Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Plenary Meeting Minutes, July 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-07 |
| 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 July Plenary meeting, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting July 11, 2022 8:00 to 10:00 a.m. ET**

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

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

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

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

**Editor: Carol Ansley (Cox)**

**An ad hoc session was called to order by the Chair at 8:03 hrs. EDT**

Agenda slide deck 11-22/1010r00

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 (ad hoc session):**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ July Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 13:30-15:30
	+ Timeline review: Can we complete comment collection and agree on D1.0 during July session?
* 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: [11-22/0973r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-00-00bh-cc41-comments-against-d0-2.xlsx); plan for resolutions
	+ Organize contributions into groupings/against comments (if/where possible)
	+ Other comment groupings?
	+ Volunteers to prepare resolutions?
	+ Review editorial comments
* Contributions (slide 16)

Any comments, any objections to agenda, Agenda accepted.

1. **Results of Comment Collection on D0.2**

The group reviewed the results ([11-22/0973r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-00-00bh-cc41-comments-against-d0-2.xlsx)) of the comment collection held on Draft 0.2. There were 65 comments received during the comment collection and they are only available in spreadsheet form, there being insufficient comments to justify entering them into the comment management database. Time was spent considering the comments by topic so that they could be assigned to volunteers.

Jay Yang (Nokia) volunteered for the pre-association/unassociated and STA ID comments, along with several others.

Sid Thakur (Apple) volunteered to handle the definition of opt-in (CID 2). Kurt Lumbatis (ARRIS/CommScope) will work with Sid as Kurt has a related presentation. Thakur will look at the other CIDs that are grouped as “opt-in”.

Dan Harkins (HPE) volunteered to resolve the comments in section Z.

Carol Ansley (Cox Communications, TG technical editor) will review the editorial comments for disposition.

Graham Smith (SR Technology) will work with Yang on the MLME comments (CIDs 16 and 17). Efforts in the ARC SC will likely inform the resolution of these two comments because ARC is revising the existing MLME text in the base specification, perhaps for inclusion in IEEE 802.11me. It was suggested that CID 17 could be solved with a MIB variable rather than an MLME primitive. On the basis that both comments might be resolved via the MIB, both CIDs 16 and 17 were re-assigned to Mark Hamilton.

C- In regards to CID 8, verification failure might need to be signaled by a reason code if the AP is strict in rejecting unverified associations as opposed to accepting them without verification. Mixed mode APs would allow unverified associations for STAs that haven’t opted into the scheme.

Yang and Jouni Malinen (Qualcomm) will discuss the matter offline.

CID 9 is assigned to Yang as the offered resolution was for the commenter (Yang) to do so.

CID 10 questions what happens or should happen if a STA uses an old device ID.

C- it should be allowed as long as the ESS doesn’t mind.

Yang will resolve the CID.

C- A stolen ID should be subject to a rejection reason.

C- The opaque blob is encrypted over the air (in the 4-way handshake), and thus not to subject to “theft”. In any case, the validity of the blob is outside of the scope of the standard.

CID 11 is assigned to Yang.

C- The device identifier should be updated per association, effectively not allowing reuse of an old one. This is because the device ID may be exposed in the clear after assignment depending on its later usage (possibly as a MAC address or in some other scheme). The comment should be rejected.

Harkins is willing to accept the re-assignment of the comment to himself and will discuss it with Yang.

CID 12 notes that Device ID is a term within IEEE 802.1AR and suggests that a different term in IEEE 802.11bh.

C- I am supportive of such a change and has already given it some thought.

The comment is assigned to the commenter, Antonio de la Oliva (InterDigital).

CID 13 asks whether there isn’t some confusion over FILS (Fast Initial Link Setup) and FT (Fast Transition) cases.

C- I caution that there are constraints between the cases and I request that the comment be rejected.

De la Oliva agreed to withdraw the comment and will send an email to the chair/reflector to make that happen.

In CID 14, the question is what should be done if a Device ID is not recognized.

C- I agree that the use of the Device ID should be better delineated, although a change in the term “Device ID” could be part of the way to make that happen. This will be added to the “ID verification” discussion.

Q- If the ID is used at the application layer, then why is it generated at the IEEE 802.11 layer?

De la Oliva will start the discussion amongst interested parties.

The “pre/un-assoc” CIDs are assigned to Yang.

C- CID 25 is marked like an editorial change – asking for description and unification of terms like “identifier”, “opaque identifier”, “blob”, “ID”, etc.

C- This discussion is contingent on the renaming of Device ID.

The comment is assigned to de la Oliva.

CID 26 is assigned to Yang.

CID 31 asks for clarification of subclause 12.2.11 about how the transition from having no ID to having an ID occurs.

C- This is an upper layer matter.

C- This comment to be related to opting in.

C- I’m not sure that’s really the case.

C- The commenter may be confused.

Thakur volunteered to address the comment because he has a related contribution.

C- It doesn’t feel like it’s worth addressing, but I’m happy to see the language reviewed.

C- The submitter of CID 32 agrees to its withdrawal, as it is similar to CID 13.

De la Oliva will write up a rejection reason as it is obvious that multiple task group members find the text confusing.

C- CID 33 is similar to CID 50.

These are opt-in related comments and will be assigned to Sid Thakur. CID 49 is also assigned to Thakur.

C- Perhaps we can use a MIB variable as a means of achieving the “may” language.

Hamilton is willing to work out the MIB bits once Thakur and the group have decided on the language covering optionality.

Harkins will look at adding a reference to Annex Z to resolve CID 34.

