Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, Plenary November, 2021  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2021-11-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
| Stephen ORR | Cisco | NY |  | sorr@cisco.com |
| Peter Yee | NSA-CSD/AKAYLA |  |  | peter@akayla.com |

Abstract

This document contains the minutes of the IEEE 802.11bh telecom Interim meeting November, 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Nov 10, 2021 7.00 to 9.00 pm ET**

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

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 7.03 hrs. EDT,**

Agenda slide deck 11-21/1628r2

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

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:
  + November Plenary meetings: Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
  + Approve Sept interim and October/November teleconference minutes
* 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)
  + Response draft: TBD
* Issues Tracking: [11-21/0332r22](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-22-00bh-issues-tracking.docx)
* Draft 0.1 status
* Contributions (slide 20)

Nothing submitted on the WBA Liaison response

1 new topic submitted.

Any comments, any objections to agenda, Agenda accepted.

3 meetings at this Plenary.

1. **Approve Minutes**
   * Sept Interim session: [11-21/1545r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1545-00-00bh-minutes-tgbh-sept-interim-2021.docx)
   * Teleconference minutes:
     + Oct 12: [11-21/1682r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1682-00-00bh-802-11bh-telecon-minutes-oct-12-2021.docx)
     + Oct 21: [11-21/1739r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1739-00-00bh-802-11bh-telecon-minutes-oct-21-2021.docx)
     + Oct 26: [11-21/1766r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1766-00-00bh-october-26th-meeting-minutes.docx)
     + Nov 4: [11-21/1789r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1789-00-00bh-minutes-tgbh-nov-4-2021.docx)

Any concerns? None

Moved: Kurt Lumbatis

Seconded: Stuart Kerry

Result: Unanimous Consent

1. **Technical work**

Check that no contributions for the WBA response? None.

Chair will try to get something before end of the Plenary

1. **Issue Tracking Document**

Chair reminded TG of what TGbh is tasked to do. Issues tracking document 11-21/0332r22

Plus following Proposals received:

* [11-21/1083r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1083-00-00bh-a-signature-based-method-for-identifying-stas-with-randomized-mac-addresses.pptx): A Signature-based Method for Identifying STAs with Randomized MAC Addresses (reviewed July 15)
* [11-21/1585r9](https://mentor.ieee.org/802.11/dcn/21/11-21-1585-09-00bh-identifiable-random-mac-address.pptx): Identifiable Random MAC address (reviewed Oct 21, updated);
  + [11-21/1673r6](https://mentor.ieee.org/802.11/dcn/21/11-21-1673-06-00bh-proposed-text-for-irma.docx): Proposed Text for IRMA (briefly reviewed Oct 21, updated)
  + [11-21/1720r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1720-01-00bh-irm-advantages-and-use-cases.docx): IRM advantages and use cases (reviewed Nov 4)
* [11-21/1378r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1378-00-00bh-client-id-query-concept.pptx): Client ID query concept (reviewed Aug 19);
  + [**11-21/1379r3**](https://mentor.ieee.org/802.11/dcn/21/11-21-1379-03-00bh-proposed-text-for-id-query-action-frame.docx)**: Proposed text for ID Query Action frame (reviewed Oct 21)**

**Identifiable Random MAC address new slide edited.**

Olivia Fernandez presented the Slides on the IRMK Check that have been updated to cover the spoofing idea broached at the last meeting.

C – How does this work, address is over the air. What address is used on the LAN? MAC addresses must have same format. How would ARP work and proxy ARP? The STA is connected with an IP address.

A – On each association the STA has a MAC address, and that is the address it uses. It stays the same throughout.

C – AP can request Check after association. But exposing multiple bits of the key.

A – AP sends the Check challenge after association. Also AP can request a Check to help find the key.

C – Both sides have the IRMK?

C – Everything after 4-way. Everything after association.

A – First Check is to down select IRMKs, 1000 down to 4.

C – Protected ID sent in any frame, or higher level protection. Approach to address pre-association may present other problems or complexity. If opting in at supermarket not really associated to the network. Do you have feeling in practice to target pre-association use cases.

A – Looked into the use cases and keeping X number of STAs, time to live etc. AP can’t go through hash for too many keys, hence the check was added.

C – Trade off can be covered later for each Use Case.

C – Exposing Check exposes bits in key. Check can be used to track.

A – STAs cannot be tracked because STAs use random Mac and Hash, so no way of knowing if same STA even if it uses the same offset.

