D1.0 (slide 23)**

1. **Approve Minutes**
   1. July plenary session: [11-22/1272r1](https://mentor.ieee.org/802.11/dcn/22/11-22-1272-01-00bh-minutes-tgbh-plenary-meeting-july-2022.docx)
   2. Teleconference minutes:
      1. July 26: [11-22/1234r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1234-00-00bh-802-11tgbh-telecon-minutes-july-26-2022.docx)
      2. Aug 2: [11-22/1351r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1351-00-00bh-802-11tgbh-telecon-minutesaugust-2-2022.docx)
      3. Aug 16: [11-22/1362r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1362-00-00bh-802-11bh-telecon-minutes-august-16-2022.docx)
      4. Aug 23: [11-22/1374r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1374-00-00bh-agenda-tgbh-2022-aug-23.pptx)
      5. Aug 30: [11-22/1441r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1441-00-00bh-802-11bh-telecon-minutes-august-30-2022.docx)
      6. Sept 6: [11-22/1532r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1532-00-00bh-802-11bh-telecon-minutes-september-6-2022.docx)

Moved: Peter Yee

Seconded: Graham Smith

Result: Unanimous Consent

1. **Timeline**

The timeline currently shows a desire to have an initial working group letter ballot on Draft 1.0 this month, but that is admittedly somewhat questionable.

Q- What constitutes Draft 1.0? Isn’t it supposed to be feature complete?

A- The procedures don’t use that term, but they imply that the document should be feature complete.

C- I don’t think we have to struggle with this, procedure wise. I wouldn’t be comfortable bringing an incomplete document before the WG and it would be a large waste of time.

Q- Could you clarify where we are? We have two outstanding points: 1) STA generation of ID, and 2) identification of the STA by the AP prior to association.

A- There’s a third one point, which constitutes a collection of smaller issues. We are not making a lot of progress on the first two points because none of the proposals on those topics have not received 75% support needed to incorporate them into the specification. If a majority of the group feels that a topic should be covered and yet it is not incorporated, then we’re likely to be stuck when it comes time for a working group ballot, because we won’t get 75% approval there. Thoughts?

Q- I thought STA generation of the of identification was less controversial than the pre-association identification. Do you agree?

A- The difference between those two are subtle in terms of support. We have a presentation on Wednesday that might be helpful.

C- We have to be careful with the pre-association case, because there are multiple sub-cases there. Maintaining an identity not tied to a particular prior association or device, so that a network hearing that identifier recognizes the non-AP STA coming into an environment is one use case. We need to be careful and perhaps split the pre-association use cases into separate use cases or sub-use cases and advance those that we can.

C- I’ve noticed a couple of people talking about using the MAC address again as an identifier. I’d like to request we not go down that path again. RCM was a notable effort to get away from using MAC addresses that way. Let’s not push for MAC addresses as identifiers.

C- That’s the problem. A one-time MAC address is what’s being proposed and not as a universal identifier. That was an unfair comparison of MAC addresses before and the current proposal. These are not universal MAC addresses and are for use only with the network for which they were generated.

C- What I’m trying to say is that even using a specific MAC address for a particular network can lose privacy. The MAC address is used over the air clearly, allowing nearby devices to profile the STA.

C- It’s a one-time MAC address. So, it cannot be profiled or tracked. The RCM can also be tracked depending on how long it is used. Just because it is using a MAC address as an identifier does not mean that everyone can identify and track the device. Do you want to have pre-association identification or not?

Q- Why is it perceived that there is a privacy issue?

C- This is a good discussion, but really, we were just looking at the timeline. Let’s get to the meat of this discussion with a presentation. I do want the group to be thinking of the timeline and how we can reach consensus.

1. **Issues Tracking**

C- The issues tracking document ([11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)) covers our thinking on use cases. The motions recorded in [11-22/0651r05](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-05-00bh-tgbh-motions-list.pptx) show formal decisions taken. The spreadsheet covering comment collection resolutions is found in [11-22/0973r09](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-09-00bh-cc41-comments-against-d0-2.xlsx).

1. **Issues Tracking**

Jouni Malinen (Qualcomm) presented [11-22/1078r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx) on “**Device ID indication**”. It covers CID 50 (the part about the identifier vs. a new identifier), CID 51, and CID 52. For CID 50 about section 12.2.11, Malinen has new text to differentiate identifier and new identifier, but overall this topic will be covered separately as part of the “opt-in” rewording that someone else is contributing. CID 51 is accepted in revised form by supplying proper names for particular 4-way handshake message references in the text and making other small clarifications. CID 52 is similarly resolved.

C- My upcoming contribution pulls some of this in, so it might be helpful to look at that.

Q- You’re next in line to present your document. Is it in alignment with this presentation?

A- Yes, quite so.

Q- Any objection to going to that presentation?

A- None.