CID 35 is assigned to de la Oliva as it is related to CID 25.

C- Annex Z goes to a lot of trouble to foil traffic analysis, with the assumption that the identifier will be used outside of the 4-way handshake. Thus, the comment relates back to CID 11. But if no one cares about opaque identifiers, then Annex Z is unneeded.

CID 35 is re-assigned to Harkins.

CID 50 appears to cover multiple topics including the meaning of identifier.

C- The meaning can be huge if we start getting into the application side of things. And whether “opt-in” or “may” is the right way to describe STA behavior is an open question.

C- User consent needs to be reflected and “may” not be appropriate to such consent.

C- The meaning of identifier needs careful consideration.

The new/old identifier portion of the comments is assigned to Malinen. Thakur will cover the rest of it.

Malinen will address CID 51 about FT operations and frame naming.

CID 52 is assigned to Malinen.

CID 53’s opaque identifier part is assigned to Harkins. The remainder about identifier naming goes to Malinen.

CID 54 is assigned to Harkins.

Hamilton will look into CID 55.

CID 58 goes to de la Oliva as another naming comment.

CID 59 goes to Hamilton to check the unclear language.

CIDs 60 and 61 are assigned to Yang as they are related to other comments he is to deal with.

Hamilton will handle the missing PICS in CID 62.

CID 63 is assigned to Thakur, while CIDs 64 and 65 are in Yang’s bailiwick.

**The ad hoc session was adjourned at 10:00 EDT.**

**Meeting July 12, 2022 13:30 to 15:30 ET**

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

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

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

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

**Editor: Carol Ansley (Cox)**

**The meeting was called to order by the Chair at 15:33 hrs. EDT**

Agenda slide deck in 11-22/0844r02

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda (ad hoc session):**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ July Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 13:30-15:30
	+ Timeline review: Can we complete comment collection and agree on D1.0 during July session?
* 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: [11-22/0973r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-00-00bh-cc41-comments-against-d0-2.xlsx); plan for resolutions
	+ Organize contributions into groupings/against comments (if/where possible)
	+ Other comment groupings?
	+ Volunteers to prepare resolutions?
	+ Review editorial comments
* Contributions (slide 16)

Any comments, any objections to agenda, Agenda accepted.

1. **Approve Minutes**
	1. May Interim session: [11-22/0773r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0773-00-00bh-minutes-tgbh-interim-meeting-may-2022.docx)
	2. Teleconference minutes:
		1. May 24: [11-22/0822r01](https://mentor.ieee.org/802.11/dcn/22/11-22-0822-01-00bh-802-11bh-telecon-minutes-may-24-2022.docx)
		2. Jun 14: [11-22/0903r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0903-00-00bh-802-11bh-telecon-minutes-june-14-2022.docx)
		3. Jun 21: [11-22/0924r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0924-00-00bh-802-11bh-telecon-minutes-june-21-2022.docx)
		4. Jun 28: [11-22/1060r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1060-00-00bh-802-11bh-telecon-minutes-june-28-2022.docx)

Moved: Lei Wang

Seconded: Alan Berkema

Result: Unanimous Consent

1. **Motion to appoint a secretary**

Peter Yee was appointed task group secretary. Moved by Joseph Levy, seconded by Lei Wang, with unanimous consent.

1. **Timeline (**Slide 18)

PAR approved Feb 2021

First TG meeting Mar 2021

D0.2 CC May 2022

Initial Letter Ballot (D1.0) Jul 2022

Recirculation LB (D2.0) Sep 2022

Initial SA Ballot (D3.0) Jan 2023

Final 802.11 WG approval May 2023

802 EC approval Jul 2023

RevCom and SASB approval Jul/Aug/Sep?’23

The timeline was reviewed. The target is to have a Draft 1.0 coming out of this week in order to have a timely response to the market pressures for an RCM solution.

Any discussion? None

1. **Issues Tracking**

The issues tracking document remains as [11-22/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx), which was last updated in June.

1. **Contributions**

Graham Smith presented [11-22/0955r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0955-00-00bh-pre-association-and-probes-in-tgbh.pptx) on pre-association and probes in TGbh. There are three schemes: Device ID, MAAD, and IRM. There’s also RRCM that is used to derive multiple addresses used for probes and association, which MAAD and IRM are also capable of doing. There are broadcast probes (wholly random addresses are fine here) and active directed probes (which could use an address that is then used in association but never used again). The question is whether there’s a need for more than one address. For use case 4.1 (pre-association client steering), there doesn’t seem to be a need for multiple addresses. For use case 4.2 (during association/parental controls), likewise, there don’t need to be multiple addresses as the use case occurs during association and therefore a single address is all that’s needed. For use case 4.8 (infrastructure), there’s no apparent benefit to multiple address. Finally, for use case 26 (virtual BSSID), which is another “STA in the vicinity of a network of interest”, given that the network is driving the address generation, it’s not apparent that more than one address is needed. ANQP could use multiple addresses (one for determining what services are available from the AP, another for associating), but it’s not clear that multiple addresses are needed.

C- In general, this seems optimistic that there are no active attackers that are trying to track a STA. Also, addresses don’t change until a successful completion of the 4-way handshake. An active attacker in multiple locations could spoof the local BSSID and track the STA. Only when a connection to a bona fide network is made is the STA’s address updated.

C- I disagree with your assertion that a STA would only be dependent on a single SSID and therefore that SSID could be duplicated all over the place for the purposes of tracking.