C – Check field if STA used same offset if it used can be tracked.

A – Maybe bits of keys but very difficult to track them as STA is impossible to identify.

C – If overlap of the offset is close then possibility of tracking is possibly higher

A – Still need to know who it is. It is a probability. IRMK Offset could be made to be offset by at least 8 bits, easily, and tie to the number of times also to when to change key. But still cannot tell who the STA is or correlate the Check to an IRMK.

C – Verbiage required to make sure STA does not use the same offset, then it would be very difficult to track.

C - If check request not necessary then any STA can spoof. Maybe AP should always send the Check.

A – If AP password is shared, then AP could send the check, but if secure network may not be needed.

C – Need to keep within our scope and not solve new problems. Must consider, do the solutions fix the problems introduced by RCM and not introduce any new privacy problems.

Chair – Started to look at Issues Tracking document sections 5 and 6 looking at solutions and metrics on how to assess pros and cons so we can take next step for what to add to first Draft.

Need to take next steps. Do we feel that any or all of the proposals are useful and should be considered for entering into the Draft? Solutions may be overlapping? Open to suggestions?

Thoughts, comments?

C – Like the approach, how does each solution relate directly to each use case.

A – Not sure how to do that except for authors to express and this could take a long time. Can members think about this themselves?

C – Can authors complete this themselves?

C – IRM proposal has done that. That seems a reasonable thing to do.

C – Onus is on the authors, but can write against the Use Cases, but difficult to explain every nuance of the scheme, and also how to address certain trade-offs and behavior.

C – Regarding mandatory behavior, should realize we are providing tools, then people can use these tools. E.g. a door that locks, could sell a door that locks itself, but some might not like that. Should not mandate use of any of these tools.

C – Is this end user or implementers?

C – Users, example captive portal solution. But to say everyone must do this….

C – Agree these are tools. But people may not know they have a problem until too late.

C – Can provide a set of tools, but if you use tool X you must do this (a set of rules)

C - Optional to implement can still have mandatory components to it. If you choose to implement it then you must do such-and-such. If you choose not to implement it then fine.

Chair – Is list of attributes that we considered last time complete?

Ask contributors to look at these lists.

**Transient Station Identification, presented by Nehru Bhandaru**

21/1839r0

C – Cannot use “TSID” as already exists

C – Slide 9 Probe request has the hash. Can that allow the device to be tracked?

A – As long as keep same MAC can use the TSID. IF change MAC, need to send update and switch TSID.

C – What goes into Probes?

A - Same MAC as before, with same TSID, but if wants to change, sends probe with update.

C – IF STA wants to discover AP is same as previously associated to. Do we assume STA knows the network? A- Yes, can discover network before doing this

C – Is STA sending same TSID and hash until it gets the right response? What if rogue Aps. How does TSID change.

A – Need to work out details. Needs to send special hash. AP and STA could get out of sync and need a new TSID.

C – Is probe request with update authenticate the AP?

A – Not in this proposal, could look at that.

C – Probe requests need to directed. Not wildcard. Only way an AP can handle this.

A – Yes, might need some back end co-ordination.

Next steps?

Discussions in next meetings

**Out of agenda**

**Meeting recessed at 8.58pm ET.**

**Meeting Nov 11, 2021 13.30 to 15.30 pm ET**

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

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 13.03 hrs. EDT,**

Meeting notes taken by Peter Yee. Secretary converted into Minutes

Agenda slide deck 11-21/1628r4

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

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:
  + September Plenary meetings: Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
* 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)
  + Response draft: TBD
* Contributions (slide 20)
* Issues Tracking document: [11-21/0332r22](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-22-00bh-issues-tracking.docx)
* Draft 0.1

**WBA Liaison:**

Chair - started to work on a response to the WBA Liaison, but it’s not yet ready for review by the task group.

