Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11 bh Plenary Meeting Minutes, July 2021 |
| Date: 2021-07-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11 bh telecom Plenary meeting 13, 14, 15 July 2021

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer given

C- proceeds a comment

**Meeting July 13, 2021 13.30 to 15.30 hr ET**

**Chair: Mark Hamilton**

**Secretary: Graham Smith**

**1. The teleconference was called to order by Chair 13:30 hrs. EDT,**

Graham Smith (SRT) volunteered to be acting secretary.

Agenda slide deck 11/21/0942r3

1. **Policies and procedures were presented by the chair. (Slides 5 to 15)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda July 13 13.30 -15-30 ET:**
	* Attendance, noises/recording, meeting protocol
	* Policies, duty to inform, participation rules
	* Organization topics:
		+ July Plenary meetings: Tuesday, 13:30-15:30; Wednesday 13:30-15:30; Thursday 13:30-15:30
		+ Nominations for Editor
		+ Approve May interim and June teleconference minutes
		+ PAR: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html) , CSD: [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
	* 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)
	* Contributions:
	* Issues Tracking: [11-21/0332r9](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-09-00bh-issues-tracking.docx)
	* “Solutions” contributions pending: [11-19/0179r3](https://mentor.ieee.org/802.11/dcn/19/11-19-0179-03-0arc-idquery-query-message-proposal.pptx) [11-19/0496r1](https://mentor.ieee.org/802.11/dcn/19/11-19-0496-01-000m-id-query-proposal.docx) [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)

The Chair reviewed the agenda.

The proposed agenda was approved without objection.

1. **Nominations for Editor**

One nomination recieved**.**

Chair asked if any other nominations – none

Chair closed nominations. Election will take place Thursday.

1. **Approve Minutes**
	* May Interim session: [11-21/0882r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0882-00-00bh-minutes-may-interim-tgbh.docx)
	* Teleconference minutes:
		+ June 14: [11-21/1023r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1023-01-00bh-802-11bh-telecon-minutes-june-14-2021.docx)
		+ June 28: [11-21/1029r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1029-00-00bh-minutes-tgbh-june-28-2021.docx)

Moved: Peter Yee Seconded: Carol Ansley Result: No objection

1. **Liaison from WBA**

Document 11-21/0703r0. Embedded documents, the letter and detailed concerns.

Chair suggests we acknowledge this and then wait for issue list to be completed and see if we need add.

Any comments? – None

Plan accepted.

1. **Issues Tracking Document 21/0332r9**

Next issue is 3.10 from the TIG report.

Residential gateway with wireless hotspot.

Service providers are deploying residential wireless gateways with public hotspots to expand their network coverage and capacity. With millions of hotspots available, subscribers can enjoy the benefit of complementary and seamless 802.11 connectivity while on the go. When a subscriber is at home, however, their devices should connect to the wireless home network rather than the hotspot available on the residential gateway. If a device connects to the hotspot, the subscriber doesn’t have access to their local network, cannot print files or access storage attached to the network. Neither can they enjoy their gigabit subscription. The gateway can prevent “home devices” from connecting to the hotspot based on their expected unique MAC address

C – Decision STA makes, not sure what is expected of the Gateway.

C – Such devices are being deployed. Should MAC be used? No. Valid use case? Yes. Could point out a better way to do this.

C – I have Comcast and internal service, but Gateway also offers Xfinity WiFi. Idea is to steer those with private side to the internal. Handled by the STA, my STAs connect to the private side.

C – Passpoint could be used.

C – Could be left to the STA, as to which network to associate to. A lot of effort for 802.11 to come up with rules.

Chair – Hearing this, use case is solved at the client end and may not be within our scope.

C – If we develop solutions to other Use Cases, we may get this one for free.

C – STA has two profiles, one for internal and one for the public side. Hence idea is to prevent a connection to the wrong one. Not sure this comes up with another use case.

C – Think not valid use case as STAs should have their own priorities. Connection to other network should not be prevented.