Q- You list broadcast and directed probes. The broadcast case uses a wildcard SSID, right?

A- Yes, that’s correct.

Q- Is A1 a unicast address used as the destination of the directed probe?

A- [Not certain.]

C- In MAAD and IRMA, the 4-way handshake needs to be completed for the STA to update its random MAC address. When a STA roams (via FT) between APs, there’s no 4-way handshake, so it can’t update its MAC address.

C- We’ve already discussed that we don’t change addresses in FT (re-association) usage.

C- Devices are trackable in a particular area (the area of a network).

C- You mention that MAAD and IRMA can handle multiple MAC addresses. If you carry multiple addresses, you need an extra 6 octets per address. A third party can use the size of the frame to determine how many addresses were being sent.

C- I don’t see the point of having more than one, so even if you stretch it to two addresses, it’s still more efficient than transmitting a 16-octet seed value.

Q- I don’t disagree with your conclusion, but I don’t understand how being in the vicinity of network affects actual operations. If the STA knows it’s in the vicinity of the network, what’s the logic the STA implements to determine what type of address to use?

A- The determination of vicinity is likely from hearing beacons. Assuming these work with non-random MAC addresses, then for identifiable MAC addresses, the STA can decide which address it wants to use.

Q- Why would you use a passive method to determine the vicinity followed by an active probe.

A- I wouldn’t do that and don’t know why anyone would. This is really about ensuring that association works for identifiable addresses. I don’t think combined passive listening and active probing makes sense.

C- If we can detect the STA during the association and the AP rejects the association, we can’t steer that STA as part of that rejection. I’d like to see the association occur, followed by steering.

C- I agree, but I need to think how that affects recognizable addressing.

Q- I think the pre-association use cases have not been thought through. What happens when an association fails?

A- Our PAR doesn’t say we have to solve every use case.

Q- What happens when the AP changes its MAC address?

A- It doesn’t. STA should be understood to mean non-AP STA in the context of this presentation.

Q- On the STA, is the MAC address stored per BSSID or SSID? If I have two APs that are broadcasting the same SSID, each would have a different address for the STA that had been assigned?

A- STAs remember things per SSID – this isn’t changing. The use of random addresses isn’t changing operations.

Q- But if I have two APs that advertise the same SSID but do not intercommunicate, how does moving between them work? Does the second AP issue a new randomized MAC address? And then moving back to the first AP, the STA can’t use that address successfully.

A- That’s correct. You are just not recognized. I would hope that a common SSID implied that the overlying application (for access control purposes) could talk to all its APs and ensure coordination.

A- An access control system that is based on denying known MAC addresses is too weak to make it work in the face of randomized addresses. This was previously discussed on a call.

Q- There have been discussion by operators that with RCM, they are losing the ability to troubleshoot their networks when there are problems with a user getting onto the network. Using an identifiable MAC address when the association is failing, the operator can track the device and figure out what’s going wrong. The focus of this group is to try to reinstate some of the things that were lost due to RCM. We need some pre-association capability to address those use cases. Others disagree and it’s not in our baseline. I agree with the possibility of active attackers that put up a false network to mount a successful attack, but I think that’s a corner case and not worth addressing. I would like to see IEEE 802.11bi address those sorts of things. IEEE 802.11bh should address simple, focused solutions.

C- Regarding the pre-association client steering use case, there are two mechanisms. In one, APs learn which STAs can associate to 5 GHz networks by watching the STAs probe requests on the 5 GHz band, and they try to steer them to 5 GHz networks instead of letting them associate on the 2.4 GHz band. Regarding our supporting every possible use case that was out there before RCM, I disagree with that. Fix the ones that can be safely done, but don’t chase every use case. I don’t agree with solving pre-association client steering. No STA should be sending a non-random probe. The diagnostic case is interesting. I don’t know if the STA could be made to keep a fixed address for diagnostic purposes.

C- There is another IRM version out there that might apply.

C- The probe request is tricky. It’s also used for more than discovering an AP. The concept for allocation of multiple, random MAC addresses for a STA comes from these multiple uses.

C- The user has to accept the risk of being identified by a network.

C- This isn’t forced on anybody. The network can advertise what it supports (as determined by the upper layer application).

C- Perhaps you don’t randomize your MAC address on every probe. If you do it every 20 seconds, that might be enough time for an AP to do band steering without a great loss of privacy. There’s also text in IEEE 802.11 that says you shouldn’t do directed probes.

C- I don’t want us to keep revisiting use cases that we have agreed not to address. Some of those use cases aren’t likely to get sufficient support to be added to the draft, so let’s work on those things where there is enough support.

C- We had two buckets of comments that came in during the comment collection. One was pre-association; the other was STA-generated identifiers. Think about what we want to address.

C- We discussed dealing with pre-association steering and there was a successful straw poll about that.

Q- We need to consider whether we address pre-association issues and to what extent? Does it suffice to say which address should be used for pre-association? The answer to handling pre-association probably depends on how it is used. We probably don’t want to solve every possible pre-association scenario. How do we reach closure on the scope?

A- We ran various motions and ended up with network-generated identifier in the baseline. The STA can choose not to use the network-generated identifier. We haven’t come to an agreement on how to handle other schemes and use cases. Why don’t we just work with the existing specification text rather than having circular discussions?

A- We are proceeding with the existing specification text, and we sent that out for comment collection. And that resulted in a significant number of comments that requested support for pre-association use cases. So, we sort of have to figure out how to resolve those comments. If we can set them all aside, we are back to the existing specification text, but we aren’t there yet.