Kurt Lumbatis (ARRIS/CommScope) showed [11-22/1329r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-03-00bh-cid-resolutoins-for-12-2-11.docx)., which is about “**CID resolutions for 12.2.11**”. It covers all the comment resolutions for section 12.2.11, including CIDs 50, 51, and 52. It rewrites the text of 12.2.11 (Device ID indication).

Q- Why did you take out the BSS in the paragraph (leaving only ESS)? For most home AP situations, an ESS is basically just a BSS. It gets confusing not to allow for the single BSS case. An ESS implies a DS and multiple APs.

A- This came out of the discussion from our last teleconference, and I was asked to remove BSS from the text.

C- I think the case of a single BSS as an ESS is allowed and doesn’t require a DS. I think it’s confusing to say BSS or ESS.

C- It would be helpful to have a redline against the current draft to determine what’s really being changed. The redlines in this document are confusing.

C- Those redlines are against earlier versions of this document itself, not the baseline. If we reach agreement to do so, I can change over to a redline against the baseline.

C- The statement about an ESS recognizing a non-AP STA, I find questionable since this is a network-generated ID. Where in an ESS does that networking aspect come into play? I’m uncomfortable removing network from the text, because I don’t think the ESS is supplying the ID. The ID is passed through the ESS by the network.

C- This arose from the conversation about “what does ‘network’ mean?” IEEE 802.11 doesn’t define that term. So, we needed something else. If we need more words than ESS, we can consider that.

C- I think ESS is the correct term here. There are things that are just outside of the scope of our standard. I would object to going beyond ESS, although we can clarify what the ESS is doing.

C- It’s not the ESS that’s make the identity, but the AP that does so after some network entity tells it to do so. Yes, all the APs have to have this information and it is distributed by the ESS and it comes from somewhere, but it’s the AP that does the recognition.

C- I think it’s the AP that we are talking about here.

C- I’m not sure that’s correct.

C- [Suggestions of “all of the APs” or “each AP” in the chat.]

C- What about to provide the ID to any AP in the ESS to allow the AP to recognize the device.

C- That might be acceptable.

C- The sentence is too complicated. It’s a compound sentence. We try to use simple statements. That helps to make things clearer.

C- Maybe we work on that offline and bring something back to the group. To be clear, we are looking to define what an identifier is and use that term universally.

C- Maybe we spell identifier with a capital ‘I’ to remind us that we need to replace that with a term, once we figure it out.

C- A STA indicated activation of Device ID differently between when using FILS (Fast Initial Link Setup, IEEE 802.11ai) and when not doing so.

C- It might be clearer to discuss STAs and APs in the Association Request and Response in separate sentences.

C- The deletion of the parenthetical elements indicating non-AP STA and STA might be making it harder to read.

Q- Do we allow APs to send new identifiers to non-AP STAs that haven’t activated the feature?

Q- Do you support having this one-bit field somewhere? I think there’s some advantages to having the bit there as it will lower the traffic over the air by setting an expectation of what’s supported and therefore the appropriate behavior.

Q- We need to be careful to remember that this is the RSNXE and not RSNE, which are different things. The flow diagrams (lower in this document) start from the non-AP STA’s side. So, it’s not clear that the AP is getting any information to help it optimize. Will the AP discovering that it needs to generate a new identifier in the middle of the 4-way handshake slow things down? Do we want to optimize the non-AP STA to not have to send in the Device ID if the AP does not support it? Maybe we do want the AP to advertise that it supports Device ID. If so, where’s the best place for the necessary bit? RSNXE or is it a basic capability bit?

A- The Beacon frame and the Association Response frames can convey this information. I think it’s less important to optimize the non-AP STA, which has less work to do anyhow. I’m assuming the ESS will have the capability or not.

C- There’s a case for both sides needing to know. The AP needs to know about a returning STA. This helps the AP know that as the STA requests an association, it can know to expect a device ID. If the Device ID is the MAC address that the STA is presenting, the AP knows to check it as a Device ID and not just treat it as a MAC address. A STA would like to know if the AP supports the feature, because it could then choose an AP that supports it over one that does not.

C- All that needs to be said is that the STA sets the bit. Put the capability bit wherever. No need to separate out FILS and non-FILS until you try to associate.

C- I’m not understanding how the AP or the STA advertise support prior to message 2 in the 4-way handshake.

C- Advertising support allows the AP to know what to do during the 4-way handshake. Otherwise, there’s confusion.

C- I don’t understand. We associate. Then during messages 2 and 3, the STA and AP let each other know about their capabilities.

C- That’s way more complicated. What’s wrong with indicating things up front. It’s cleaner.

C- The optimization is to allow the AP not to send a new identifier when the STA does not supply one. That’s why this bit is here. To tell the AP to provide one if the STA did not provide one.

