Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Teleconference Minutes, October 31, 2023  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2023-10-31 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA, US |  | [peter@akayla.com](mailto:peter@akayla.com) |

Abstract

This document contains the minutes of the IEEE 802.11bh teleconference of October 31, 2023.

Note: Highlighted text are action items.

**Meeting October 31st, 2023, 9:30 a.m. to 11:30 a.m. EDT**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox Communications)**

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

The agenda slide deck is [11-23/1850r01](https://mentor.ieee.org/802.11/dcn/23/11-23-1850-01-00bh-agenda-tgbh-2023-oct-31.pptx). The agenda was updated with additional comment resolution presentations, as show in [11-23/1850r02](https://mentor.ieee.org/802.11/dcn/23/11-23-1850-02-00bh-agenda-tgbh-2023-oct-31.pptx).

1. **Policies and procedures were presented by Chair Mark Hamilton. (Slides 4 to 15)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
  + Timeline reminder (slide 16)
  + Motions record: [11-22/0651r26](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-26-00bh-tgbh-motions-list.pptx)
* **MOTION:** 
  + Approve comment resolutions through Oct 24: Motion #22 in [11-22/0651r26](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-26-00bh-tgbh-motions-list.pptx)
* **Comment Resolution**
  + Comment resolution document: [11-23/1152r24](https://mentor.ieee.org/802.11/dcn/23/11-23-1152-24-00bh-ieee-802-11bh-lb274-comments.xlsx)
  + Comment resolution queue (slide 17)
* **Discussion on response to WBA liaisons (was due Sept):** [**11-21/0703r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx)**,** [**11-21/1141r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-1141-00-00bh-excerpts-of-wba-document-wi-fi-id-scope.pptx)**,** [**11-22/0668r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0668-00-0000-liaison-statement-from-wba-re-wi-fi-devices-identification-group.pdf)**,** [**11-22/0653r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0653-00-0000-2022-march-wba-whitepaper-re-device-identification.pdf)
  + [11-23/0888r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0888-00-00bh-wba-liaison-discussion.pptx) Stephen Orr

The agenda, with comment resolution submission updates acknowledged, was approved with unanimous consent.

1. **Timeline Review**

Hopefully, we will be able to wrap up comment resolution in time for a recirculation ballot by November, if not earlier. We still appear to be on track, but only one teleconference remains between now that the November meeting.

1. **Motion**

Motion #22 found in [11-22/0651r26](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-26-00bh-tgbh-motions-list.pptx) was shown. It reads:

Approve the resolutions to CIDs listed below, per the resolutions recorded in 11-23/1152r24 marked “Ready for motion”, and incorporate the text changes into the latest TGbh draft:

- CIDs: 30, 48, 90, 120, 143, 163, 258, 290, 291, 20, 89, 76, 130, 261, 262, 247, 13, 236, 237, 238, 176, 180, 255, 226, 24, 177, 253, 248, 1, 83, 145, 174, 246, 75, 123, 249, 106, 105, 121, 91, 92, 172, 166, 251, 178, 171, 34, 241, 109, 128, 137, 148, 160, 164, 156, 240, 196, 198, 208, 214, 19, 88, 40, 170, 104, 103, 244, 72, 65, 214, 129, 192, 200, 201, 203, 260, 266, 12.

The motion was made by Graham Smith (SR Technologies) and seconded by Jay Yang (ZTE). The motion was approved with unanimous consent.

1. **Topic**

Graham Smith continued from the last meeting with some final comment resolutions in [11-23/1373r05](https://mentor.ieee.org/802.11/dcn/23/11-23-1373-05-00bh-cid-resolutions-irm-2.docx). His first resolution pertains to comment ID (CID) 107 (see [11-23/1152r24](https://mentor.ieee.org/802.11/dcn/23/11-23-1152-24-00bh-ieee-802-11bh-lb274-comments.xlsx)), which claims there are misordered sentences in subclause 12.2.11.2. The resolution is aligned with a similar device ID resolution but applied to IRM instead. There’s one part of the text that the group will need to select one of two possible sentences covering the dependence of the mechanism on the configuration and advertisements of all of the APs in the ESS. Both sentences could actually be used as one covers configuration, the other activation. The dependency of the IRM mechanism on all APs in the ESS being configured would be better worded to say that the correction operation of the IRM mechanism is the dependency. Smith will make this change and will propose a similar change to the resolution for (the just motioned and approved) CID 103. Some additional rewording was made to clarify the resolution for CID 107, which the group found agreeable.