C- We agreed to deal with pre-association, so I hope we can go forward that way.

C- In the set of motions, MAAD got strong support, although many didn’t understand it. Straw polls since show strong support for pre-association. These proposals aren’t made for fun, but from a sincere desire to solve these problems as much as we can. The issues tracking document is at revision 37 and still isn’t done. When do we finish things up?

C- I agree (with a previous speaker) that we need to get the existing draft moving forward. Other ideas should be presentations of specification text that is subjected to a straight up-or-down vote for incorporation. We need to move quickly and we may not fix all the corner cases. If we keep trying to polish for too long, others will come up with proprietary solutions and IEEE 802.11’s won’t be picked up.

C- We would be okay with focusing on the post-association use cases, but we are also interested in getting a STA-generated identifier in there as well. There’s also user consent. After that, we’re done with IEEE 802.11bh.

C- Let’s think about the pre-association and STA-generated concepts overnight and then see what we can do to resolve the related comments. If we decide support one or both of those, we do have proposed text already, so it’s not too hard to augment the existing specification text. The proponents of those schemes should be ready to defend the text to save time.

**Meeting recessed at 15:31 EDT.**

**Meeting July 13, 2022 8:00 to 10:00 EDT**

**Chair: Mark Hamilton**

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

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

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

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 8:03 hrs. EDT**

Agenda slide deck 11-22/0844r03

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda:**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ July Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 13:30-15:30
* 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: [11-22/0973r1](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-01-00bh-cc41-comments-against-d0-2.xlsx)
	+ Comment resolutions
* Contributions (slide 22)
* Way forward to D1.0 (slide 23)

The Chair reviewed the agenda.

The proposed agenda was adopted without objection approved by unanimous consent.

1. **Straw polls**

Straw polls were held to gauge the next steps.

1. **The first straw poll covered whether non-AP STA generated IDs should be added to the amendment.**

C- I’m in favor of this option. A lot of work has been done in this area, so it wouldn’t be hard to add text quickly.

C- I’m against this option. The use cases indicate that there isn’t much call for it. Look at captive portal issues, where it’s a slight pain to reenter credentials. All of these types of use cases derive from network requirements, so the network owns the name space and should come up with the identity. Although the STA could generate the identity, I don’t think it would solve any of the problems with the use cases and it might cause problems if there are STA-generated collisions.

C- I would like to speak in favor. It’s important from the standpoint that the STA can identity itself using a mechanism that it can define. It won’t change much to RCM. A lot does change with opt-in verbiage and opt-in’s definition. If it is opting in, a STA should be free to choose its identifier.

C- I would speak in favor of STA-generated IDs. There are certain systems that employ user-supplied IDs.

C- Regardless of who owns the namespace in general, I would like to see the STA control its identifier. It already controls its MAC address. A simple AP at home case would work well with STA-generated IDs. A STA-generated ID works well in enterprise situations with multiple but poorly coordinated APs where the STA can successfully push its ID to all of the APs.

C- I don’t object to STA-generated IDs. The only problem we have previously discussed is poorly generated IDs. I think the straw poll should be slightly reworded to work around that.

C- I speak against this proposal. STA’s having their own MAC addresses doesn’t apply to the identifiers we are talking about. These are network services and a network-generated ID makes the most sense.

C- STAs don’t provide their own MAC addresses. They are purchased/obtained from IEEE to ensure that there are no conflicts at the block level. The reason RCMs work without collisions is the low probability of a collision in 46 bits. If we allow STAs to come up with whatever name they want, the name would have to have significance to the network without collisions. The assumption that there are no poor implementations that generate collisions seems untenable.

C- The only point of the ID is to allow a STA to identify a network when it returns to that network. Not allowing the network to generate the ID seems to be anti-network control. And the STA can always choose an RCM when it joins a network. This is about the identification of a STA to a network that it has previously associated with. As for the “Starbucks use case”, the APs in these places don’t share identifiers and create a database they all update. Therefore, the identifier really should be under network control.

C- I’m not sure what use cases utterly require STA-generated IDs, but I won’t vote against it either. The identifier should be random (as RCMs are) and could be larger (like a random UUID) to help work against collisions. I would be against using “[user’s first name] laptop” as an identifier. We would need to define some rules for the STA-generated IDs.

C- I don’t think we need to get into the type of identifier yet, but it should be deterministic. It should definitely not be another MAC address, which would defeat the point of RCM. It should come from a name/number space large enough to defeat collisions.

C- I support the comments from the network-generated ID side. With the lack of knowledge of the use cases that we want to support, it’s not so meaningful to have this discussion here. The IETF MADINAS WG is looking at this problem too. They are looking at a broad range of use cases. MADINAS will liaise with other organizations such as WBA, WFA, and now here too. It would be useful to share thoughts between MADINAS and IEEE 802.11bh. MADINAS will look at a broader solution space owing to its position in the network stack. We could highlight gaps, including ones that are not solved in the IETF, like passing RADIUS messages that weren’t there before. It would be good for both groups to take a broader view instead of just focusing on the Layer 2 identities. A system view is important. I wouldn’t support making a decision until we have that broader discussion.

C- I dislike stopping people and devices from doing what they want to do. Both sides have sensible arguments. I don’t see why you can’t have both STA-generated and network-generated identifiers. The AP advertises what it will accept. If it doesn’t want STA-generated identifiers, it can simply not advertise their support. And vice versa. Why not satisfy both sides? The network has the final word because it chooses what it will accept.