C- There are three situations. Non-AP STA has an identifier and wants to use it. The second is the STA doesn’t have one but supports it; it signals in message 2 that it wants one. The second is the STA doesn’t supply anything in message 2, so the AP doesn’t supply one in message 3.

C- This document seems to support that, but I’m not sure the optimization is done right here. Clarification is needed on the bit placement for optimizing. The question is whether the AP gets information early enough to do something without a delay.

Q- I’m trying to understand what was said earlier. Is the indicator only sent in message 2 from the STA? If the Device ID is being used, isn’t association required in order to choose which credentials to use?

A- We might have a chicken-and-egg problem that we haven’t discussed before.

C- That gets back to whether we want the AP to identify the STA before association.

C- This bit would be in Beacons and Association Requests.

C- It would also be in FILS without the text around that differentiation between FILS and not.

Q- Can we agree that a STA shall not send a Device ID to any AP that does not indicate it supports it.

C- We need to indicate where.

Q- Is there any way we can get to sending the Device ID without having seen the RSNXE?

C- The RSN element is a capability. It doesn’t say it’s active. Don’t we need to say that separately?

C- We need to reword the text to say its active and not just supported.

The presentation then went on to the text about “When a non-AP receives a zero-length identifier…”.

C- I’m against zero-length things and don’t see the benefit. And sending that to an AP for the first time, doesn’t seem right. I’d like to see this paragraph removed. There’s something different between “I have this active and I want a Device ID” and “I have it active and don’t want one”.

C- The use case is that Device ID is active, but the first time you connect to a new ESS, you can ask for a Device ID.

C- The capability bit in the RSNXE can do that. The capability bit is sufficient without the zero-length Device ID. No need to say that Device ID is active, but I don’t want a Device ID.

[Discussion flowed back and forth about what the STA does to indicate its desires.]

C- The group seems to be mostly not in favor of the zero-length identifier.

C- I feel the logic of the zero-length identifier provides a helpful symmetry.

C- The first association is tricky because subsequent associations depend on that first one. Zero-length thus makes sense to me.

C- The consensus still appears to be against zero-length. But a presentation defending its addition would be helpful.

C- There are benefits to both the capability bit and zero-length. But I don’t really want both.

[A flow diagram with FILS and non-FILS cases would be helpful to understanding how all this works. Offline discussion is suggested as well.]

**Recessed at 12:30 p.m. HST.**

**Meeting September 13, 2022, 1:30 to 3:30 p.m. HST**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

Mark Hamilton, the TG chair, called the meeting back to order at 1:33 p.m. HST.

Policies and procedures were presented. No responses to call for essential patents. Copyright slides were presented.

1. **Agenda**

The chair displayed a new revision to the agenda.

Chair: That means we first consider [11-22/1599r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-00-00bh-revisions-to-rsn-extension-element.docx) and then return to [11-22/1329r06](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-06-00bh-cid-resolutoins-for-12-2-11.docx)?

Q: I have been working on opt-in comment resolutions based on our 0.2 draft, but we seem to be discussing very major changes in some parts of the document. Is 0.2 draft still a good baseline?

Tech-Ed: Editorial comments are considered last in case technical contributions change text that renders them unapplicable. If you want to build on someone else's changes, make changes in their draft, even though it's not approved yet.

C: I will try to address this offline.

C: We have not actually approved any updates to the draft, so in my view 0.2 draft should still be a good baseline.

1. **Contributions**

Kurt Lumbatis presented [11-22/1599r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-00-00bh-revisions-to-rsn-extension-element.docx) on “**Revisions to RSN Extension Element**”.

The presentation changes the label Device ID Support to Device ID Active.

C: I don’t understand how this aligns with our MIB activities?

Q: This bit is in the extended RSN element? I think that how it works is that it’s a single, global bit on the AP. And so, the AP sets it to true in beacons, probe responses, etc. On the non-AP STA side, the value of that bit could vary depending on the network you connect to? And that behavior needs to be per SSID. That would cause us to have to structure the MIB with a view to having one bit per SSID. I think the only time the non-AP STA sends an extended RSN element is in the association phase?

C: I don't think we have a list of profiles on the non-AP STA. I think it’s enough with a single MIB variable on a non-AP STA.

C: I’m confused why we would want to be structuring a MIB variable around this bit. This bit tells the AP that the requesting device wants an ID. Then the requesting device can use the ID if it wants to. We don’t need to specify that it has to use it.

C: You do have to track on a per-SSID basis whether you want to store an ID from that network.

Q: Why wouldn’t the STA just say, “always support”?

A: So that we optimize and don’t send out IDs to STAs that are not interested.

Q: What are the use-cases for this?

A: We only have a network-generated ID, so the STA isn’t giving up anything by forcing the network to generate an ID that it will never use. If we have a non-AP STA-generated ID too, it could be convenient to be able to signal this.