Chair – Use case not to be considered

Next Case – 3.11 Pervasive Surveillance

Some organizations, both public and private, have a strong desire to monitor people in their behavior and habits. Having a device constantly emitting a unique identifier can help such these organizations surveil people. When people move around, sensors that passively detect these unique identifier emissions can make note of the identifier. Time and location of the sensor can combine with this datum to create a large database of information that can enable tracking of people. Habits can be recorded and observed and deviations from an established baseline can result in an alert regarding the person’s behavior. Artificial intelligence and big data analytics can use this database of information to facilitate this effort. A database of who is where and when can be used for a multitude of purposes, some benign and some nefarious. Records in the database can be used as evidence in a government’s case against a citizen, and personal, and private information about people can be sold without their knowledge or approval.

802.11 is an obvious technology to build such a surveillance apparatus. Fixed MAC addresses will be used in mobile devices even when SIM cards are swapped out or removed. Laptops typically do not have a method of network access that is not bound to a MAC address. The tendency of unconnected devices to find a network results in active probing which can be passively detected, thereby enabling the surveillance apparatus. Indeed, the very nature of 802.11 network discovery and connection establishment compels exposure of MAC addresses and there is no way to disable their use. Using 802.11 to construct a surveillance database is an obvious choice.

Q – Isn’t this the exact reason why government introduced Privacy Laws?

C – Sometimes this may be carried out by Government.

C – Issue is that regulations grant a particular right. Note that nefarious use may be by anyone. People should be able to protect information.

C – How to place equipment that complies with privacy and data protection? Not just in interest of individuals, but in interest of suppliers. Standard needs to be capable of addressing protection.

C – Never benign, probably valid use cases for tracking large number of devices, but with is title cannot support Pervasive. Hence maybe re-name?

C – Differentiate between lawful intercept and then 5G cases with a court order to get information from service providers. Is there a way to allow surveillance?

C – Have discussed tracking in a Shopping Mall, how is this different?

A – Other cases are an ‘opt-in’ scenario.

C – Is there some document that mandates such operation? Where is this Use Case coming from?

C – Confused but this use case. MAC randomization is already in STD. This use case seems to want to fix the MAC address. Nothing here is broken by RCM. Enhanced privacy is TGbi.

C – Before RCM MAC address could be used.

C – This used to work, now it does not. Hence, should we fix it?

C – In WBA Liaison document they consider Lawful Surveillance, and that is the use case we should be considering. Pervasive is bad and is made more difficult by RCM , so that is good, lawful surveillance is good, and made more difficult by RCM. Hence substitute the lawful case and delete this pervasive one.

C – Lawful surveillance, I am not compelled to assist interception of me. Can be legally gathered with warrant but not compelled to make their task easier. This use case negativity was intentional as TIG was adding use cases that showed RCM was a problem and wanted to add a case where RCM was good. This is not something we want to fix. We could drop this as intention was simply to add a case where RCM was good.

C – From legal standpoint are we compelled to aid the government? Individuals are not compelled to aid the govt., but are service providers compelled?

A – Yes, but now, with RCM, the info is garbage. Govt. needs to overcome RCM or user could simply turn off RCM

C – MAC was never intended for tracking. Was a happy accident for trackers? RCM makes surveillance not an option at all.

C – So question is “do we have to help the govt”

C – When a ‘flaw’ is built in that allows pervasive surveillance, then could bring customers into problems.

C – If anyone has evidence as to real intercept requirements then would like to know.

C – MAC randomization was introduced in vehicles.

C – Go back to PAR, goal is not to degrade privacy provided by RCM. Need to still allow a user a level of privacy for their devices. So if we do at least as well as RCM offers, we are good. Don’t go to the regulations arena, too many.

C – In terms of surveillance, not just about governments. Out of scope at this level. But if RCM has given a level of privacy, we need to protect it.

Q – Any objection to not “fixing” this one? But need a bit of background as to why we feel we do not have to.

C – Easy way out is “beyond scope of PAR”, could mention MAC addresses never meant for tracking purposes.

C – Happy to get rid of this.

C – Clear to me that our PAR is clearly against this.

C – Will take much effort to find my MAC address, so why should a govt want to know my MAC address. Our commitment should stay with the user.

