IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Mixed Mode Plenary Session 10-14 July 2023 |
| Date: 2023-05-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Stephane Baron | Canon Research Center France | Cesson Sévigné, France |  | Stephane.baron@crf.canon.fr |
| Jay Yang | ZTE Corporation |  |  | Yang.zhijie@zte.com.cn |
|  |  |  |  |  |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place during the IEEE 802 Mixed Mode Plenary Session 10-14 July 2023. The on-site location for the meeting was Berlin, Germany.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**1st slot. Monday 10 July 2023, 13:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron acting secretary for this meeting**

**Vice-chairs: Jerome Henry, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

Chair calls meeting to order at 13:32 local time.

Agenda slide deck: [11-23-1001r0](https://mentor.ieee.org/802.11/dcn/23/11-23-1001-01-00bi-july-plenary-agenda.pptx):

1. Reminder to do attendance. Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.
2. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
3. The chair covered the IEEE copyright and participation rules.
4. **Discussion of agenda 11-23-1001r1**
	1. Further submissions added to the agenda
		* Doc 11-23/1160r0 added upon author request
		* The Chair asked for people having preference in presentation order or timing.

0873r1 ask to be presented first.

Chair ask if there is any opposition for this change. No answers.

Order of presentation modified accordingly.

* 1. Agenda as amended approved by unanimous consent (26 remote participants, 18 in-room)
1. **Administration**
	1. **Need for a secretary**

The Chair reminds that the secretary position is open and call for volunteer.

Secretary election will take place at the end of the week.

Secretary for this session is Stephane Baron (Canon)

* 1. **Motion #31**

	**Approve the minutes for:**

**2023 May 802.11 Interim: 11-23/903r1,**

**TGbi Teleconference: 11-23/1196r0 (06 July)**

Moved: Antonio de la Oliva, Seconded: Stephane Baron

Approved by unanimous consent (28 online, 19 local)

5.3 **Remaining meetings for this Plenary session reminder by the chair:**

* Tuesday 07/11 PM2
* Wednesday 07/12 PM2
* Thursday 07/13 PM1
1. **Technical Presentations**

**6.1 Client Frame Tracking Countermeasures** (**11-23/0873r1),** Philip Hawkes (Qualcomm Technologies, Inc)

Presented an update from previous presentation

Main modification is made to allow a client to initiate the change of MAC address.

**Discussion:**

Q: how does AP and client epoch work together. Do you mean that a station will have to maintain context for AP driven Epoch and potentially Epoch initiated by the STA?

A: Yes this is what I have in mind.

Q: So what if the client requests a change that is very close to the Epoch start defined by the AP?

A: Good point, we may need to raise conditions for the client.

Q: Can AP request for everyone, or a group of clients?

A: It would be nice to have a group of clients to initiate the transition but I haven’t got any though about that right now.

Q: Do you think there would be a reason for the AP to say no to a client request?

A: We need to think about it, this is good question.

Q: in case of rejection, how can we indicate another MAC address?

A: Since the client is already registered, we can have an encrypted frame exchange to indicate MAC address change, or propose a new one in case of rejection by the AP.

Q: I agree we need flexible operation and the proposed change goes in this direction. Considering the soft transition do you have a conclusion on that?

A: This is something that still need further discussion.

C: In another contribution (1148r0) scheduled after this one, we will discuss around the need for a soft transition.

C: In general, in this transition, we see lots of value in a station initiating the change and selecting most of its CPE parameters, and in automated change of most of its parameter at once. For some parameters like AID that are difficult to decide by client, AP will provide.

No more question

**6.2** **RCM follow up** **(11-23/1148r0),** Stephane Baron (Canon)

Q: Can’t we use the event of reception of frame addressed with new MAC address as trigger for the transition is any case?

A: This event can be used to start earlier the transition but we much have a constraint to avoid an attacker to make a station to change its MAC address by sending a frame to that STA address with a new MAC address at any point of time. So, indicating an instant after which the reception of a frame addressed with a new MAC is valid is necessary.

Q: do we need specific mechanism ? Can’t we let it implementation dependent?

A: We need to indicate in the standard when a given MAC address is valid to allow interop.

C: I think we just need a simple mechanism where the receiver needs to be flexible

A: Yes, I agree, and indeed this is what is explained on the presentation, the AP and STA are flexible from reception point of view allowing RA set with current and new MAC addresses, but is strict from emission point of view as describes in slide 8.