C- In principle, I don’t like having two solutions to the same thing, but I also want to see what we develop here actually get deployed. I see a trust issue where each side doesn’t trust the other side to generate the IDs in a way that preserves anonymity. There are lots of ways for two peers to input entropy into the generation of an identifier. But if we make the argument that we can’t trust the peer’s implementation, we have a problem. I’m in the middle ground. We should pursue what’s behind the use cases and determine if that really results in two methods. Regardless, we shouldn’t make assumptions about how networks are deployed and managed, and whether they have centralized or decentralized management.

C- I think IEEE is a very open group. Both APs and STAs should be allowed control if there are use cases that benefit from that.

**The choices were 1) this feature is important, 2) this feature is acceptable, and 3) this feature should not be pursued. The result of this straw poll was: 10/13/6.**

1. **The next straw asked whether pre-association/not associated use cases should be covered. The choices are 1) this feature is important, 2) this feature is acceptable, and 3) this feature should not be pursued.**

C- I think this straw poll covers a combination of use cases we have previously discussed. I’m against some of the use cases but not others. I would probably vote the middle one, but for certain use cases, I would vote the last choice.

C- In a previous meeting, there was a straw poll that showed almost 90% for the pre-association use case. I don’t think we need a second straw poll on this topic. Looking at the issues tracking document, there are several use cases that are in scope of 11bh. If we don’t cover them, then 11bh won’t finish its job.

C- This is one of the cases where it’s a little dangerous. Pre-association use cases are prone to eavesdropping. There are pretty severe privacy issues there as well. I don’t think we can find a good solution unless we can deal with those issues.

C- We have pre-association use cases. To say ‘no’ to this means we think that some use cases are a waste of time and won’t be addressed. Then perhaps we are fighting WBA’s and IETF’s views. I’ve tried to show that these use cases aren’t prone to drastic eavesdropping. I wouldn’t put forward a solution I thought was weak. We can find solutions that are very safe and secure. You are wild dreaming things, like 100 APs scattered around some area all pretending to be my home. If I used a random MAC trying to associate to my home AP, you can assume it’s a member of my family. I think this is an important feature. If a network doesn’t want to support it, that’s a choice the network can make. We should be flexible and provide solutions for different places. Why stop networks from doing what they want do properly? Many networks will be happy with network-generated ID. Others won’t. Why stop them? Not every device has to support everything, although a STA might want to support multiple solutions if it doesn’t know what networks it wants to use. Let networks decide what they want to support.

C- I don’t think this use case needs to be solved. For the vast majority of the use cases, they are legacy use cases and we have better solutions for them. Maybe diagnostics is covered, but there are better ways to handle that and 11bh shouldn’t cover it. Regarding the security aspects of it, if we come up with a secure method that addresses more than the post-association methods, maybe that would be acceptable. And active attack by cloning an SSID where you expect a victim to be doesn’t seem like a difficult attack to mount. This isn’t the mainstay of the use cases be solved here, but it’s possible. I’m not in support of general solutions to pre-association use cases, but might support it for some edge cases.

C- I agree. I don’t think there was a good solution discussed previously. We wouldn’t allow 5 GHz devices to connect to a 2.4 GHz paired network. Lots of devices are scanning on both bands and will find both networks. APs already communicate whether they are congested. The STA might be blocked from using the most optimal radio, so network steering based on an AP decision isn’t always the best. We might also be harming the coexistence of other network resources by blindly steering. Wi-Fi 7/IEEE 802.11be devices using MLD may be having multi-band connections anyhow.

C- We have some pre-association use cases, but here we are talking about MAC randomization. We aren’t trying to deal with client steering. We’re trying to fix things that MAC randomization messes up. If the issues tracking document doesn’t cover every pre-association use case. If we don’t address them now, future implementations will suffer.

C- I don’t think this needs to be solved. We have been discussing pre-association use cases for a while without generating progress. If TGbh was formed to allow networks to provide services to clients and they trust the network to do so, then I don’t think we need to address these use cases.

C- Pre-association use cases are already implemented. That’s why 11bh should address them. If you don’t see the benefit, you don’t have to support them, but you shouldn’t stop them either. Use cases 4.1 and 4.26 are examples. Why would you want to stop VBSS use cases, for example, that have been in use for 20 years?

**The vote was 8/10/11.**

C- Hopefully this gives some background to the on-going discussions and comment resolution.

Q- Any objections to having the opt-in discussion now?

A- If you want to have a good basis for that discussion, we could have a straw poll as well, as in Kurt Lumbatis’ presentation.

1. **Contributions**

**STA ID opt-in 11-22/1084r00 presented by Sid Thakur**

Several comments from the comment collection are about the STA’s ability to opt-in to being uniquely identified by a network. There are regulatory and technical reason why opt-in might be necessary. The end user should always provide consent, and this should be an opt-in by default, not an opt-out by default. The STA should not be tracked unless it opts into this. The current draft doesn’t cover consent for opt-in. A MIB Boolean variable (perhaps *dot11UserConsent*) could indicate this consent. The current draft uses a network-generated ID, but the user has no way to signal willingness to be tracked. This means the AP will provide a Device ID, even if not desired by the STA. The AP wastes memory and computation doing so if the STA is not planning to use the network-generated ID. Opt-in would allow the AP to not waste its resources. The STA should be able to signal its willingness for tracking. Normally, a STA’s user only knows about a network’s tracking policy after association and authentication. A separate signal can let the AP know that the STA would like the network to clear/delete all information for this STA. Signaling can be performed during association, reassociation, and deauthentication/disassociation. Post-association opt-in can use a Robust Management Action frame to indicate the STA’s willingness for tracking. Opt-out can signaled likewise. The identifier sent in message 2 of the 4-way handshake can be encrypted. All other signals can be protected using RSN. Data clearing can also be signaled separately from opt-in/opt-out.