**Contributions:**

**ID Query**

Mark Hamilton presented an analysis ([11-21/1853r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.11_dcn_21_11-2D21-2D1853-2D00-2D00bh-2Did-2Dquery-2Danalysis.docx&d=DwMFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=Z3s2jA8rgZoSco8f4kvDx_nOirz2RA_bah_KFKOseb8&m=13NnkbxbCRdUROnGZ1uyfy7L-KB30x9pkzqxif8iBrc&s=A-E7I7_1M0hOh1VH4sWWI15mUVgFB3xLjMpNY8lcGAE&e=)) of the ID query proposal ([11-21/1378r00](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.11_dcn_21_11-2D21-2D1378-2D00-2D00bh-2Dclient-2Did-2Dquery-2Dconcept.pptx&d=DwMFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=Z3s2jA8rgZoSco8f4kvDx_nOirz2RA_bah_KFKOseb8&m=13NnkbxbCRdUROnGZ1uyfy7L-KB30x9pkzqxif8iBrc&s=jCcf6AA8NX23R9qMQBvqJDdJi-xNofaSlewsa4DJ80E&e=)). The analysis compares the proposal against the use cases and desirable attributes document in the Issues Tracking document ([11-21/0332r22](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.11_dcn_21_11-2D21-2D0332-2D22-2D00bh-2Dissues-2Dtracking.docx&d=DwMFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=Z3s2jA8rgZoSco8f4kvDx_nOirz2RA_bah_KFKOseb8&m=13NnkbxbCRdUROnGZ1uyfy7L-KB30x9pkzqxif8iBrc&s=l_GDw7Y3ZkeYvOse6qLdjoa32iYIn72_L_PurlMLiUY&e=), at the point of the presentation).

Presenter believes use cases 4.1, 4.2, 4.3, 4.6, 4.10, 4.14, 4.15, 4.21, and 4.25 are probably covered by ID query. It’s not clear that it works for 4.23 and 4.25 (when using IP addresses).

C - the notes for 4.1 make it clear that what is meant here is PASN (Pre-Association Security Negotiation) with authentication. PASN can also be used in a non-authenticating mode.

C - disagree that pre-association identification is not in scope for IEEE 802.11bh.

C - the group had agreed to post-association, opt-in identification.

C - PASN is relatively expensive from computational cost.

C - The issues matrix document ([11-21/1140r01](https://urldefense.proofpoint.com/v2/url?u=https-3A__mentor.ieee.org_802.11_dcn_21_11-2D21-2D1140-2D01-2D00bh-2Dissues-2Dmatrix.pptx&d=DwMFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=Z3s2jA8rgZoSco8f4kvDx_nOirz2RA_bah_KFKOseb8&m=13NnkbxbCRdUROnGZ1uyfy7L-KB30x9pkzqxif8iBrc&s=ssY52ZFq8tNgX4_cxY27E6Wzzt2OprVtm8d_fQskxWs&e=)) suggested that we would handle certain pre-association use cases and not cover things like parental control. It seems the issues tracking document and issues matrix are not completely aligned.

C - the task group should revisit the disconnect.

C - agreed that parental control-type access cases should not be in scope, but more interested in post-association identification use cases.

Q - In regards to use case 4.3 does post association means an encryption key has been established?

A - we may have been a bit loose in our terminology. Meant the devices are in State 4. That should probably be clarified in the Issues Tracking document. Use case 4.6 may work with PASN, not just post association.

Q - does that use case mean that the device was already authenticated to the network, which meant it was identified?

A - for pre-shared key authentication, there wasn’t a real identity for the device.

C – believe that clarity about the network authentication type probably should be factored into what a use case implies

C – note that the broader confounding factor that Layer 3 or higher can be used post-association for identification purposes.

C - it’s a question of a reasonable and efficient way to handle a use case, and whether the use case has any possibility of being applicable prior to association (albeit perhaps with PASN).

C - believe that most services are going to have their own identification schemes and aren’t likely to use a Layer 2 identity.

C –remember that the impetus for TGbh was the use cases that were noted as breaking with the introduction of RCM.

C - agrees that most IoT systems will need to log into a system at a higher layer than Layer 2.

C - 4.6 should not assume that the device is associated with the infrastructure network – they may use other networks and it’s only their location that matters. PASN-type statefulness might be possible, but generally there won’t be a user credential for the grocery store’s network. Even for home networks, if a solution only works where the identity is bound to the network authentication credentials, that’s too limiting. That’s a big change in the user experience from what we have today. Families aren’t going to hand out passwords to each family member. Specifically, if we need PASN to work for pre-association, non-infrastructure, non-IP use cases, that suggests we may need identities at Layer 2. In comparing the different schemes, where there are pre-association frames with different MAC addresses for each probe, schemes that are bound to the MAC address are not very efficient if the MAC address changes rapidly. We shouldn’t over-complicate the design for edge cases.