Q: On your slide 8, on the left side you indicate “RCM ready (n+1)” and on the left “RCM ready” only, what is the reason?

A: sorry, this is a typo, should be RCM ready (n+1) on both sides, I’ll fix it in further revision.

Q: I generally agree with the direction and I think we are inline if you suppress the n x TBTT on slide 7 for the transition duration. I think the duration is not predefined and should last as long as needed by the emitting station

A: I indicate a duration here to limit the time during which the station needs to maintain in memory two MAC addresses and associated CPE parameter set. I think we need to define when a station will free the memory. But I agree we can move the transition end time toward the end of the epoch.

Q: Your proposed solution, to me, looks like re-keying mechanism. I wonder if you need both margins, you just need to be flexible and allow using old and new for a while?

A: Both margins correspond to different needs for solving sync issues.

Q: In Slide 7 you indicate that MPDU can aggregate old and new frames, right?

A: On the contrary old and new MAC address shall not be mixed in a same TXOP to avoid easy correlation of the two MAC addresses.

C: ok I misunderstood the sentence.

Q: Your figure shows case where the non-AP STA is late, but I think the proposed margin mechanism cannot solve issues when the station is in advance.

A: In fact, the mechanism is symmetric, and both STA and AP implement the margin mechanism. So, if you consider on the figure the STA is late, you can see it as AP is in advance, even if we consider the AP as a reference. So, since AP also have this margin mechanism, if the STA is in advance, this is the AP margin that will solve the sync issue.

Q: I don’t see why you need those margins, why don’t just use a transition period allowing both addresses?

A: we have to be strict on emission and flexible in reception to solve synchro issues.

C: I think having a Timer is a bad idea. It is difficult to define good value.

A: Timer is a security mechanism to be sure the transition ends.

Q: Your proposal looks like re-keying, why do not reuse same mechanism?

A: I am not familiar with this mechanism, I will study it and come back later.

Q: Can’t we use a sliding window mechanism instead of your proposal, since you want to flush old packets, and time required to do that is not predictable.

A: A sliding window mandate AP and STA to be aware of the peer buffer status content to determine when to remove the MAC address for valid list.

Q: Why do you need margins; you already have a transition period to solve clock drift?

A: Transition is not dedicated to the clock drift, but rather flush buffers those are two different problems

Q: Why indicating the usage of old parameters on slide 7?

A: In this slide it means that a MAC address is linked to its parameters, you cannot mix. So, when using Old MAC address, you have to use old parameters.

C: Understood. It would be better to add this in your document.

Q: What about the triggering, and the AID value?

A: You mean the AID used in the trigger frame, right? The AP will use the new AID parameter as soon as the transition period will start.

Q: But how can a station answer a trigger frame with new AID, using prepared old frames.

A: When receiving a trigger frame, the sent frame in UL is not prepared in advance because the STA cannot know the allocated size. The non-AP STA will then prepare a new frame with MAC address and params corresponding to the received AID.

No more question, SPs are deferred.

**6.3 Proposed spec texts for probe request (23-11/1079r0)**, Po-Kai Huang (Intel)

Propose to solve requirements (Req3 and Req20) linked to the obfuscation of the probe request frames, and especially to the set of IEs sent in those frames.

C: Concerning the DSSS rate and 2.4 GHz, I think we have to get ride of it. We already spend a lot of time without finding any consensus on this subject.

A: You know this is mandatory, but I put it as a should. I think this requirement should be moved to REvme that is a more suitable place to take this action.

Q: This solution does only come for OFDMA is reasonable

A: ok I hear you

Q: Concerning the data rate, up to 24 is mandatory in the spec.

A: up to 24 is mandatory but you can indicate more.

C: this info is already in the standard.

A: but you have to indicate the way you support it.

C: I put a list of parameters you can drop or not.

A: I disagree with this list.

Q: chapter 35.3.4.5: do we cover the case where a station does not support EDP extension?

A: AP requirement should be the same.

C: You mean I have to rewrite a whole paragraph with single SSID only AP?

C: ok, I will revise according to the received feedback.

Q: according to the propose rule, does it mean that an AP will reject the probe request, if the list of IEs is not correct?

A: In the spec there is not lot of case when you do not answer to probe request, I just propose to create a list.