C: But you don’t know the network you connect to, in general. The terms and conditions are not known at the time of association, so it’s not a choice you can make at this time of the connectivity set-up.

C: I think if we use this design, it will only be implemented in such a way that the non-AP STA tells the AP it wants an ID always anyway. It’s too soon in the association process. After the handshake would seem a much more intuitive place for this feature to me.

C: I don't see the burden for the AP of generating IDs.

Q: Relating to device ID per ESS. Have you considered the case where you want to be identified by an ESS at some times, but not at other times?

Q: I’m confused that yesterday we had a zero-length identifier to indicate that an identifier was wanted, and that was rejected. But now we have an even more complicated system with a bit that gets flipped on and off.

C: We could put this only in the beacon. We’re trying to solve network problems, so if the network puts this information in the beacon, the non-AP STA will find it. Then the non-AP STA can indicate only after it knows the AP has this capability whether it wants to profit from that.

C: We don’t need to toggle these abilities back and forth. An ID is provided, part of how the association is configured, if the non-AP STA does not want to do it, they throw away the ID. I don’t see that we need to do very heavy tracking in a MIB or similar.

Chair: We may need to go back and review what’s been done, where we are, what the scenarios are that we want the text to be able to accomplish.

Jay Yang (Nokia) briefed [11-22/1079r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1079-03-00bh-cr-for-sta-generated-id.docx) on “**CR for STA generated ID**”.

This is proposed resolutions to 11 comments that concern STA-generated IDs. There are open questions with respect to pre-association use-cases and whether TGbh should also supply a STA-generated ID. Different options to combine existing proposals exist.

C: Regarding the case where multiple RMAs (random MAC addresses) are generated, which rules are actually proposed? To me it seems it’s fully decided by the non-AP STA the way you’ve currently phrased it. The AP would then have to remember all those RMAs, and that could be up to 65000 addresses per STA, and they would then all need to be verified. That will be very expensive computationally for the AP, so we need to keep that in check.

C: I like the introduction of several RMAs. This is a big improvement to precious rules-based RMAs we’ve seen presented, but I agree we need to think about AP overload.

A: In our presentation we don’t mention that many specific examples of where additional RMAs would be computed or checked. That could be a start for limitation. We would also welcome comments on this text.

C: I would like to see a separate subclause describing how you protect this system against active attacks. We can take this offline.

Q: Will we have a straw poll?

A: Yes.

Q: Why do we have these two proposals?

A: The use-case document specifies that we need some pre-association mechanism for identification as well.

Q: As far as I recall we had a lot of discussion on this, we then had a motion on the pre-association use-case in the last meeting, it failed. Are we now bringing back the pre-association use-case?

A: The issue tracking document and use-cases tracking means we need to meet these use-cases to finish our job.

C: In general, our draft 0.2 already covers some device identification.

C: I support this direction and I think we should focus more on how to generate and discard addresses. We need a bit more management of how discarding and changing the MAC addresses will actually work.

C: We may also need some information on the frequency of address changes implied by this text.

Chair: Should we do a quick straw poll on whether to continue in this direction?

C: Our preference is keeping the option here with both MAAD MAC and RRCM.

C: I want to keep things simple in this amendment, so I would not be very favorable to putting in two additional mechanisms.

C: I think we need to keep in mind a third way forward which is to have none of these additional mechanisms.

Chair: We are out of time for this session. Any other business?

**The meeting was recessed 3:31 p.m. HST.**

**Meeting September 14, 2022, 8:00 to 10:00 a.m. HST**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

The meeting was convened again at 8:03 a.m. HST.

The agenda is now [11-22/1282r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1282-04-00bh-agenda-tgbh-2022-sept-interim.pptx). Policies and procedures were briefed. No IPR issues were noted.

The group is attempting to determine how we can make progress given strongly opposed parties who favor network-generated IDs and STA-generated IDs.

1. **Contributions**

Antonio de la Oliva (InterDigital) presented [11-22/1588r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1588-00-00bh-resolution-comment-32-11bhd0-2.docx), which provides a “**resolution for comment 32 for 802.11bh**”. The resolution of this comment is to clarify when the Device ID element is present in the Association Request and Response frames.

C- I don’t think you should eliminate the optionality of the Device ID’s presence, because it might not be present if the non-AP STA does not have one at the moment.

C- Because this amendment will be rolled into IEEE 802.11, the base specification, the optionality is required unless IEEE 802.11 would be required to use it in all cases. And that doesn’t seem likely.

C- The non-AP STA has the right not to send this information if it does not want to.

C- The optionality in the case of dot11DeviceIDActivated being true needs to be contemplated.

Q- If dot11DeviceIDActivated is true, if the STA doesn’t want to send the Device ID, why doesn’t it just turn the value to false?

A- The STA might make a decision based on the protocol steps that come before.

