Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, August 30, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-8-30 |
| 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 30, 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 30, 2022 9:30 a.m. to 11:30 a.m. ET**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

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

Agenda slide deck [11-22/1397r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1397-00-00bh-agenda-tgbh-2022-aug-30.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)
* **Motions:** [**11-22/0651r03**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-03-00bh-tgbh-motions-list.pptx) **(motions #9 and #10, on slides 16-17)**
* **Results of Comment Collection on D0.2:** [**11-22/0973r08**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-08-00bh-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
	+ [*11-22/1069r01*](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) – reviewed Aug 23, bring back updates*
	+ [11-22/1078r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1078-00-00bh-device-id-indication.docx) – Device ID indication (Jouni Malinen)
	+ [11-22/1218r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-03-00bh-device-id-synchronizatoin-and-control.pptx) – Device ID synchronization and control (Kurt Lumbatis)
	+ [11-22/1329r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-01-00bh-cid-resolutoins-for-12-2-11.docx) – CID resolutions for 12.2.11 (Kurt Lumbatis)
	+ Walk-through CIDs
* **Contributions (slide 16)**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Motions**

Motion #9 was shown (as found on slide 16 in [11-22/0651r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-03-00bh-tgbh-motions-list.pptx)). It reads:

Move to approve the resolutions to the CIDs listed below, per resolutions recorded in 11-22/0973r8:

* CIDs 1, 3, 13, 14, 55, 59, 60

and incorporate the text changes into the latest TGbh draft.

C- I have a presentation covering 3 and 55, but he can build on the motion-approved text.

C- Please make sure that that submission has a unified update to the text because they might otherwise be incorporated in the wrong order.

C- My submission is a rewrite of 12.2.11. I’m not sure how that works.

C- Your submission will be considered as a way forward from the approved text.

Kurt Lumbatis moved the motion. Jay Yang seconded it.

The motion was **approved by unanimous consent**.

Motion #10 was shown (as found on slide 17 in [11-22/0651r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-03-00bh-tgbh-motions-list.pptx)). It reads:

* 802.11bh shall provide a mechanism for the infrastructure to identify a previously known non-AP STA that is using a randomized MAC address, when that STA transmits Public Action frames, Authentication/Association Request frames and post-association Probe Request frames.
* Note: the mechanism shall not decrease users’ privacy.

Q- What changes with the passage of this motion? Is it just a statement of intent?

A- It’s just a statement of intent

Q- Where is it recorded? The minutes only?

A- Yes, the minutes only.

Q- Does this motion bind the group? Is it the equivalent of a straw poll?

A- We are trying to settle on what the group can commit to doing so that people with contributions know what to work on.

Q- How do we interpret the results? Is it a technical motion requiring 75%?

A- I’ve struggled with that, but I believe this should be technical. Treating the motion as technical will see if there’s enough support to make generating text worthwhile.

C- I agree with that interpretation.

Q- If this is approved, does that mean we delay going to ballot with the draft?

A- It sets an agreement within the group that we are not done until we deal with this topic. That way, we agree whether a contribution is within in scope. I don’t see that that would stop any particular draft from going to ballot, because a ballot doesn’t have to imply that the document is fully fleshed out. TBDs can be found in balloted documents. Mostly, this is trying to steer our discussion.

Q- If this motion fails, will we amend the PAR? And if it passes, will we amend the PAR?

A- Do we think what’s stated in the motion is in the PAR? PAR amendments can be brought forward at any time.

C- I believe this motion is an attempt to clarify what we believe the PAR is stating and what’s in scope for this group. I think we are trying to mitigate returning to an AP for identification after an initial association. The other thing is that an unassociated STA can be identified to the network to guide it where it needs to go or to troubleshoot the network without compromising the privacy of the individual wishing to use RCM. Suggestions to turn off RCM for the latter would seem to go against the PAR. I think the unassociated case is a critical case. It came from WFA, WBA, and members internally. This motion highlights that we need to address this case and I speak in support of the motion.

Q- I want to know what happens if the motion fails, what we can do. Does failure mean that we cannot address this scenario?

A- That’s a good question, but I don’t have an answer for that. I’m trying to capture the group’s feelings on this topic. Someone could bring a separate motion that says we aren’t covering this.

C- Btw, I’m in favor of this motion.

Kurt Lumbatis moved the motion. Joe Levy seconded.

Q- The text talks about post-association Probe Request frames, but it also talks about other frames. Do we need to be clear about pre-association activity, post-association activity, and activity upon association? I believe the text needs to be clearer in that regard. I don’t think we have sufficient clarity in the motion text at this point.