C - Missing point. Lawful tracking is primarily for criminal and terrorist prevention yet all we hear is personal protection. Vast majority of uses of this have been in such cases. Still not a case for change, however.

C – Place is not at layer 2.

C – Is happening in western govts. Govts Put a lot of trust in statistical likelihoods.

C - If not aware of any legal requirement to prevent us ignoring this use case.

C – Tracking of cellular as SIM cards give out ID. Do need reason to find cell phones.

C – Requirements for operators but nothing for the standardization. No need to look into this use case.

Chair – leave at that

That ends Use cases from the TIG report.

Emergency Services? Is there something damaged?

C – Have discussed previously, may be based on bad assumption and not something to fix

C – Is there an emergency alert were ID required to find someone through their MAC?

C - Trying to find a non-associated STA based on MAC address?

C - E911 case structure to provide location was translated into AP providing MAC addresses. Not sure how this worked with the metadata and registering on a central database.

Another possible case:

Roaming from AP to AP within a Public Hotspot. Not same ESS but same Hotspot ID.

C – Think this is covered by other Use Cases.

C – Enterprise with multiple APs, same ESS, requirement is that re-association with same MAC. If you associate fresh, all rules are off and your problem.

C – Stations should not do this

C – We heard that total RCM was now possible, or the time out. Do we assume this is not allowed?

C - We should assume baseline. General agreement that if changes, then client has chosen to do this.

C – Only concerned with devices in agreement with our Standard.

C – Can we add 21/1140r0 to agenda next. Issues Matrix.

A - OK

C - WBA Document has several Use Cases. Document “Excerpts of WBA Document” has been prepared with precis. Will post and this could be used to identify if any new cases.

**Out of time**

**Meeting Recessed at 15.31 ET.**

**Meeting July 14, 13.30 – 15.30 ET**

**The teleconference was called to order by Chair 13:30 hrs. EDT,**

Agenda slide deck 11/21/0942r4

1. **Policies and procedures were presented by the chair. (Slides 5 to 15)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda July 14 13.30 -15-30 ET:**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ July Plenary meetings: Tuesday, 13:30-15:30; Wednesday 13:30-15:30; Thursday 13:30-15:30
	+ PAR: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html) , CSD: [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
* 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)
* Contributions: 11-21/1141r0, e911 discussion, 11-21/1140r1
* Issues Tracking: [11-21/0332r10](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-09-00bh-issues-tracking.docx)
* “Solutions” contributions pending: [11-19/0179r3](https://mentor.ieee.org/802.11/dcn/19/11-19-0179-03-0arc-idquery-query-message-proposal.pptx) [11-19/0496r1](https://mentor.ieee.org/802.11/dcn/19/11-19-0496-01-000m-id-query-proposal.docx) [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)

Agenda adopted without objection.

1. **Contributions**

**WBA Document**

Graham Smith Presented 1141r0. Looking at issues raised by WBA and making decisions as to include as new Use Case in the issues tracking document.

* MAC-Based access control - Already covered
* Passpoint Profiles

C - Terms and conditions outside scope

C – Acceptance of conditions is not defined in 802.11. Not the root of the problem, but better solved in WFA and is in scope for them.

C – Just consider as a note or leave it to WFA.

Q – Any objection for that approach - None

* Client Steering – covered in Tracking document
* MAC Collisions

C - Did we enter anything in 11aq on this?

A – Nothing particular in 11aq. We do not tell anyone to randomize all bits. Would be in favor of randomizing all bits rather than 802.C.

C –Maybe not all bits

C – 802C is not practical hence a STA should randomize as many bits as can.

C – We had a ton of comments on this. We added advertising the MAC policy.

Q – Should we enter this into tracking document? - General agreement

* Physical Layer Analytics – Covered
* Accounting and billing issues

C – Don’t understand use case, that it relies on MAC address, but does indicate a way to do this. CUI is the solution for billing, so in favor of using that. Not sure what the “rate” is referring to. Without more details should not do anything on this.

C - If I were implementing a client, I would use a random MAC to do the ANQP query and then change it prior to selecting and associating with the network

C – One example is if I have a better rate than ‘normal’ then I need the system to identify me.