For CID 195, the group has already spent quite a bit of time refining the wording, but there are still two possible resolutions. The second resolution drops a requirement on APs storing the IRM as the non-AP STA’s identifier. The group prefers the longer version, with a clarification that the non-AP STA is storing this IRM identifier for itself.

Smith will post a revision to his resolution reflecting the discussions.

1. **More topic**

Jay Yang picked up with [11-23/1353r04](https://mentor.ieee.org/802.11/dcn/23/11-23-1353-04-00bh-cr-for-cids-relevant-to-device-id-part-2.docx) at CID 97. His resolution adds “the Device ID is encrypted” to the text and seems agreeable to the group. CIDs 42, 99, 124, 125, and 126 all deal with unclear notation (“aa”, “bb”, etc.) and the wording around it dealing with “in the clear”. Yang’s resolution would eliminate the notation in the text and the related Figure 12-0a (for CIDs 127, 187, 188, 265, and 281). Several additional changes to the notation were requested by the group and will be incorporated into the next version of Yang’s resolutions.

Yang then went on to CID 146, which is resolved with a missing close parenthesis. CID 181, which asks for clarification on the use of “MAC1”, “MAC2”, etc. is resolved with revised text that makes it clear what the antecedents of those terms are rather than assuming implicit connection between entities and MAC addresses. CID 182 is accepted outright. CID 183 asks for changes to “first PASN frame with device ID active”, but Yang’s resolution seems to place a MIB attribute in the frame. Instead, the setting to TRUE of the related bit in the RSNXE should be used. CID 184 also deals with the slightly obtuse “aa” type notation and clarification of the encrypted transmission of the device ID. The group lightly revised Yang’s proposed resolution. Time ran out to address the remaining CIDs in the document.

1. **LB274 CID Resolutions for PASN**

Okan Mutgan (Nokia) offered [11-23/1726r01](https://mentor.ieee.org/802.11/dcn/23/11-23-1726-01-00bh-lb274-cid-resolutions-for-pasn.docx) on “LB274 CID Resolutions for PASN”. It covers CIDs 84, 85, and 87. The first CID asks for details on the encryption of the IRM element in PASN frame 3 and the device ID element in PASN frame 2. Mutgan offers updates to subclauses 12.7.1.3 (taking into consideration IEEE 802.11az-2022’s pairwise key hierarchy) and 12.13.7 to fix that. He also adds a new subclause 12.2.11.3 on encryption of Device ID and IRM IE in PASN. There was a suggestion to instead adapt the FILS KDE mechanism for PASN in this context rather generating a new encryption scheme, especially as the key in question is short-lived, only used during authentication to encrypt the Device ID IE or IRM IE.

CID 85 is resolved by noting that “The Device ID element shall be encrypted with the chosen cipher suite.” This is the commenter’s accepted resolution.

CID 87 similarly clarifies that the IRM element is encrypted (in the third PASN frame) with the “chosen cipher suite” instead of the fixed use of AES-128-CMAC. That needs to be clarified further that the chosen cipher suite is the one specified in the first PASN frame. Mutgan will bring back a revised resolution.

**Meeting adjourned at 11:31 a.m. EDT**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 10/31 | Ansley, Carol | Cox Communications |
| TGbh | 10/31 | Cain, Carl | USDOT, Noblis |
| TGbh | 10/31 | De la Oliva, Antonio | InterDigital |
| TGbh | 10/31 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 10/31 | Huang, Qisheng | ZTE |
| TGbh | 10/31 | Kneckt, Jarkko | Apple |
| TGbh | 10/31 | Levy, Joseph | InterDigital |
| TGbh | 10/31 | Li, Yan | ZTE |
| TGbh | 10/31 | Luo, Hui | Infineon |
| TGbh | 10/31 | Magrin, Davide | Meta |
| TGbh | 10/31 | Montemurro, Mike | Huawei |
| TGbh | 10/31 | Mutgan, Okan | Nokia |
| TGbh | 10/31 | Orr, Stephen | Cisco |
| TGbh | 10/31 | Patwardhan, Gaurav | HPE |
| TGbh | 10/31 | Rosdahl, Jon | Qualcomm |
| TGbh | 10/31 | Sam, Harvey | Broadcom Corporation |
| TGbh | 10/31 | Smith, Graham | SR Technologies |
| TGbh | 10/31 | Wang, Zisheng | ZTE |
| TGbh | 10/31 | Yang, Jay | Nokia |
| TGbh | 10/31 | Yee, Peter | NSA-CSD |
|  |  |  |  |