Q- I think you misspoke when you said that the opt-in should be the default. You meant the opt-out should be the default, right?

A- Yes.

C- This proposal seems unnecessary. If the STA doesn’t want to use the network identity, it can just throw it away. This whole thing about clear bits and telling the network to delete all data it has seems officious.

C- I think there’s some value to providing user consent via the MIB. As far as the over-the-air parts, I’m not convinced it’s needed. I think it can lead to fingerprinting. Freeing up AP resources seems technically all right but not all that useful. I think it is easier to receive the network-generated blob and decide whether to use it at that point without making the over-the-air protocol more complex. I think the profile deletion request (not mandate) might be helpful for regulatory purposes. This is a useful discussion, but mostly I support the MIB variable and the request to drop stored user information.

C- This is a very complete set of cases on how to control/not control the use of the identifier. There’s very little need to have this level of network control of these processes. We’re really talking about a MAC-level identification, not some higher-level privacy-meaningful ID. And the STA can always throw out the network-generated ID and there’s nothing stopping it from doing that. I can see the clear data bit being useful, but there’s not much to be deleted unless you are associating the ID with something at a higher level and that’s not happening at Layer 2. I don’t think we need to be this dogmatic and careful. This proposal is rather unnecessary other than being polite to the AP.

Q- What’s the point of this scheme?

A- It allows opt-in and opt-out at any point in time rather than requiring a device to disassociate and re-associate to escape its network ID.

C- I agree with general direction of the presentation. If a STA wants to be de-identified from an AP that makes sense, but I think the opt-in language generates unnecessary controversy. If you introduce extra bits, you might be allowing more bits for fingerprinting of devices. I’m not aware of any regulatory concerns about tracking of a random identifier. I don’t think this proposal will help network operators be compliant with regulatory burdens incumbent on them. It will require some higher layer solutions and lawyers. The STA no longer using the network-generated ID would be the optimal solution.

A- As an example, a hotel chain might be able to correlate multiple IDs for a single STA over different hotel properties. This proposal allows the STA to signal its unwillingness for that to happen.

C- We have to remind ourselves that we are constrained to the MAC/PHY levels. The delete all data bit is restricted to that level and is therefore uninteresting. I would challenge any statement that the GDPR applies here. But that’s the short pole in the tent on information that the network can gather on you, like what websites you visit and for how long. Setting a clear data bit at Layer 2 won’t affect any of that. Anything we can mandate clearing in IEEE 802.11 is going to be minimal and meaningless.

C- This proposal simplifies setting and forgetting identifiers, which saves on associating/deassociating as a means for managing identifiers. If we always generate these identifiers, we will have zombie identifiers on the AP as it waits for the STA to return. Having a control to clean up those zombie identifiers is a nice feature.

C- I think this proposal is way over the top. We are trying to keep things simple. The first time you associate, you indicate a desire for an identifier. Now, I’m going to reconfirm that choice? Why do you have to be nice to the AP and indicate that you don’t want the identifier? This is more complicated. I’m not convinced that we have to a hard opt-in/opt-out and the ability to switch between those choices. If you don’t want to be identified further, just don’t use the identifier going forward.

A- Support vs. consent need to be explicitly separate states. When we talked about parental control and troubleshooting, you need to be able to turn the feature on and off. I need to be able to disable the identifier without having to disconnect/reconnect to the network.

C- Why do you need to communicate this? This is belts, braces, and parachutes. It’s too much.

C- I kind agree with the opt-in. Otherwise, we don’t advertise support for the network-generated ID. But perhaps instead of a clear data bit, a TTL on the network-identifier would be helpful.

C- I think we should allow a STA to indicate when it wants to be identified and when it does not. As a STA, we need to control what’s done with the identification data.

**Opt-in verbiage 11-22/0832r02 by Kurt Lumbatis**

This presentation doesn’t cover implementation, just verbiage. Do we want to use the term “opt-in” or something else? A checkbox is a typical interface element for indicating opting in or out. IEEE 802.11-2020 doesn’t have any discussion of the optionality of tracking. IEEE 802.11be does allude to allowing the user or a higher-layer function to have control of certain such functions at Layer 2. A set of MIB items is needed to for signaling opt-in/opt-out.

C- It occurs to me that originally, we had MAC addresses, which meant you were recognized. There was no concept of opting in or out. The idea is that an application wants to do something with the MAC address. If you want to opt out, just use a different MAC address. If you want to opt in, keep using the same MAC address. I’m a STA that decided to use a network. The only tickbox needed is whether I keep using a particular MAC address. I’m a little worried that we are going too far.

C- I think that defining ways to opt in or out are helpful and we can probably define a Layer 2 solution, but it’s not enough. We have to consider how the upper layers deal with the opting in or out too.

C- We can only work on Layer 2 issues. This presentation isn’t about implementation, it’s only about verbiage. Not whether it is a good idea.

C- We aren’t defining any interface to an interface. We need to provide a means for the upper layers to drive the lower layer behavior. The words don’t matter. I think it’s a good thing that opt-in/opt-out don’t appear in IEEE 802.11. IEEE 802.11aq introduced MAC randomization with an interface for that. That’s the model we should follow. A MIB variable obviates the need to worry about the particular words used in IEEE 802.11.