Q: if you’re EDP STA and connect to EDP AP, does the EDP AP may omit the supportive rate?

A: All these functionalities are optional, even if there is no EDP around the STA should be able to connect.

C: But we should have a rule where the client omits parameters.

A: The EDP AP should support removing parameters when answering probe omitting params.

Q: what does a Station should indicate if it supports 11bi? You say that indicates the non-AP to do this to reduce it finger print.

A: You didn’t need to indicate that in your probe request.

C: The non ap STA may have two intentions when sending probe request: connect to an EDP or to a non EDP. In that case the client may indicate all params.

Po kai will revise according to the received comments.

SP is deferred.

**6.4 Next meeting reminder**

The Chair reminds next meeting date and time: PM2 tomorrow.

**6.5** AOB:

no other business.

Chair recess at 15:25 local time.

**2nd slot. Tuesday 11 July 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Jay Yang acting secretary for this meeting**

**Vice-chairs: Jerome Henry, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

Chair calls meeting to order at 10:02 ET.

**Agenda slide deck**: [11-23/1001r2](https://mentor.ieee.org/802.11/dcn/23/11-23-1001-02-00bi-july-plenary-agenda.pptx)

1. Reminder to do attendance
2. Review of policies and procedures.

IEEE individual process slides were presented.

1. The chair mentioned the call for essential patents

No one responded to the call for essential patents

1. The chair covered the IEEE copyright and participation rules.

No questions

1. **Discussion of agenda 11-23-1001r2**

Adoption of agenda by unanimous consent (25 participants on-line, 10 participants in the room).

1. **Administrative**
	1. Need a secretary for today’s call and next week’s sessions
		* Jay Yang to cover today’s call

**13 Technical Presentations**

**13.1 23-11/1160r0-proposed-spec-for-encrypting-(re)association – Po-Kai**

Q&A:

C: I feel confused on RCM binding DS mapping, if the STA doesn’t associate to the AP, there is no mapping between DS and the RCM.

A: I’m saying here only in BSS transition, before BSS transition, you already have an old one, during BSS transition, you should use authentication, DS should map to the new one. It’s not just FT, in FT, yes.

C: the key is not over the air in authentication, how to find the key to decode the association frame

A: first, you will do the authentication, after authentication, you have the key,

C: first question is RSNXE, there is a lot of requirements, for each requirement, we put the support bit in the RSNXE capability, it becomes bigger and bigger in RSNXE.e.g. in your previous contribution, you also use RSNXE capability.

A: RSNXE procedure is well defined in the following authentication/association steps. If we use

 extra element, we need to define the corresponding procedure everywhere.

C: RSNE/RSN a good place, how about to define extra privacy element for 11bi

A: at the beginning, I also propose the define a new field, the problem is how much reserved bits we define in this field, it still has some limitation to extend it in the future.

C: 12.13.X.1 non-MLO part, the third paragraph, last sentence, “EDP non-AP STA.... 12.5.4. GCM”, but non-AP chooses the cipher suite according to the 802.11me.

A: the proposed text said "After ...during the Authentication frame exchange", indicate the non-AP STA choose and use the cipher suite, yes, you need the cipher suite as you need to know the key size in Authentication frame.

C: the ideas here is that decides the cipher suite in the authentication frame exchange, and use the same cipher suite in the association frame exchange

A: Yes, you need to know the key size before decrypt it.

C: cipher suite may be not GCMP, CCMP, need to check, and same stuff in MLO case.

A: suppose its CCMP, GCMP, offline talk it.

C: use a RCM, how the AP decrypt it

A: the STA in authentication procedure to use new MAC, and the following association also use such MAC.

C: how to handle the AAD?

A: for the non-MLO case, use A1, A2, no problem.

C: how to handle the subsequent data frame?

A: all things rely on how we define. at this point, all encryption/decryption rely on MLD MAC address. Usually, the MLD MAC address is not exposed.

C: non-MLO may be not working, RCM is exchanged over the air, as the RCM is used to retrieve the PTK. While MLD can handle such case.

A: let's me think about it. for MLO, no problem, as MLO address always the same.

C: there is no sentence to describe the MIC,

A: there are same as PMF in GCMP, CCMP, like AAD, there are addressed in there, I just add two frames.

C: in 9.4.2 the MLO and non-MLO case put together.

A: I can split up the non-MLO from MLO case in two paragraphs if the group agrees on this direction.