C- I agree, there’s no requirement for the STA to identify itself if it does not want to. This comes down to what the device wants to do and whether the application the device is running can benefit from this service. I think the optionality is correct.

C- We had a discussion about “is activated” meaning “I want to use it”. If you don’t want to use it, don’t activate it. This is not a capability bit.

C- I argued that there was an array of bits for whether this mechanism is used. The bits should be set based on what the device is going to do.

C- It’s more dynamic than you understand. It’s based on lots of things. You might be unwilling to send out the Device ID based on what happens leading up to the decision. We shouldn’t mandate that a STA provide something it doesn’t want to provide. There are conditions where the variable can mean the device intended to send it the Device ID, but then changed its mind.

C- I’m so confused. I thought Device ID was the identifier, but then it seems to be a bit indicating support.

C- We could argue that the Device ID is empty, as discussed yesterday.

C- This should be in the Association Request/Response.

C- Careful. This is in the context of FILS only. The dot11FILSActivated is true here.

Q- Why does the Association Response have the Device ID?

A- FILS piggybacks off the Association Response, which is the equivalent of message 3 in the 4-way handshake.

C- We are in danger of going around in circles. We do not have a presentation saying things like “first time association using FILS, first time association without FILS, here’s what happens.” Then we need to know what happens subsequently. I understand what was said today, but yesterday, we seemed to argue against the kind of optionality discussed now. I’d like to see it in black and white.

C- That’s what Kurt Lumbatis presented in [1218](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx).

C- We are mashing together multiple things. When this element (dot11DeviceIDActivated) is present and the IDs are being exchanged, this still doesn’t mandate that the IDs be used. Using the IDs is a different decision from exchanging the IDs. We shouldn’t mandate usage during the element exchange.

C- These things were put in the [11-22/1218r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) document and optionally presented as we discussed the other day. For the first time a STA comes in and is looking for the AP to assign an ID, this doesn’t need to be there. And in the Association Response frame, if the STA has sent an ID and it’s recognized, the AP doesn’t have to send one back unless it’s assigning a new identifier. The [11-22/1218r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) document tried to lay that out. There was a strong opinion that the AP should always send the Device ID.

C- I see this MIB variable being highly dynamic. The setting of the value should be done after the decision making is done. The Device ID should be present if the value is true. If you don’t have one yet, you can’t send one, but that would just be another condition in addition to the MIB variable values.

C- This MIB variable is used for two different things over the air. I do not think Clause 9 should describe behavior. It should discuss frame format. If the group is happy for the MIB variable to change in the middle of an interchange, we can do that. Then the optionality could be dropped.

C- We need to come to agreement on how we see the information flow happening before we ask authors to write text to that agreement.

C- I think a different MIB variable is needed for STAs and APs.

C- I agree with the need to reach an agreement first. One way to do is the capability bit is dynamic. But I like the idea of asking for the Device ID from the AP explicitly. We shot that down way too early.

C- Let’s keep the discussion at a conceptual level rather than giving details about information is exchanged.

C- The [1218](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) document had a truth table to do just that. I can try to have a presentation for tomorrow with a logic table. I’ll try to remain conceptual.

C- We should also look in the baseline text and see if there are gaps and differences or not.

Jouni Malinen (Qualcomm) asked for **consensus to adopt the comment resolutions** in [11-22/1078r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx).

Q- Our bigger discussion on “how things work” could change these resolutions. Is there objection to agreeing that the resolutions are ready for motion?

A- [None noted.]

Q- In my understanding of FILS, you have a certificate that allows you to know who is doing the authentication. How does that work with Device ID?

A- FILS can do EAP with certificates or it can do public-private key pairs. I think Device ID makes a lot of sense for FILS.

C- My understanding of the way FILS works is a session sort of thing that starts with a normal authentication. Upon return to the network, then the STA can do the optimized FILS process. But that ages out and then the STA has to start over, although Device ID could be used for further authentication. The initial authentication to start FILS might look like the normal non-FILS cases.

C- For the authentication server (AS), ESS, etc., we try to avoid the term network. The AS can be operated by a different entity than the AP in an ESS. We are targeting the AP here. We might want to have a short discussion to make sure everyone understands the difference. But I believe the FILS backend is out of scope for this task group. The only reason we talk about FILS here is because of the difference in the STA-AP communications that re-arranges the traditional 4-way handshake conveyance. Otherwise, it’s fairly similar. There are corner cases and modes, but they shouldn’t affect us.

C- I may be getting fast BSS transition mixed in my head with FILS.

C- We talked a lot about what’s in the draft, using the handshake, embedding the device ID. There’s lots of discussion about pre-association use cases. Is there anything that talks about how that meshes with the draft? Things like pre-association recognition?