A- I think those questions would be answered as part of the submissions made in response to the passing of this motion. I don’t think we need to put the answer in the motion. I have a problem with post-association Probe Request frames.

C- This is meant as a general direction for the group to show its agreement so that submission writers know what to work on.

Q- Maybe add the word “optional” before “mechanism”? Would that make people more comfortable?

A- My reading of the words is to provide a mechanism, but that it would be optional to use.

C- We could say that this was for upon-association and post-association activity, but not pre-association.

C- That would be modifying the list of behaviors in the motion. Let’s look at optionality first.

Q- I think changing “shall” to “may” might help. But does that mean shall means the mechanism is mandatory.

A- I think this means text will be added to the document, but usage is optional.

C- I think this motion is clear as stated. We put in specific frames that are part of non-associated transformation of information. All are pre-association frames with respect to the AP to which they are transmitted. This were some frames that were addressed by some of the previous contributions. It’s not a complete list. There’s a need for an identity capability for these frames that was lost with RCM.

C- I’m against making the mechanism optional. It goes back to why this group exists. If we are not solving the problem, we should disband. The problem being identifying STAs pre-association. Authentication requires identification. It’s pointless to assign a new identity. If we don’t deal with pre-association, it’s pointless to have this group.

C- You are opposed to optional for the mechanism or changing “shall” to “may”?

A- I’m opposed to the changing the “shall”. The optionality of the mechanism is okay.

Q- Mover, are you willing to accept insertion of “optional” as a friendly amendment?

A- I’m opposed.

Q- Seconder?

A- I too am opposed. I think it just confuses things. Those are decisions to be made to be later.

C- I don’t understand how this motion binds us, but I support this effort. If we all we do is identify STAs after they have authenticated, then we should disband. Authentication already implies identification. If our entire work is to allow a single password for an ESS deployment scenario, we shouldn’t bother. I thought the group existed to solve this problem. I speak in favor of the motion.

C- I speak in opposition. I don’t see what this motion achieves. I would rather vote for a specific mechanism than a general direction.

C- I agree with the previous speaker. We do have work that we are doing with proposal already in flight, that have comments that we are trying to resolve. If this motion fails, do we have to disband? Probably not. To get hung up on pre-association activity seems to be a drastic overreach in terms of privacy.

C- There are a lot of use cases for pre-association/not-association caused by RCM. If someone says they don’t want to address this issue, then I agree with a previous speaker about disbanding this group. A lot of devices don’t have an association. Then how is it identified. If we say we don’t address these use cases, why do we have this group at all?

C- We aren’t doing anything to allow a user to be identified. We are allowing the network to identify a device across Probe Requests and other pre-association mechanisms over the air. The devices just use a non-identifying MAC address to be used for troubleshooting, steering, and other things that were lost with RCM. This is to allow the network operators to do what they were doing before. I don’t see this as privacy endangering if done properly.

C- I don’t agree with that statement. It’s one-way identification. There’s no way for the STA to know what network is identifying it pre-association. Without the STA knowing that, I think these mechanisms are dangerous. As for networks being hurt by using RCM, well, networks are still operating. Some use cases may have become harder, but that was the intent of using RCM. Let’s not go back and backtrack and lose 10 years of progress made with RCM.

C- I think there’s a fundamental misunderstanding of what the proposal is. There’s no way for a network to identify a STA if there was no prior association. This motion deals with STAs that have had an association, then gone away, and then returned with a different MAC address. The network would like to recognize the STA because there was a previous association. Meaning that the STA and the AP trusted each other previously. Let’s continue to build on that previous relationship. This proposal does not cover STAs that have never associated with networks they haven’t authenticated or associated to previously.

C- In a pre-association state, the STA cannot identify the network to know that the AP is a genuine AP that it previously knew. So, it might release some identifier that could be captured when it doesn’t want to.

C- IEEE 802.11bi has already to carrying the SAE identifier in the authentication frame. Why is that okay there but not here. I am requesting a recorded vote.

C- This motion is for a previously known non-AP STA to an infrastructure.

C- All non-unanimous motion results are to be recorded in the minutes. When we made the change to allow teleconferences to have motions, the requirement was for the group to approve having a motion on a call, with 10 days’ notice. And the results are to be explicitly recorded in the minutes. Straw polls are not recorded. But motions are to track if there’s stacking of the room.

C- That’s news to me and perhaps other [task] groups.

Validated motion results: 11/7/3 (Y/N/A) – motion fails due to a lack of 75% approval.