**13.2 23-11/0214r0 - Proposed text for MAC Privacy section – Carol**

C: do you have any definition on EDP

A: not yet,

C: a lot of things can be enabling over the air. In general description, I think we don’t list all of them.

A: agree.

C: you only talk management frame, data frame. control frame also be impacted.

A: try to make it more general, delete the frame list

C: why put the MLO and non-MLO case together? While in other contribution, the case is separated in different paragraph.

A: put MLO separately because there is a lot of procedure in that part. In general part, I think it's OK.

C: no strong opinion to add this NOTE in sub clause 9.2.4.3.1, suggest change to "OTA" MAC address in the note.

A: OK.

C: confuse to change the OTA MAC address, the note is hard to understand.

A: this is the first time I present this, I will reword it.

C: RA or TA is RCM in the NOTE in last paragraph?

A: RA can be randomized, so I say it’s may.

C: the proposal to modify the MAC address, and then you add the note RA/TA may be randomized in the OTA, maybe not.

A: I understand your point. and add a new note that "this assumes viewing OTA contents versus within/after processing”, I will think about, may be something need to be separated, like EDP.

A: thanks everyone, I will get it back again. Especially on the green text.

**13.3 23-11/1147r0 – Obfuscation Computation Procedure - Julien**

C: the value N used in anyway, I feel confused. Or it’s used now or future?

A: the value N is the current value, N use to calculate the next value, like SN, PN, etc.

C: suppose you don’t use N directly, e.g., if N is 15, you don’t use 15 anywhere.

A: it’s just the previous value.

C: slide 7, if the attacker is very closed to the authenticator, it may be captured the frame, and get PTK as the seed.

A: use PTK should be OK. Just try the cover unassociated client. It’s more simplicity

C: SN is already designed in baseline, don’t need to extension every time.

A: Offline talk.

Q&A to continue next call.

SP#1--defer to next call.

**13.4 AoB**

* 1. No other business.
1. Chair adjourned the meeting at 12:00 ET.

**3rd slot. Wednesday 12 July 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron acting secretary for this meeting**

**Vice-chairs: Jerome Henry, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

Chair calls meeting to order at 13:32 local time.

Agenda slide deck: [11-23-1001r4](https://mentor.ieee.org/802.11/dcn/23/11-23-1001-04-00bi-july-plenary-agenda.pptx):

Chair calls meeting to order at 16:02 local time.

1. Reminder to do attendance.

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. The chair mentioned the call for essential patents

No one responded to the call for essential patents

1. The chair covered the IEEE copyright and participation rules.

**18** Need a secretary or secretaries for this session

Stephane to take notes on this meeting

1. Remaining Meetings:

Thursday PM1

1. 10 people in the room 22 connected via webex

**20 Technical presentations :**

**20.1 Obfuscation Computation Procedure** (23-11/1147r0) – Julien Sevin (Canon)

Julien briefly reminds his presentation slides presented yesterday.

Presentation shows a method to generate at once a set of CPE parameters using only one PRF call.

Questions:

Q: Your obfuscation apply to different parameters including the AID, can you explain how to do that ?

A: in previous contribution we have a mechanism to generate the AID and in case of collision we have a frame for the AP the provide it. Close to 11bh discussion this morning, if there is a collision, we use a frame to solve the collision.

A: 11-23/0336r0 describes a proposal for a STA to compute its future AID value randomly. If the AP detects a collision, it sends a new AID using a dedicated protected frame. This proposed solution also includes sending the range values of the valid AID for a STA among which the STA selects the AID.

C: for the MAC we can have the same collision issue. No solution is perfect we need some solution to protect.

C: we do not need to do anything on the scrambler seed. For AID I think it is better that the AP provide. For SMAC, DMAC this is a separated discussion.

A: I made a list based on previous contributions, but I agree that we can discus on some params like scrambler seed.

C: we have requirement 9 that requires to obfuscate the scrambler seed, but if the solution is to do nothing since this is already in the spec, this is OK.

Author ask to run the SP#1

SP#1 initial text:“Do you support the computation procedure used to obfuscate the values of CPE parameters as described at slide 6

A: Yes

B: No

C: Abstain

D: would more information”

Question on SP:

Q: SP refers to slide 6 or do you want to make it more generalized, because slide 6 includes many details.

A: The idea of slide 6 is to have computation of several CPU parameters.