C- To keep the group out of the circular mud, let’s talk about what we want to accomplish. Currently in the draft, we have a network-generated ID that can be used while associating and associated. We have discussed STA-generated ID. And we have discussed an early in time ID that could be used. And we’ve talked about probes pre-association. We have a lot of pieces. The group needs to decide what to pursue before we talk about how they interrelate. Until we know what needs to interact, we shouldn’t discuss how they do so.

C- I was suggesting that the discussion would bridge the different points.

C- Every time we start to talk about things working together, we end up with someone saying, “I don’t want that thing to work together with the other things.”

C- Months ago, I did a presentation on how you can have multiple schemes. They nicely co-exist. You could send the Device ID and the MAAD ID in separate elements without selection or interaction. I was worried that the group would be worried about having multiple schemes, so I showed in several presentations that multiple schemes didn’t interfere with each other.

Graham Smith (SR Technologies) briefed [11-22/1584r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-00-00bh-more-than-one-scheme.pptx) about “**TG bh: More than one scheme**”. We can look at each scheme in depth and argue over who wants it and who doesn’t. Or we can look at the privacy side. This is an attempt to put TGbh to bed before we have votes on things. The proposed schemes include Device ID, MAAD, IRM, and RRCM, each with its own merits. These have been shown to coexist without a selection process. And some of these schemes beyond Device ID have shown a majority support, even if not reaching the threshold for incorporation into the draft. Given that there are use cases that Device ID does not cover, why do we want to restrict solutions that cover them? None of these schemes are mandatory.

C- There are whole businesses that based on tracking on devices/users. If security wasn’t an issue, this would be easy.

Q- The answer is, “What security?” The schemes proposed address the tracking and don’t have security issues. This is a philosophical argument.

A- The group needs to discuss what problems we would like to solve and then discuss if we have solutions for them. We will immediately rathole back into technical arguments. Let’s say we understand your point without diving back into it.

C- I disagree respectfully that the security issues have been addressed. Turning off the device is the only secure thing. So, there’s a continuum of security. Anything with a Device ID has a security risk.

C- Having lots of schemes requires a lot of implementation and validation, so it’s not trivial. And who gets the benefits of doing these schemes? The pre-association cases don’t seem so beneficial. I don’t want to see a Device ID mandatory to associate to a network. The security and privacy aspects are super important, but we shouldn’t force devices to reveal their identity. What’s the benefit to the STA to revealing its identity?

C- I agree that we can define multiple schemes and the protocol work. Covering all the use cases without losing privacy is good. But there are security issues with some of the proposals here. Without technical proposals that meet the PAR requirements for privacy and security, I can’t support some of these schemes. Some of the proposals have extreme requirements on the AP. It might be possible for the authors to fix their schemes, but some schemes bog down with lots of STAs. Yes, we should cover the use cases with suitable proposals, but we shouldn’t add every single proposal. We don’t need to define things that aren’t going to be used either. I believe we have a motion to address so-called pre-association use cases. I think we can cover some of them, maybe based off of Device ID.

C- I thought we had a clear idea of the discussion when Graham presented it, but now we are talking about security and privacy. Graham was talking about high-level ideas. I’d like to ask at the high-level if there’s a need for something. Not everything is a smartphone. There are IoT devices. We should maintain a conversation about the need before getting into the technical details.

Smith then moved on to [11-22/1230r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1230-00-00bh-background-use-cases-par-privacy-etc.pptx) (“**TG bh: Background, Use Cases, PAR, Privacy etc.**”), which addresses some of the above comments. This material was previously presented, but many participants do not seem to be aware of it. He points out the pre-association proposals can meet all the use cases, not just pre-association ones. The presentation gives a history of some of the reasons that RCM came into being. He noted that he had a separate presentation on how to prevent a STA from probing for or associating with a spoofed AP. Smith argues that the pre-association schemes do not have a unique privacy problem. Returning to [11-22/1584r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-00-00bh-more-than-one-scheme.pptx), he once again that MAAD, IRM, and RRCM could also co-exist using separate KDEs (key data encapsulations). Each scheme can have its own subclause. The market and the application can decide which schemes should be implemented and used. This would also allow TGbh to finish up by not blocking everything.

C- I agree that some use cases and schemes can co-exist. But there are privacy issues in some of the proposals. Claiming one-time use of a value isn’t accurate. Things like MAC addresses. Like between two failed connection attempts. There are trackable issues with re-used MAC addresses. All that said, for some of the use cases, I do believe it can be done, perhaps with a time-based hash value. I don’t think the current proposals are likely to get 75% support for incorporation.

C- With RCM, the address doesn’t change every time, so I agree that the schemes shouldn’t have to do so either. IRM allowed frequent changes, but the AP had to do a lot of work. I ended up with simple schemes because they seemed to suffice.

C- If the group has generally agreement that some of these cases are interesting, but that any solutions do not cause privacy problems, then we might have a way forward to work on the schemes. Let’s think about that.