C – not that it hasn’t been determined if use case 4.14 is in scope. Several people noted that other organizations have worked on on-boarding protocols that 4.14 tries to cover. Thus, it may not be necessary for IEEE 802.11 to solve it. Pointing to those other solutions is an acceptable answer to current day problems.

C - since other organizations have already looked at the problem and provided solutions, we should have no problem promoting them.

C - believe we should not promote any insecure mechanisms. There are many better, secure solutions and IEEE 802.11 shouldn’t do something worse.

C - agree and disagree with those points. Those organizations were solving their own problems. It’s not clear they were solving the exact same problem that we are trying to handle. So, we should be very clear whether the solutions and their matching problem statements are compatible with our own use cases.

C - do not want us to promote any insecure solution from IEEE 802.11, even if there were no other organizations solving the problem. It would be better not to provide a solution than to provide one that’s insecure.

Several agreed

Use case 4.15 (customer support and troubleshooting

Presenter - We have not decided yet if this is in scope or exactly what it means. There’s a bifurcation between enterprise vs. residential sub-use cases, and pre-association vs. post-association scenarios. For use case 4.21, it’s not clear if we’re providing a more secure solution, but caution that we are only trying to get back to the status quo (insecure accounting and billing), not provide a better system for those purposes.

C - challenge the assertion of getting back to the status quo, because an attacker could sniff a MAC address and piggyback off someone else’s account. A secure identity would be preferable.

C - there’s a trade-off between a MAC address as a public ID and the use of the ID query scheme to obtain a secure ID that a knowledgeable user might be able to extract and disseminate.

C - these use cases generally work with a captive portal for identification and billing, with the MAC address then used to allow the device to bypass the captive portal until its paid usage period is over or the device signs out of the service.

C - with MAC address changes much easier than before, use of the MAC address as an identifier in this scenario is unwise and we shouldn’t work to re-enable it.

C - believe ID query for use case 4.21 should be declared out of scope. There’s no binding between a captive portal authentication and the MAC address other than the billing system’s belief that a MAC address can be used for this purpose.

C - Agree that we shouldn’t promote poor schemes, but the organizations that have chosen to deploy them have made a conscious trade-off to accept some loss in exchange for a very simple scheme. WBA has asked IEEE 802.11 to solve the problem because their users want it solved. We can certainly provide comments that highlight the insecurity of the scheme. It’s within our charter to address.

C - think that organizations would like to perform more secure accounting and billing, so we should indicate that the scheme is insecure and should be reconsidered.

C - we can certainly give opinions to the WBA about the use cases, not just solutions.

C - would like to see these opinions documented. Use case 4.22 (QoS/QoE) has not been declared in scope yet. Client ID query would solve the use case if it was. Use cases 4.23 and 4.24 (DHCP pool exhaustion and inconsistent DHCP address assignments) are also use cases that we have not yet decided on. Client ID query might not solve the problem either, but maybe using a common DHCP ID and (IEEE 802.11) client ID could work. One other suggestion is that coupling the DHCP pool timeout duration and MAC address longevity might be helpful but isn’t really something IEEE 802.11 can specify.

C - prefer to leave DHCP problems to the upper layers and take IEEE 802.11 out of it. Also worried about use of a common identifier between Layer 2 and higher layers in most cases, as that might lead to accidental exposure at a higher layer. Use case 4.25 (ACLs/firewalls) would seem to be in scope and solvable with Client ID query, assuming the firewalls are filtering on MAC address and not IP address.

C – think that the firewall would not be co-located with the AP, so wondes how the firewall would make MAC address-based decisions using Client ID query.

C - the firewall might be part of the AP, but look at the WBA’s query again to see what they were thinking.

Chair brought the Issues Document back for discussion.

C - It was quite clear that the task group had not converged on a common understanding of which use cases were in scope and which were not, let alone precisely what a particular use case means.

C – ask that there be an agree/disagree column added in the issues tracking document to lock down what use cases we will address.

C - use case 4.1 (pre-association client steering) isn’t something IEEE 802.11 itself has. Not sure we should be creating a whole new scheme for it.

C - ANQP neighbor reports could be used to allow a client to make a better decision about where to associate.

C - disagree that IEEE 802.11bh needs to flesh out a scheme for client steering.

C - believe the use case is out of scope and that there are ways to do steering atop existing IEEE 802.11 services. MAC address-based responses to the ANQP query are probably a misuse of the standard. If there’s something we can do to improve the use case without compromising privacy, that might be a nice-to-have feature.