Q: slide 6 lists a lot of parameters can we have something more high level?

C: proposal to just indicate “exact list of CPE parameters is TBD”

Q: a more generic wording is proposed that do not mention slide 6, but keep the main idea.

C: as far as this new formulation is not prohibiting other inputs, I am fine.

SP is run with Final SP#1 text:

“Do you support the use of a single PRF to generate new CPE parameters with inputs such as the current OTA MAC address and a shared private key?”

A: Yes

B: No

C: Abstain

D: would more information”

SP result: 8 Yes:8, No:0, Abstain:3; Would more information:7

**21 Change of agenda: presentation order**

Chair ask if the presentations 11-23/1246r0 and 11-23/0416r1 are linked and should be presented together.

Author of those contributions indicates no preference and let the chair decide.

Considering remaining time in this session, the order of presentations is changed:

first 11-23/1216r0 then if time permits 11-23/1246r0 and 11-23/0416r1.

**22 Technical presentations**

**22.1 TID Obfuscation Discussion** (23-11/1216r0), Carol Ansley (Cox)

Presenter presents document 1216r0 sharing some though around the need to obfuscate TIDs not only in MAC header but also in other usage of the TIDs.

This would end up with a change of the requirements and require a motion for that to move TID

Questions:

Q: You touch a tricky point: traffic analysis. If you use other analysis like packet size or other you can track station. So even is TIDs are a small set of values, those are very important, like value 6. So, I prefer to obfuscate TIDs over the air as stated in previous presentation by Julien.

A: yes, but what about the other place it is used? do we obfuscate it everywhere?

A: yes, I think this a key point is to make it obfuscated everywhere.

C: I think TID appears also in some non-encrypted frames

A: Let me check that offline.

Q: It is easy to fingerprint the traffic, so we need to obfuscate not only the header. I think this is an “all or nothing” processing required here.

A: agree

C: If we can encrypt a frame like SCS, that would be preferred to obfuscation. For TID there is a real time requirement making it more complex so obfuscated the field in mac header is a way forward.

C: I would suggest to extrapolate and have no parameters in clear that allow fingerprinting and so tracking.

Presenter decided not to run the straw poll but indicated that this type of procedure needs to be carefully considered especially if we have a lot of stations. In that case analyzing the TIDs in the traffic is complex.

**22.2 Proposal for sliding window MAC address rotation** (23-11/1246r0) - Antonio de la Oliva (InterDigital, UC3M)

Presenter presents document 11-23/1246r0 indicating this has been discussed by several people involved in 11bi from various affiliations.

The document provides a soft approach for the MAC address transition.

Questions:

Q: I think this a good direction. Just a clarification: what stations perform transition?

A: the transition is for all the stations.

Q: When can I flush my old packet?

A: I discuss that with people and this can happen at a given time but this is implementation dependent.

C: Thank you, this is like what I have in mind. I support having a timer that guaranty we have an end of transition. We need to define this value to make sure this transition is as short as possible.

C: Agree the direction. Only worry about power saving clients. I support flexible approach since it is difficult to define correct timer value due to unpredictable traffic.

C: There is another presentation 11\_23/1272r0, to be presented, addressing similar topic and allowing a STA to indicate that the buffer is empty of old frames.

Author requested to run an SP.

Original text of the SP :” Do you agree on working on a solution considering a sliding window of 2 MAC Addresses for Rx and Tx?”

Questions on the SP:

Q: sliding window seems to indicate this is a fixed rate?

A: no

Q: What does this figure shows us? do you separate TID?

A: no, this figure shows packets without specifying the TID.

Q; What happened during transition period for new packets ?

A: everything that is new is addressed with new MAC.

C: Proposal to add “for each STA” at the end of the SP.

A: agree.

Q: What sliding window means? can we just indicate a window ?

A: agree

Q: Can we indicate “work on a solution indicating a window of time where two MAC addresses are valid?”

A: Agree.

Q: In a transition time we have 3 MAC addresses, handled differently (previous, current, and next one)

A: We have only 2 MAC addresses in the A1 filtering.

Q: can we indicate old and new MAC in the SP

A: agree

SP is amended according to previous questions and comments.

SP text : “Do you agree on working on a solution for MAC address changing in which a STA has an old and a new MAC address valid for a window of time?