A – Do we need a recommendation or such and hence keep in our document?

General acceptance to add so as to make some comment. (Noting we do have a solution)

* QoS and QoE

C – May be similar to post association access control.

Q – Add to document? – no objections

* DHCP and ACLs IP address

C – We do not have, add to document? No objection

C – Different items in this which may need addressing differently. Inconsistent DHCP address assignments and ACL identifier using IP address?

C - Client can ask for specific IP. Maybe related to 802E work.

* Lawful Intercept – In document
* Future Investigation

C – Easy Connect could be used. Should be Enhanced Open, but that will not help.

C – At some time we should plan to go back with detailed responses to these.

C – Not sure Capport may help, may streamline but would need modifications.

C – Easy Connect relies on MAC address – countered, need not include MAC address in QR code.

We do owe WBA a response.

**E911 Discussion**

Background - In 2014, national database, goal of having any network records any device that beacons, when device placed emergency over LTE or Wi-Fi, MAC address is in metadata, declared location then used. However, this database was cancelled mid-2020. So nothing to worry about anymore. No mandate now on a client device to send MAC address.

C – Understand requirement now not out there anymore, but given location and our specification, should we still make known that Wi-Fi location makes sense, and could be used for E911 purposes. Hence, we do supply a solution?

C – We are supposed to work on items that used to work and got broken. This may be a new project but not TGbh.

C – Do agree. TGaz did look into this. AP can compute the distance of the STA

**Issues Matrix 21/1140r0**

Presented by Dan Harkins.

Authorization decision / authenticated identity matrix

Authorization decision based upon no authenticated identity, “yes/no” is a bad idea – e.g. Home automation, parental control. Hence spend no time looking at these.

Authorization decision based upon an authenticated identity, “yes/yes”, is a good idea – e.g. Emergency services, residential hotspot

Need to focus on “no/no” issues where no authorization decision is based upon no authenticated identity – e.g. Grocery store, airport security queue, pre-assoc steering, connection issues. Move them to yes/yes

C – Have ideas to change home automation and parental controls, but I am not in product development and should not spend time showing bad product manufacturers how it should be done. Question whether we should be giving solutions.

C – Or are we determining a feature that .11 should provide? If yes, then in our scope.

C – Very helpful but now need to complete the list. Which is maybe a way to organize the tracking document.

Q – Is the yes/no based on customer opting in or out?

A - Home automation example, garage door opens based on MAC address. Bad decision as based on network access based on easily forged ID. Nothing to do with opting.

C – yes/yes assumes an authenticated identity? Is that always true? What about emergency service? Depending on how you access emergency services, anyone can call 911 without authenticating.

C – But can only call E911 so no authorization decision at all. Could move it.

1. **Issues Tracking Document**

Looking for volunteers to turn the notes into text. Then to take those we feel are in our scope and work on them.

Back to looking at the Use Cases added from the WBA document.

MAC Address collisions

C – We should advise to randomize 46 bits and make check that no collision.

C – Not sure can support that.

C – Could put 802C info in the beacon?

C – Beacon or ANQP for policy for MAC addresses?

Q – Are we saying that more text is required to 11aq? Recognizing the pain we had getting that text accepted.

A – Yes, to be frank it was unpleasant and was a compromise and does need to be modified.

A – Yes the RAC did not want to recommend MAC randomization, so a compromise. Text I suggest is to explain how the compromise might work. Am confident to state that no-one has used the 802.C policy.

C – Improvements to that clause could be done in TGme. Since 11aq there have been efforts to educate RAC on how 802.11 works.

**Out of agenda items and time**

**Meeting Adjoined at 3.26 hr ET**

**Meeting July 15, 13.30 – 15.30 ET**

**The teleconference was called to order by Chair 13:33 hrs. EDT,**

Agenda slide deck 11/21/0942r6

1. **Policies and procedures were presented by the chair. (Slides 5 to 15)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda July 15 13.30 -15-30 ET:**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ Editor election
* (Reminder: 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) – respond soon)
* Contributions:
* Issues Tracking: [11-21/0332r11](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-11-00bh-issues-tracking.docx)
* “Solutions” contributions pending: [11-19/0179r3](https://mentor.ieee.org/802.11/dcn/19/11-19-0179-03-0arc-idquery-query-message-proposal.pptx) [11-19/0496r1](https://mentor.ieee.org/802.11/dcn/19/11-19-0496-01-000m-id-query-proposal.docx) [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)
* Next Steps:
	+ Timeline review
	+ September plan
	+ Teleconferences

No new contributions on Issues Tracking document.