Individual votes:

 Y N A

 -------------------------------------------------

 [V] Peter Yee, NSA-CSD | X | | |

 Dan Harkins | X | | |

 [V] Dorothy Stanley HP Enterprise | X | | |

 [V] Amelia Andersdotter, Comcast | | X | |

 [V] Stephane Baron Canon | X | | |

 [V] Patrice NEZOU, Canon | X | | |

 [V] Mark RISON Samsung | | | X |

 [V] Jay Yang[Nokia] | X | | |

 [V] Bo Sun, ZTE | | X | |

 [V] Liuming Lu OPPO | X | | |

 [V] Kurt Lumbatis ,ARRIS/CommScope | X | | |

 [V] Carol Ansley Cox | | | X |

 [V] Robert Stacey, Intel | | X | |

 [V] Po-Kai Huang Intel | | X | |

 Harvey Sam | | | |

 Yong Liu | | X | |

 Jarkko Kneckt | | X | |

 SK Yong | | X | |

 [V] Okan Mutgan Nokia | X | | |

 [V] Max Riegel - Nokia | X | | |

 [V] Carl Kain USDOT; Noblis | | | X |

 Joseph Levy [InterDigital] | X | | |

C- The group will have to interpret what the failure means.

Q- How do we deal with CIDs that pertain to pre-association use cases? How are they to be addressed?

A- I’m not sure what to tell you other than to take into account some of the comments made during the discussion. Some people seem willing to accept a presentation in this direction if the privacy is maintained. At least that’s what I think heard. We’ll have to see the response to submissions.

C- If we are still debating this issue, I don’t know how to proceed.

C- I will do my best to keep us discussing in-scope topics but remember that we are contribution driven. I’m open to further discussion and straw polls. So far, we keep getting mixed responses.

Q- Without a direction, it’s hard to move forward. There are no further comments in the reflector, so how are we to proceed?

C- Another way we can handle comments [on pre-association] is to reject them because we couldn’t agree to address them.

C- We can also reject comments and we can focus on the existing draft.

C- If you want to reject those CIDs, then we need ¾ support.

C- The rejection reason is important. If you can’t write such a reason, then you can say there was no consensus. That phrasing reflects that state of the task group.

C- I’d like to caution people around “no consensus”. It’s used in the very last stages of balloting after thorough balloting and attempt to reach consensus. We aren’t there yet. There’s been a comment collection. You don’t have to resolve all those comments. Maybe your Draft 1.0 doesn’t pass. Maybe it will. Keep discussing comments, but don’t feel that you must resolve them all. You do have to resolve them for a letter ballot.

C- This motion didn’t pass with a 75% majority, but it did get a majority. So, while there’s no technical consensus, people shouldn’t read into this that there’s no support for the motion. We are at an impasse because of the 75% requirement, but what we have here is a minority stopping a majority from going in that direction. It’s the majority’s responsibility to convince the minority to change its position.

C- In order to be able to make progress, we must have agreement in the group about what we do with these topics. The majority felt this was important. They are responsible for working offline to convince the minority otherwise. We can’t spend our calls arguing these points to no avail. Circular discussions are not making progress.

1. **Resolution of a Few Comments**

Dan Harkins (HPE) spoke about [11-22/1069r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1069-02-00bh-resolution-of-a-few-comments.docx), the revision of last week’s presentation. For CID 21 (foil traffic analysis), he proposes to replace “foil” with “mitigate”. For CID 22, remove “For an 8 octet tweak that would be 25 octets.” as the simplest solution. No change to CID 23’s resolution. CID 34’s resolution is unchanged. CID 54’s resolution is now to point at [11-22/1082r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1082-04-00bh-cr-for-device-id-generated-by-network.docx)’s resolution of CID 3. There were no objections to this plan.

C- These resolutions will be prepared for a motion during the September mixed-mode session.

1. **Device ID Synchronization and Control**

Kurt Lumbatis talked about [11-22/1218r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-03-00bh-device-id-synchronizatoin-and-control.pptx), an update on “Device ID Synchronization and Control” based on comments from the previous briefing of this presentation. Now, in subclause 9.4.2.241, the Device ID Support bit is indicative of both implementation and activation of the device ID feature.

Q- Does this apply to both AP and non-AP STAs?

A- Yes.

Q- Why say implemented? You can’t activate what isn’t implemented.

A- I can remove implemented.

Q- You are looking for input which will inform a specific proposal with text?

A- That’s correct.

C- I see a comment that “bit” should be changed to “field” or “subfield”.

C- I’ll check on what we use.

C- You’ve talked about the AP advertising support in Beacons. It’s not clear to me that the non-AP STA will get that prior to sending an Association Request. And one item on slide 7 is based on the non-AP STA having knowledge based on that.