C – believe that there are systems that are capturing probe requests for STAs that are “unhappy” and they use the STAs’ MAC addresses to track and steer them. RCMs have broken that.

C - such a problem could be solved by having a STA continue to use a MAC address for probing over a short period of time, but not sure if want to promote that solution.

C - concerned that we are deciding on whether a use case is in scope based on whether we can envision a solution.

C - pre-association client steering can be done within an AP, between bands.

C - suggest we treat the use case as in scope, but with a recommendation that doesn’t actually require any schemes out of IEEE 802.11bh.

C - would solve 4.1 if some other use case solution we are working on happens to be applicable, but wouldn’t perturb our solution to solve 4.1 specifically.

C - For use case 4.2, it should be marked out of scope. Can live with 4.3 but find it similar to 4.2.

C – Agree

C - disagree, suggest that not dealing with these use cases will just see them come back, unless there are widely deployed higher layer solutions.

C - agreed with last comment, think the wording of use case 4.2 to be off-putting. If RCM breaks it, we should look into it.

C – would calling the use case “post association device identification” work? Feel that would be in scope.

C - how does reconnection to captive portals fits in with this use case?

A - the MAC address can be used by the captive portal to determine if it’s going to intercept a connection or let it through. Some captive portals use cookie-based solutions to determine the identity of a returning device and make an access control decision.

C – my browser settings cause the deletion of cookies in real-time, so if there isn’t a MAC address-based solution, I have to log in all the time if cookies are the solutions.

**Out of time**

Meeting recessed at 3:30 p.m. EST.

**Meeting Nov 12, 2021 9.00 to 11.00 pm ET**

**Chair: Mark Hamilton**

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 09.03 hrs. EDT,**

Acting Secretary Stephen Orr.

Agenda slide deck 11-21/1628r5

**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:**

* Attendance, noises/recording, meeting protocol reminders
* Policies, duty to inform, participation rules
* Organization topics (see also Backup slides):
  + PAR/CSD: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html); [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
  + Timeline estimate
* Response to WBA Liaison
* Issues Tracking
* Contributions
* Approve Draft 0.1
* Other use cases not covered
* Next steps:
  + Timeline review
  + January Plan
  + Teleconferences

The Chair reviewed the agenda.

The proposed agenda was adopted without objection approved by unanimous consent

1. **Timeline**

* PAR approved Feb 2021
* First TG meeting Mar 2021
* D0.1 Nov 2021
* Initial Letter Ballot (D1.0) Mar 2022
* Recirculation LB (D2.0) Jul 2022
* Initial SA Ballot (D3.0) Nov 2022
* Final 802.11 WG approval Mar 2023
* 802 EC approval May 2023
* RevCom and SASB approval May 2023

1. **Response to WBA liaison request** – contribution needed

Chair asked for contributions – none submitted and no volunteers

1. **TGbh Issues Tracking document: 11-21/0332r23**

Chair discussed the Tracking Document/Contributions 11-21/0332r23 **Section 5 Issues and analyses**.

* Summary of previous discussion on sections 4.2 and 4.3 on whether they are in scope

Discussion focused on 4.2 Post Association Access Control

Q – If fixing 4.2 and 4.3 require changes on the STA, why not solve this at an upper layer. Should be done above 802.11.

C – Makes sense that any identification be done at the application layer. Solves problems and allows user consent.

C – If it is pre association – how do we do this with an app

A – We would have to solve that problem

Q – What change would we need on the client side?

A – For this to work today the STA side does nothing. In the future – you would need to add a user interface component and the user to enter in the identifier (even on headless devices)

C – Interface is not possible

C – There are already STA side requirements for user interface to enact security. Has to be a way to enter in security credentials (even just a passphrase). There are additional requirements being put in place for WPA3.

Q – Are there things that are broken at the L2 network that this randomized MAC address is broken and how do we solve those issues?

C- These problems may have been solved at higher layers already.

C – Captive portal discussion in 4.2 is an item that is somewhat broken by the MAC address change and we do not have a good solution. Using a cookie – anyone concerned with privacy would be using a browser that would be clearing cookies. The captive portal case could work if the MAC Addressed is not randomized on return to a known ESS.

C – There were implementations that some STAs were randomizing MAC addresses on a periodic basis even for the same BSS. Is the STA direction to change their MAC addresses on a periodic basis.