“Solutions” contributions. 21/1083 will be considered at this meeting as requested by the author. The other two may wait until Issues Tracking comment is considered further.

Agenda adopted without objection.

1. **Editor Election**

Call for candidates for Editor was open June 28 – July 13.

One candidate was nominated: Carol Ansley (Cox).

With one position, and one candidate, suggest unanimous consent acclamation.

Any objections? - None

Congratulations and thanks to Carol

1. **Contributions**

**“A Signature-based Method for Identifying STAs with Randomized MAC Addresses”**

Presented by Liuming Lu (OPPO)

Contribution introduces the ‘address signature’ method for the station identification - a scheme to uniquely identify STA with RMA (randomized MAC address)

Use Cases:

Home Automation Detection Assisting

Router parental control

Background:

The STA has a pair of private key and public key, and the private key is never disclosed. The private key is used to generate the signature, and signature signed by the “private key” can be verified only by the “public key”.

* The STA transmits its public key to an AP, and AP caches the public key.
* The STA signs the RMA with its private key to generate an address signature.
* The AP verifies the Address signature by the STA's public key.
* The AP distinguishes different STAs by STA's public key

Pause at slide 7

C – to work each message with signature needs the Public Key, but this would allow tracking. Also, public key and ID needs to be given to AP. Issue of who holds the pubic Key, Parent or Child? Lot of infrastructure missing.

A – Who has public key? Not understood

C – AP to make decision needs to know if parent or child. Public key is not enough. Every time child tries to access network public key in the clear is sent.

A – Private key used by STA, public key only used to justify signature. Applications which is parent or child.

C – Public key has to accompany the message. Or some hash of the key, but it will be static, which is a privacy violation.

A – Procedure will be shown

C – Simply replacing Public Key for the MAC Address?

A – Not transmitted frequently. Only transmitted in authentication phase

Continued at slide 8. Procedure:

* Step 1: the AP advertises its RMA capability in Beacon and Probe Response frames.
* Step 2: the STA carries its certificate in Authentication frame to the AP
	+ The STA’s certificate contains public key
	+ The AP caches the STA’s certificate if authentication is passed
* Step 3: the STA generates address signature by private key and carries address signature in (Re)Association Request frame
	+ The AP utilizes the cached certificate to verify address signature. If successful, the association can be allowed
* Step 4: after the association, the STA can carry its MAC address signature in data transmission for STA identification when RMA changes.

C - Slide 9. Certificate sent authentication frame. MAC changes and STA does association but if not authenticated with that MAC, then can’t associate. AP has 100s Public keys, and MAC address changes need to have packet with public key to find which signature is valid. It won’t work. On right track but needs more work.

C – State machine must advance with same MAC address. Hence cannot re-associate with new MAC.

A – This might enable change.

C – If public key remains same across all networks, same problem.

A – Only sent in authentication. Not often. How can check STA with public key?

C – Walking down mall, can track key if remains the same

A – Let me think on this.

Chair – maybe needs to be in reflector exchange

C – AP needs to identify correct STA, that is addressed. Issue is certificate is involved in authorization frame(s) Therefore, anyone knows it’s the same STA.

A – AP caches many public keys and searches to verify signature.

C – Attacker could inject number of frames to cause to AP to run out of resources.

C – We have solution to solve these problems, this is but the first step. Full solution can be more detailed.

C – What do we gain on solving this at layer 2? Concerns of attack are real. May be out of scope for layer 2. Only buys a second of latency in Use Case Home Automation. Can be solved at upper layer, this is application layer problem.

A – Address is changing so cannot identify STAs.

C – Can be solved once associated by upper layer application. No need to track MAC.