A: Y

B: No

C: Abstain

**SP result** Y: 14, N: 0, Abstain: 5

Author indicated he will update the presentation with the SP result.

22.3 CCMP MLO MAC rotation (11-23/0416r1), Antonio de la Oliva (InterDigital, UC3M)

Presenter presents document 11-23/0416r1 indicating the rotation of MAC address for MLO or non MLO

Presenter indicated another contribution 11-23/0850r0 that contains a text for this proposed solution

Presenter then switch to 11-23/0850r0 presentations to quicky remind its content.

Questions:

C: I think IRM solution is reasonable to integrate in 11bi, but IRM is scenario specific. So I think this is better to make it optional.

A: I don’t say anything is mandatory, I just say both solutions may exist.

C: You say IRM MAC is the same as DS MAC, but one is in clear and used during association, and the other is not in clear, so I think those are different.

C: For MLO and CCMP we have to secure the MLD MAC Address

A: Agree but for non MLO we can rely on CCMP encapsulation and decapsulation.

Q: We will end up by generating 4 different alternatives for architecture (protected/non protected for MLD/non MLD). This is why I think this is better not to have legacy mode in the game.

A: agree, but I am talking about new stations that are not MLO by using the same CCMP block to reduce complexity.

Q: We were talking deriving key from the MLD MAC address, but now replacing by the DS address?

A: what I say is that for the CCMP, the encryption is the one associated to the DS MAC that provide a single architecture.

Q: I am worry we are breaking something in the security machine and requesting expert in security to check

A: I am not changing anything. You generate the key as before, and then just using the DS MAC in the CCMP instead of the OTA MAC.

Q: We need to use the same MAC address for encryption and decryption, right?

A: Right, this is what we are doing here.

C: I think this is good to have DS MAC and MLD addresses different only if we go with the wifi7 architecture.

A: If we do not something as it is presented, we have to touch the CCMP because otherwise it will not work. We cannot do nothing.

C: I need more time to think about it when we have wifi 7 and legacy devices on the field. I am just worried about mixture of 11bi and legacy STAs.

A: legacy will not implement bi. We can have single link bi and using the proposed mechanism with no issue.

C: Instead of considering the OTA MAC for encryption/decryption, we use the DS MAC address and it works. I don’t see what can fail here, nothing is new.

A: side 6 : IRM is transmitted in clear in next association, but DS should never be transmitted in clear, this is why I think there is no relation.

C: I wonder how a legacy device will communicate with an EDP AP ? Maybe it is probably best to have different scheme for wifi 7 and Wifi 8 stations.

Q: So what you mean by legacy stations?

A: I never mention legacy stations. Wifi 7 will use the same algorithm, I don’t understand.

A: you answer my questions but I think to see if this possible or not from an implementation point of view.

C: I have to remind that the OTA MAC address will change and we need a partition between OTA MAC and DS MAC

Q: If you use DS\_MAC in AAD, that implies you shall use DS\_MAC in authentication and association, which violates the requirements for DS\_MAC.

A: the key we use is the one attached to the DS MAC. Not the DS MAC itself.

C: it works for MLD case

A; agree and I am just saying we should reuse if for non MLD.

C: Let people sleep on it and come back. I think the direction is good and of course we need to carefully consider details not to break security.

C: If you come back please clarify this is for non MLO since for MLO it is already there

A: agree

SP is modified accordingly and will be run tomorrow.

**23 Future sessions schedule**

Chair indicates we need to discuss tomorrow for the future sessions scheduling.

**24 Chair indicate Recess at 17:59**

**4th slot. Thursday 12 July 2023, 13:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stephane Baron, Canon**

**Vice-chairs: Jerome Henry, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

Chair calls meeting to order at 13:33 local time.

Agenda slide deck: [11-23-1001r5](https://mentor.ieee.org/802.11/dcn/23/11-23-1001-05-00bi-july-plenary-agenda.pptx):

Chair calls meeting to order at 16:02 local time.

1. **Reminder to do attendance**.

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. **The chair mentioned the call for essential patents**

No one responded to the call for essential patents

1. **The chair covered the IEEE copyright and participation rules**.
2. **Agenda approval**:

Agenda approved with unanimous consent (19 people 9 in the room)

**29 Motion to confirm secretary position**

Motion #32

Approve the appointment of Stephane Baron to the position of Task Group secretary for TGbi

Mover: Steve Rodriguez

Second: Jay Yang

Approved by unanimous consent, (22 on-line and 10 local).