**Meeting recessed at 10:00 a.m. HST.**

**Meeting September 15, 2022, 8:00 to 10:00 a.m. HST**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

The meeting called back to order at 8:02 a.m. HST.

Policies and procedures displayed. No IPR assurances noted.

The agenda is now [11-22/1282r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1282-05-00bh-agenda-tgbh-2022-sept-interim.pptx).

1. **Motion to create Draft 1.0**

There was a discussion on whether a motion should be raised to instruct the editor to create a Draft 1.0 for submission to a WG letter ballot.

C- This motion is premature. We haven’t made important decisions, like whether STA-generated IDs will be allowed. And we are lagging behind on our espoused position to move quickly and fix things that industry has pointed out as being broken by RCM. We aren’t supposed to be increasing privacy in this group – that’s TGbi.

C- If we have a ballot motion, it would have to follow motions #11 and #12, cutting off any other input. It seems surprising to hold a ballot motion right now.

C- Agreed, that’s the only spot that makes sense.

C- My suggestion is that we go with the agenda as given. When we get to the end of that, we can consider whether it makes sense to hold a ballot motion. The contribution on “more than one scheme” will inform that, as will the diagrams that Kurt Lumbatis generated overnight. We should take Lumbatis’ presentation first, then Smith’s. Then we consider the motion, although we could start with straw polls first to see if we should consider further pursuit of those proposals or just finish off the draft as we have it and go to ballot.

Assuming we are not going to a WG letter ballot out of this meeting, the TG chair is requesting 4 slots during the November plenary. Teleconferences will be held weekly on Tuesdays, starting 27 September 2022 at 9:30 a.m. ET. Teleconferences will not be held on 4 October and 1 November.

The comment collection document is now [11-22/0973r10](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-10-00bh-cc41-comments-against-d0-2.xlsx).

1. **Motions**

Motion #11 was offered:

Move to approve the resolutions to the CIDs listed below, per resolutions recorded in [11-22/0973r10](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-10-00bh-cc41-comments-against-d0-2.xlsx):

* CIDs 21, 22, 23, 34, 54

and incorporate the text changes into the latest TGbh draft.

Moved by Peter Yee, seconded by Kurt Lumbatis. The motion was approved by unanimous consent.

Motion #12 was offered:

Move to approve the resolutions to the CIDs listed below, per resolutions recorded in [11-22/0973r10](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-10-00bh-cc41-comments-against-d0-2.xlsx) (per [11-22/1078r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx)):

* CIDs 50, 51, 52
  + Note: CID 50 is only partially covered, as it is 2 different issues.

and incorporate the text changes into the latest TGbh draft.

The motion was amended to remove CID 50 and the associated note because of potential confusion as to what part of CID 50 was covered. CID 50 will be dealt with separately. The amended motion reads:

Move to approve the resolutions to the CIDs listed below, per resolutions recorded in [11-22/0973r10](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-10-00bh-cc41-comments-against-d0-2.xlsx) (per [11-22/1078r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx)):

* CIDs 51, 52

and incorporate the text changes into the latest TGbh draft.

Moved by Sidharth Thakur, seconded by Jouni Malinen. The motion was passed by unanimous consent.

A motion to approve requirements 38, 39, 40, 41, 44, 45, 46, 48, 49, 50, 51, and 52 (basically, all requirements that passed by unanimous consent in straw polls) in [11-22/1848r13](https://mentor.ieee.org/802.11/dcn/21/11-21-1848-13-00bi-requirements-document.docx) was itself approved by unanimous consent.

1. **Contributions**

Kurt Lumbatis presented [11-22/1625r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1625-00-00bh-non-ap-sta-device-id-implementation.pptx) on “**Non-AP STA Device ID Implementation**”. There’s been a lot of discussion about how the higher layers interact with Device ID activation and usage. There are 3 options:

1. non-AP STA Always Indicates Device ID Activated (dot11DeviceIDEnabled = 1)
2. non-AP STA Indicates Device ID Activated per SSID
3. non-AP STA Never Indicates Device ID Activated

To be clear, Lumbatis expects the group to choose one of these options for implementation. This is not a set of options that a device implements and then picks from on an operational basis.

C- I don’t think these options cover all the scenarios we have discussed. The STA may not want to send the Device ID to a specific AP in an ESS. Do you want to add another option to cover this scenario.

C- Options #1 and #2 are very simple. The AP looks at the indication and whether it received a Device ID to determine whether to send a Device ID.

C- I think these options should be simplified and the fourth option added. The key thing is this is a choice by user input or upper layer software that makes a selection to employ Device ID. I don’t think it’s just a function of the non-AP STA indication. There are myriad ways to toggle things. But those things are secondary to the 1-bit mechanism that indicates whether to use the facility. You can discuss option #3, but I think we don’t need to go there.