C – Not sure best use case is home automation. Trust of infrastructure is needed. Useful to identify STA when it returns. Need to fix a couple things, however, I like direction, STA first authenticates and has hidden handshake when it returns. This is first step. Happy to work with you.

Chair – off line discussion may be useful. Thank you.

Presenter – please send discussion/questions to me.

1. **Issues Tracking Document 21/332r11**

Finished “MAC address collision”, started to look at “Accounting and billing”.

Accounting and billing

MAC Address is tied to this in some use cases where rates rely on a unique device ID.

Inserted text from the WBA document

C – Should be split into two parts. WBA provide solution for one., Use of device to select different billing options and the other is need for STA to identify itself to the network, in a protected manner.

C – Billing etc. may use Passpoint or such. Not sure that MAC used.

C – Different because do not see how CUI works for first part on billing charges. Only used for specific user.

C – Seems incredibly poor choice to tie this to a MAC, as easily forged even before RCM. No reason to have any sympathy for this.

C – Maybe ask for more details. Could be a captive portal and then get special price, that might make sense.

C – AAA also ends with “Accounting” so no sympathy to do this without the other As in AAA.

C – Is this really just “post association” same as Use Case 4.2. Hotel portal? Could merge this?

C – Yes I think we should do that.

Q – Do we have a process for WBA? And ask questions?

A – We do need to reply and we could ask questions. We need text – any volunteers?

C – There is an offline liaison so only if we have specific questions.

QoS and QoE

APs that form the network hold a synchronized list of MAC address to QoS/QoE mapping to ensure that Wi-Fi clients receive a uniform QoS/QoE treatment throughout the full network.

C – Same solution may be as per the parental controls. QoS treatment for a given client as does AP to AP roaming.

C – Seems to be a mobility discussion linking QoS with mobility. Current rule is to maintain MAC address throughout ESS. Hence may be a misunderstanding.

C – If MAC address does not change then QoS is same. Session may have AP to AP roaming, do not change address and then no issue.

C – have protocol stream categorization service, only per association. Need to set up each time. So what are these rules that are discussed here?

C – Agree, need more clarification. Losing connectivity for a short time can be a problem wasting time to get back in correctly.

C – Key point is AP airtime scheduling queue, may be outside our specification.

C – Could be concerned with Admission Control or TPECS, need clarification. Pretty sure TSPECs are torn down on a re-association but need to check.

C – Agree not sure this is concerned with a QoS scheme in our spec.

DHCP Pool exhaustion

C – Use short lifetime (lifetime < randomization interval) – might be user experiences impacts. Or if clients can/will use a client ID and address request to solve. Just recommendations seem possible here.

C – Plenty of cases where IP address lifetime will not work.

C – Need to check impact on protocol definitions.

C – Option may be guiding STA who wants to be same IP to ask for it. Could recommend such behavior or in the client ID field in Passpoint. I.e. Protocol is fine it’s how you use it. Do we want to use the DHCP identifier versus providing a mechanism for client identification?

Inconsistent DHCP address assignment

Devices asking for IP address or renewal are identified by MAC address.

C – same as previous except short lifetime is not a solution.

ACLs/Firewalls

If MAC address has been instrumental in providing an identifier for use in ACLs, the MAC itself, the IP address, or a MAC based hostname- then ACL will not function as intended.

C – Similar to above except the IP address based variant.

C – What if ACL used for pre-association behaviour, a post association solution may not solve it. If this is for security/ACL is a device provided identifier trusted sufficiently or, do we need to add authentication to that identifier.

C – Service providers often ask for MAC address of a device.

C – Is there any value on 802.11 adding some identifier to solve higher layer problems?

1. **NEXT Steps**

Need to work on the document. What to address, what is in scope, then to talk about actual solutions.

Chair may take a first step on this but please use Reflector to discuss.

**Timelines** slide 26

Chair read through slide quickly.

**Meeting slots**, Slide 21, propose 3 slots in September avoiding conflicts.

Mondays 1 pm ET alternating with ARC.

C – 1 pm is not convenient for Asia. Please change

C – Will try to find other times.

Any other business? - none

1. **Meeting Adjoined at 3.30 pm**