**30 Teleconference discussion**:

Maintain TGbi teleconference with previous schedule: Every other Thursday 10am EDT

No opposition to maintain same schedule.

**31 Technical presentations**

31.1 MAC Transition Discussion (11-23/1272r0) – Carol Ansley (Cox)

In the scope of a MAC address change, proposal to have a mechanism to track the end of flush of the queue from Frame addressed with an old MAC address. The proposal is to send a frame to indicate the old buffer is empty. That frame would generally avoid the need for a timer.

Discussion:

Q: slide 5 : I am concerned. Some implementations cannot indicate to upper layers that buffer is exhausted. So how can trigger frame emission? How can we check that the buffer is empty?

A: agree that additional mechanism may be required.

Q: Here you assume that there is an existing mechanism that allows checking the queue contains for each 4 ACs and for old and new packets rights?

A: yes.

C: Your packets are injected in the queue and with 4 queues it is difficult for the system to maintain those different counters.

C: about the frame that is transmitted to indicate the end of the transition: you can infer the end of the change of the MAC since the frame may have a recognizable size of whatever.

A: this needs to be a protected frame, that may include padding or something to make it hidden.

C: If I have a lot of STA, I need a timer to be sure that after a period of time all my client are done.

Q: Slide 6 : about SMAC , DMAC : the complexity is increasing, and I feel uncomfortable to multiply the number of params. We can exhaust resources for instance, 4 AID per client are necessary, and it becomes too much. So, I think only old and new MAC is enough.

A: thank you. I agree with that concern.

C: We search for more privacy; we have to pay an additional price and we need to consider the tradeoff.

C: I think this is a different discussion for SMAC, DMAC. For the rest I pretty agree, this is aligned with what was presented yesterday. since you propose sending a frame instead of a timer.

C: I have concern with the transmission of frames at the end, since we may end up with a lot of simultaneous transmission.

A: agree

C: in addition, you leak the end of the transmission and can allow tracking for instance station having long process to empty their queue.

A: agree, but timer is also an issue

C: hiding the start and stop of transition depends on the number of STA in the BSS, few station easy to detect anyway, lots of station, don’t need to hide because difficult to track.

A: using traffic analysis with AI are pretty good to fingerprint station.

C: we need to consider the lifetime of the MSDU as an element to determine the end of the Old Packet queue.

A: this type of mechanism is implementation specific.

**32 Discussion on document 23-11/0892r1: requirements and tracking issue**

Chair briefly introduce the content of this new document, to be used to keep track on our progress.

C: I don’t think we have concrete progress to indicate in this document.

A: There is just an update of “still open” for some open topics we discussed this week.

Table: 3 elements updated on the fly

C: On the AID part (element 2), I think there are discussion on the AID generation (AP, or STA generated). Please clarify that the discussion is still open

Q: Can we have an element about BPE and CPE be MLD compliant or not to reflect the discussion we had in the week?

A: Agree. A 5th element added in the table for that purpose.

Q: I don’t fully understand the text in this new line

A: this is just a reminder.

Q: what is the relation with first element? I want to verify that our baseline is MLD only on non MLD or above.

A: I don’t think we address one or another in the PAR.

C: the purpose of this table is to track open subjects.

Q: Does anyone has additional subjects to add? If you think of something after today’s session, email me to upgrade the document.

A: No answer.

C: To keep track, we should have a tag tracking progress based on proposed submission and the status (SP, motion).

C: There is already some items that can enter this category.

C: Over the next couple of months, I would like to create draft D0.1, and this table may help marking some progress.

C: My understanding is that we already tracked it thanks to the requirement document. I think our goal is to solve requirements, and we need to know how many we are covering: all, or part of it.

A: This is why I let the requirements table in the document. Both tables are handling different aspects and people will use both tables.

C: It should be good to say D1.0 covers X requirements and D2.0 covers Y requirements to show progress.

A: I can add a column to indicate the requirements addressed in the Text submission section.

C; proposal to just add a title “information” to indicate the section addressed (introduction, or requirements).

C: First entry addressed by doc 1214 should be “introduction for all requirements”

Author to generate an r2 according to the received comments

**33 Back to the agenda,**

 the agenda is exhausted.

1. **AoB**

 No other business.

1. **Chair adjourned the meeting at 14:35 local time**