A- One of the comments said that MAC addresses were always there and we were okay to be identified then. That’s oversimplifying it. MAC addresses were not intended for tracking and were overused for that purpose. This is a moving landscape. Information is being collected on a user (and even sold, with or without user consent). If it were that simple, we wouldn’t have this presentation. I think we need to have this mechanism.

C- I agree that IEEE 802.11 is always using a MIB variable or bit somewhere for opting-in or out. There’s no need to debate the verbiage and complicate things. There are lots of such MIB variables.

**The meeting was recessed at 10:01 EDT**

**Meeting July 13, 2022 13:30 to 15:30 EDT**

**Chair: Mark Hamilton**

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

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

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

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 13:36 EDT**

Agenda slide deck 11-22/0844r04

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda:**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ Next meetings plan
	+ Timeline update review
* 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: [11-22/0973r1](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-01-00bh-cc41-comments-against-d0-2.xlsx)
	+ Comment resolutions
* Contributions (slide 22)
* Way forward to D1.0 (slide 23)
* Respond to Liaison from WBA: [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)
* Next steps

The Chair reviewed the agenda.

The proposed agenda was adopted without objection approved by unanimous consent.

1. **Next meetings pan**

For the upcoming interim session, 4 meeting slots are planned. Conflicts to avoid include TGbi, REVme, ARC, TGbe, and maybe TGbc.

Q- Are 4 slots enough? We have a lot work to do and 4 slots might not have enough time for comment resolution and discussions.

A- 6 slots might be hard to get, but I’ll check. We should also be doing more to prepare ahead of time such as by email as well.

Teleconferences are suggested for Tuesdays at 10 a.m. ET for 2 hours. The discussion settled on 9:30 a.m. ET on every Tuesday.

1. **Timeline update**

The task group will not be ready for a letter ballot coming out of this week’s session. The timeline will be adjusted to push everything off by one session.

1. **Motion**

Graham Smith offered a motion reading “In order to meet the PAR, the TGbh Amendment shall include a scheme or schemes that address the pre-association Use Cases identified in Document 21/332r27 as being ‘in-scope’.” The motion is offered to put the matter to bed. Kurt Lumbatis seconded the motion, which will be a recorded vote.

Q- I can’t tell what use cases are covered. Just 4.1? 4.10? Please identify the exact set of use cases that this motion would force us to address in the amendment.

Q- I also find the scope of this motion unclear. Could we get a presentation (perhaps from Kurt Lumbatis) on this motion to clarify things and then run the motion?

C- This motion seems to have been offered to get feedback now. To defer it, we would have to table it. I suggest it only covers use case 4.1 and would like to amend the motion to be explicitly use case 4.1.

Dan Harkins seconded the motion to amend.

C- The ones I see are 4.1, 4.2, 4.8, and 4.26.

C- 4.2 is during association.

C- 4.2 is on association.

C- I’m not willing to see 4.8 and 4.26 included.

C- 4.1 and 4.2 suffice.

Q- How do straw polls inform motions?

A- Straw polls are not binding in this group. They give the ability to check the temperature of the participants in a particular meeting.

Q- Why is 4.2 included? It occurs during association. Why is it included in this motion?

Q- Are you against addressing 4.2?

A- No, I’m not.

C- Then it doesn’t matter if 4.2 is included in the motion.

C- I think the motion should only cover 4.1. In our previous discussion we only talked about pre-association use cases, not association use cases.

The motion to amend was passed on unanimous consent.

C- The way I read this motion, it says you must address these two use cases to meet the PAR. If that’s true, then we would have to meet the PAR.

C- I declare this a procedural question. We can either agree to do this work or we can modify the PAR.

C- I would propose an amendment to delete “as being ‘in-scope’”.

Smith and Lumbatis agreed to this amendment.

C- Our PAR tells us to fix things that RCM broke. Whether we agree with that, it’s being done and things are broken.

Q- What does “that address” mean in the amendment? We can’t tell until the amendment is complete. I don’t even know why we are doing this motion.

A- I believe the rationale is that we have been back and forth on these topics and the group goes around in circles. This motion is trying to nail down whether we are going in this direction.

C- I sympathize. We’ve had several straw polls. There’s been a sizable number of people voting ‘no’, which would cause a particular scheme to address these use cases to fail. I’m trying to get the group to decide definitively whether we address these use cases as someone who has been working on a scheme. If we say ‘no’, then we change the PAR. I’m tired of bringing schemes and depending on who is in the room getting a different response. If this motion fails, then the PAR will have to be amended.

C- I prefer to leave “as being ‘in-scope’” in the motion. Also, use case 4.2 does access control. Our research found that almost all APs support such a feature. That’s why 4.2 is important to the Wi-Fi industry.

C- Let’s keep the debate procedural and not get into the technical validity of the use cases. If you believe the PAR covers this use cases, that’s one thing. You might believe that the PAR should be amended.

C- I was actually in the room where this started to come up. My issue with it is that it tells us how to vote when we get done. It presupposes that we must vote ‘no’ if it doesn’t have a certain feature. Everyone decides for themselves whether a feature is needed and meets the requirements. If this motion fails, that doesn’t mean we have to change the PAR. That’s a separate and distinct motion. I don’t agree with having to change the PAR at all.

C- I’m trying to get the group to agree to our scope.

The question was called. There was no objection to calling the question.

**The motion apparently passed on a vote of 15/14/5 (Y/N/A), with the voters to be validated.**

[Owing to a procedural error, the roll of voters and their votes was not captured].