C- The confusion is that text on slide 7 deals with FILS.

C- I withdraw the comment.

C- Combine slide 7 “FT” and “other exchanges”. And change “FILS Device” to “FILS”.

A- Agreed. I’ll do that.

Lumbatis explained what the combinations of Device ID support values and ID Blob contents mean to the AP and the STA.

C- For slide 11, I’d suggest that the AP switch out the identifier for a new one.

C- That’s the third and fourth point on the slide.

Q- That’s an “or” between points three and four?

A- No. The AP can assign a new ID at any time.

C- The trust tables work for a legitimate STA, but there might be attacks on the Device ID.

C- I can only see an attack if using FILS. Once it gets into the 4-way handshake, the STA has to have key material the AP recognizes.

C- There are several attacks like trying to manipulate the network. A STA could use a random ID in a flooding attack. The first time a STA comes with an empty ID bloc and Device ID Active set to 1. This would cause the AP to take an action, perhaps to assign a Device ID. For many years, the identifier was the MAC address. There are solutions based on implementations for MAC spoofing or flooding. In IEEE 802.11bh, we are changing that direction. We are now using an ID to identify the STA. So, there will be similar attacks. I’m not saying your scheme doesn’t work, but we need to consider these attacks again. Not ID stealing, but flooding.

C- The attacking device must have network credentials in order to mount an attack. For FILS, it must have previously joined the network. For non-FILS, it must have a credential to pass message 1 in the 4-way handshake. So, I think it’s better than just a MAC address identifier. I don’t know how we deal with a flooding attack on an AP. A bad actor can mount one.

C- An attacker can manipulate a network now. If you think a station is an attacker, then there are security concerns that are not addressed in this presentation. This is something to think about.

C- Once we have an actual proposal, we can consider those concerns.

C- Do we want to look at my proposal now? There are only 15 minutes, which isn’t sufficient. I’d like people to look at it first.

Q- Has the proposal been updated to match the updated truth table?

A- Yes, but not for the discussion today.

Q- Am I allowed to provide the editor with a complete rewrite of the text?

A- Yes, it’s allowed.

C- The text pulls in all the other changes that were approved.

C- Maybe you can reference those changes in the document.

C- They are there, but don’t do anything until we have a discussion.

C- It would be helpful to add a sentence referencing where the changes have come from to aid the editor in understanding the relationship between documents.

C- Please read through [11-22/1329r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-01-00bh-cid-resolutoins-for-12-2-11.docx) and submit editing changes. It brings in the logic from the presentation and spells it out. Let’s not hash out the language here.

C- We need more formalism if this is actual specification language. We need to be clear if the numbered lists are composable options or mutually exclusive options. I need to take to read this offline first. Offline feedback would be helpful.

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

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 8/30 | Amelia Andersdotter | Comcast |
| TGbh | 8/30 | Ansley, Carol | Cox |
| TGbh | 8/30 | Baron, Stephane | Canon |
| TGbh | 8/30 | Derham, Thomas | Broadcom |
| TGbh | 8/30 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 8/30 | Harkins, Dan | HPE |
| TGbh | 8/30 | Henry, Jerome | Cisco |
| TGbh | 8/30 | Huang, Po-Kai | Intel |
| TGbh | 8/30 | Kain, Carl | USDOT, Noblis |
| TGbh | 8/30 | Kneckt, Jarkko | Apple |
| TGbh | 8/30 | Levy, Joseph | InterDigital |
| TGbh | 8/30 | Liu, Yong | Apple |
| TGbh | 8/30 | Lu, Liuming | OPPO |
| TGbh | 8/30 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 8/30 | Montemurro, Mike | Huawei |
| TGbh | 8/30 | Mutgan, Okan | Nokia |
| TGbh | 8/30 | Nezou, Patrice | Canon |
| TGbh | 8/30 | Petrick, Al | InterDigital |
| TGbh | 8/30 | Riegel, Max | Noka |
| TGbh | 8/30 | Rison, Mark | Samsung |
| TGbh | 8/30 | Sam, Harvey | Broadcom Corporation |
| TGbh | 8/30 | Smith, Graham | SRT Wireless |
| TGbh | 8/30 | Stacey, Robert | Intel |
| TGbh | 8/30 | Stanley, Dorothy | HPE |
| TGbh | 8/30 | Sun, Bo | ZTE |
| TGbh | 8/30 | Thakur, Sidharth | Apple |
| TGbh | 8/30 | Yang, Jay | Nokia |
| TGbh | 8/30 | Yee, Peter | NSA-CSD |
| TGbh | 8/30 | Yong, Su Khiong | Apple |