C – Discussion of a STA UI – most default to randomized

C – there has been a move from Opt-in to opt-out of enabling RCM

C – IEEE provided the privacy protection, vendors UI and implementations can vary

C – There could be a way for the STA to notify the AP that it is a returning device. The device could be tracked by the network, but not a 3rd party. This could solve most of 4.2.

C – Device identification is on per SSID or network basis to make it clear – the same identifier would not be shared across multiple networks. We may also want some type of timeout/lifetime of identifier as well.

C – We should not mandate the type of identifier. On top of opt-in user control of over the identifier and lifetime.

C – Some UI/STA have an opt-in to have a non-persistent randomized MAC for a given ESS  
 <https://source.android.com/devices/tech/connect/wifi-mac-randomization-behavior>

C – Add one more option to randomize on return to given SSID.

C – EZ-Connect is a provisioning protocol, replacing WPS and can also issue credentials

Q – On Android 12 behaviour – if I choose non-persistent address do I have to log back in to the portal.

A – If the network was using your MAC address as the identity – then you would most likely appear as a “different” device.

C – Not all captive portals are outside security. You can deploy a passphrase so not all Captive portals are “Open”

Q – What do we mean by protected exchange of identifier? Encrypted or Encrypted and Authenticated?

C - Chair, we need to be careful about judging our use case with solutions we think we can imagine.

C – In IRMK proposal the AP is not authenticated – we are about to repeat the same mistake to allow an AP with a target SSID to receive the identity.

C – A nationwide SSID could cause the same MAC address to be used.

C - Enterprise utilizing 802.1x PMK issued by a AAA server which authenticates a user based on additional information is an entirely different use case.

C – There are some proposals that are not secure – encryption should be a minimum.

C – If we have encryption that is great – passive attacks could be minimized but active attacks would still be a problem.

Q – Who is the recipient of the ID. We could propose that the ID is only exposed if the identity is encrypted and authenticated to the AP.

Q – When is the STA authenticating the AP? EZ-Connect (without EAP), SAE-PK

C – We need to decide on if these are the use cases we need to address vs clarifying requirements.

C – Either a use case is in scope or not (ref section 4.2).

Q – Chair – have we adequately covered the use case (section 4.2) to develop the requirements?

A – Yes

Q– Suggest having a straw poll.

A – Chair – see if we can do this via unanimous consent. We still need to work through details – but conceptually is this use case in scope?

C – Two use case requirements

1. RCM breaks the current operation
2. User can opt-in

C - We should rename the 4.2 use case remove Parental Control. High level – can the network identify a returning device to the same ESS with a changing MAC address.

C – Text says should provide identifier to trusted infrastructure which implies mutual authentication is a must.

Q – The identifier could be generated may not need to be encrypted – not sure what that statement means.

A – Was taken as the ID should be opaque to 3rd parties.

C – We should use Confidentiality, Integrity and Authentication of identifier

Q – Need to be careful about the definition about 3rd parities. What is the definition of a 3rd party?

A – Chair – could be an attacker and not a part of your intended operation.

C – Any information provided should only be used within the ESS/BSS.

Chair – we are supposed to be deciding if we are going to focus on this use case (4.2) and agree to that.

Q – what does in-scope mean? Is it an interesting use case to be considered?

C – EULA agreements are outside the scope of 802.11

C – If the client can identify the network and the network can identify the client – that should fix most of these issues

C – Seems to be that we are losing focus

C – If the 3rd column is titled – Should TGbh consider this use case, it should be Yes or No then move to these requirements later.

Q – We are talking about tracking the user or just the device?

A – The user is using the device. The behaviour of the device can be used to track a particular user. If we are going to differentiate between user and device identifiers, in this case they may be interchangeable.

A – All we can say is that a device is being tracked, not the user.

C – If one person logs off then another user logs on the same device – we are not tracking the user, so the user and device identifiers are not interchangeable.

Chair – are we agreeing that a device returning to a network (ESS/BSS) and changing its MAC address is a use case we want to address and we have a need to discuss the requirements?

C – Let’s move on to the other use cases.

Chair can we live with “Yes, requirements need to be clarified (the list in the centre column is for requirements to be considered.)

No objections

**Out of time to start further discussion.**

Chair – please look at the rest of the use cases. Next step is to look at proposed solutions and how do we analyse them.

Next calls to be scheduled

**Meeting Adjoined at 11:01 ET.**