C- This isn’t a great sign that we have consensus in the room. For things to be placed in the amended, a motion passing with 75% support is required.

1. **Comment Collection**

The current results of the comment collection are found in [11-22/0973r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-03-00bh-cc41-comments-against-d0-2.xlsx). Mark Hamilton walked the group through the comments in order.

1. **Contribution**

**Device ID generated by the network 11-22/1082r02 by Jay Yang**

This presentation covers comment identifiers (CIDs) 1, 3, 14, and 60. For CID 1, the simplified change is to delete “from an AP in the ESS”. This same resolution applies to CIDs 14 and 60, which would be accepted as proposed. For CID 3, the suggested resolution is an agreement in principle, with specific text given in the presented document.

Q- I’m not quite sure how to interpret these changes. You have a couple that just say “accepted”. Where is the text deleted?

A- This is a process question. If the proposed change in the comment is clear and the editor will know what to do, then we just say accepted. Does this text to be removed appear in the document in multiple places?

A- It does, but the comments themselves are clear as to which clauses they refer to.

C- I’m fine with the frame format changes, but I don’t like the change for CID 3 that removes “an AP in the ESS”. I think we need to talk about the ESS here and is the one in which the STA is connected.

C- But if you just say the AP, it doesn’t mean the value is received from the network.

C- The text says received from the AP. It doesn’t say the AP is the generator of the value. The ESS part is there to represent the network. I don’t think we should say “the network” in anything but out informal discussions.

C- I find this language vague and hard to parse and have put my suggested change in the [Webex] chat. If you are talking about an identifier, say which identifier. Don’t say “a value”. Nowhere else in the paragraph do you say “a value”. Otherwise the question is, “what value did you receive?” I suggest you use the “identifier most recently received from the AP in the ESS.”

Q- Did you mean to change “an AP” to “the AP”? And to delete “in an ESS”?

A- Yes, but mostly I want to change value to identifier. I don’t like “an AP” as much as “the AP”, but “identifier” is the real point.

The text was rewritten to “it shall send the identifier most recently received from that AP in the ESS”.

C- I agree that the term “the network” is vague and hand-wavy. Earlier in clause 12, we have that term as well.

C- Let’s discuss that earlier usage as a separate comment.

C- The change to “that” breaks things. It should be “an AP”.

C- I’m very confused with the “from”. I can understand sending the identifier to any AP in the ESS, but not the “from” part. If you are trying to send the identifier received from the AP to any (other) AP in the ESS, this seems like pedantic wording.

C- That seems like a misunderstanding. It would be helpful to redesign the sentence.

C- I’m not sure what “to an ESS” means in this context. A STA always connects to an ESS.

C- To address a previous point, let’s imagine that the opaque identifier can be used for a pre-association. I connect, I do the 4-way handshake and get the identifiers from an AP in the ESS. I roam to another AP in the ESS. Before doing that, I use my opaque identifier to instruct the AP that I’m the guy who was previously associated to the ESS. The identifier I have is the one most recently received, but I didn’t receive it from the AP to which I’m now trying to associate.

C- The identifier is only valid with the ESS. So, it should only be sent to another AP in that ESS.

C- There needs to be a new paragraph for other cases. That would eliminate the confusion.

Q- How is that change responsive to this comment?

A- I’m not sure.

C- We could break it into “for FILS do this”, “for FT do this”, “for other cases do this”.

C- It would be good to indicate that it is an opaque identifier to align with previous discussions. Also, there’s text being proposed in the chat.

C- Things in the chat need to be verbalized as well, otherwise they may not be addressed.

Q- Is the last sentence a replacement for the previous one?

A- Yes

C- Then we need to improve the grammar.

The sentence now reads “When the non-AP STA connects to an ESS, it sends the identifier most recently received from an AP in the ESS.”

Q- For CID 60, which ESS is being discussed?

C- I’ve submitted text into the chat as a suggestion: “When the non-AP STA joins an ESS it sends the opaque identifier most recently received from an AP in the ESS to the AP with which it is associating.”

C- If I search the draft, I don’t find many occurrences of “opaque identifier”. Is there an agreement to change to “identifier” to “opaque identifier” everywhere? If so, I’m willing to see “opaque” added here.

Q- Why are we adding the word “opaque”?

C- Let’s handle changing to “opaque identifier” as a separate matter.

C- I have a problem with the clause as it now stands with the submitted text. It is requiring the sending of this identifier as it is now stated. I was under the opinion that the inclusion of the identifier is for the non-AP STA to send (if it wants).

C- Why don’t we say “may send”?

The sentence would read “When the non-AP STA joins an ESS it may send the opaque identifier most recently received from an AP in the ESS to the AP with which it is associating.”

Q- Does this sentence cover all 4 cases? If just the last case, move it to the last paragraph.

A- It applies to all cases, so don’t join it.

Q- Is the “opts-in” in the earlier part of the paragraph equivalent to “may” in the sentence?

A- Yes, but let’s clean it up later rather than wordsmithing grammar in the meeting. I think what we have now on the screen suffices to get us through four comments during this meeting.

Q- Any objection to proceeding that way?

(None offered.)

C- This change breaks the resolution to CID 1. Delete the “delete” part and the “to make it simple” part because this causes conflicts with the final instruction to the editor in the resolution.

The resolution to CID 3 is to be copied to CID 1 as its resolution.

1. **Respond to Liaison from WBA:** [**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)

Will carry this for now.

**Meeting Adjourned at 15:30 EDT**