Q- Why is it so important that the non-AP STA indicate with a bit whether it wants to be identified. I agree that you will have some way of the STA knowing it wants to use Device ID with a particular AP. You signal to the network if the STA wants a Device ID.

A- You need to signal to the STA from above that you want a Device ID.

C- But that’s internal to the STA.

Q- Are you saying that nothing changes over the air?

A- No. But the phrase “the STA indicates it wants to be tracked” is unneeded. If you supply a Device ID you do.

C- I don’t think the option #2 text says that.

C- The comment was could we operate without any indication. I don’t think we need to have the non-AP STA indicate it supports this capability, so it doesn’t get something unexpected in the KDE. There has to be a protocol change.

C- I’m in support of the feature, but not the activated bit saying, “I want to be tracked on this network”.

C- I don’t want to spend time wordsmithing this presentation. There are 3 options that are very clear. Option 1 is the STA always shows support for the option. Option 2 is a toggle. Option 3 is to never indicate usage through a bit. The question is how the STA tells the AP when it wants a new identifier. How the non-AP STA makes up its mind is common to all options. I like option 3. It’s clear and the AP doesn’t have to keep an eye out for this one bit.

C- Whether the decision is per BSS or ESS is something that can be treated as a separate discussion.

C- I can’t quite agree. Let’s duplicate option 2 to option 4 and then modify.

C- Instead of that, why don’t we just clean up the wording to indicate that the decision could be per BSS or ESS for all options. Then we don’t have to duplicate all three options.

C- That resets my thinking and I’m okay with that.

C- I like option 3. It’s cleaner. How to code that with the MIB is more straightforward. The indication is just adding the Device ID or not. That addition should be optional.

C- We have been polishing this brick for a while. Let’s just run the vote with these three options. We are worrying about things that are outside of our standard. I don’t think we should have to care about those things. Unless someone has a huge, overwhelming concern, let’s take the vote.

Q- In option 3, how would the AP behave if the non-AP STA provides an unknown Device ID.

A- That’s found in the matching text for this presentation. The AP can decide to use it (maybe it is stale) or it can issue a new one.

Q- Doesn’t that apply to all 3 options?

A- Yes.

C- Then it’s orthogonal to this presentation.

1. **Straw poll**

A straw poll will be held asking for support of each of the options.

Q- There’s a suggestion for Chicago-style voting. Is that acceptable?

A- Yes, that’s fine.

C- The poll will be with the understanding that per BSS vs. per ESS is an orthogonal issue and applies to all options. If that’s true, then we can run the poll.

The straw poll in the presentation reads:

I support the following Option to control Device ID

Option1 – non-AP STA always indicates Device ID is active and controls at the higher layers whether to store and utilize the ID

Option 2 – non-AP indicates Device ID is active on a per SSID basis

Option 3 – Non-AP STA never indicates Device ID is active and utilizes the passing of an identifier to indicate support.

The voting was taken against the terms option 1, option 2, and option 3 alone.

The vote was: Option 1: 5; Option 2: 17; Option 3: 14.

C- Does this mean we allow for both 2 and 3, or do we just pick the single option with the most votes.

C- I only want one option. Either 2 or 3 is fine. We could run a straw poll, although I don’t know that we will get any better answers.

C- Somehow the protocol machine has to be told what to do. Whether that’s a MIB variable, MLME interface, something external, that’s not too relevant.

Q- In the case “I don’t want to do anything”, do I signal “I’m privacy enabled station, but I don’t want to do it”?

C- If we have this bit set somewhere, it’s probably a bit that’s being used elsewhere as a reserved bit. It has to be somewhere in this message. We reserve a bit. By default, it’s zero. There probably isn’t any difference over-the-air whether we use the bit. I don’t think we give away any privacy information about the device whether the bit is asserted. I’m scared about debating whether we can do this without giving away information.

C- The bit is already there. It’s not a new bit.

Q- You mean in our current draft?

A- Yes. It’s not a new bit. It’s the bit in the draft. We are just talking about how to use that bit. In option 3, the STA doesn’t need it, but the AP does. The question we are asking with these options is whether the bit is in the non-AP STA. I would suggest we have a straw poll between options 2 and 3.

C- In 2, the non-AP STA uses the RSNXE capability bit. In 3, the NULL Device ID field is used. That’s my interpretation of the difference. Can we just run the straw poll?

C- It’s been pointed out that having the bit present helps the AP to know what’s coming.

A second poll between options 2 and 3 resulted in a vote of: Option 2: 19 and Option 3: 9.

Q- Could Kurt and Jouni create a diagram showing where the bit goes?

A- It’s in my diagram.

C- [It’s the in RSNXE as described in our current draft.]

C- Work will continue during teleconferences.

**The meeting was adjourned at 9:57 a.m. HST.**