IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Minutes Mixed Mode Plenary Sessions 2023  13-17 November 2023 | | | | |
| Date: 2023-11-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stéphane Baron | Canon | Cesson-Sévigné, France |  | [Stephane.baron](mailto:Stephane.baron)@crf.canon.fr |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meetings that took place during the IEEE 802.11 Mixed Mode Plenary session 13-17 November 2023. The on-site location for the meeting was Honolulu, USA.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**1rst slot : Monday November 13th 2023, 08:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 08:05 Local time.

Agenda slide deck: [11-23-1696r0](https://mentor.ieee.org/802.11/dcn/23/11-23-1696-00-00bi-november-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

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

1. Review of policies and procedures.
   1. IEEE individual process slides were presented.
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 policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-23-1696r0 (slide #15)**
   1. Discussion on agenda

No discussion

* 1. Adoption of agenda by unanimous consent (29 participants, 16 in the room).

1. **Administrative**
   1. Approval of Telecon minutes and Plenary session minutes – Motion #34

Discussion:

A: since we are in ad-hoc session so we cannot have motion

A: ok we will come back to this tomorrow.

Motion to be run during next meeting slot.

* 1. Remaining Meetings:
* Tuesday PM2
* Wednesday PM2
* Thursday PM1

1. **Technical Submissions**
   1. [11-23/1147r1](https://mentor.ieee.org/802.11/dcn/23/11-23-1147-01-00bi-obfuscation-computation-procedure.pptx) – Obfuscation computation procedure: Julien

Presented by Julien.

Follow up of the obfuscation procedure for the CPE parameters.

The objective is to precise the parameters to be obfuscated and associated procedure for the generation of each of them.

* + 1. Questions:

Q: You mention a temporal reference in your presentation. Is it the TSF?

A: It can be other reference but TSF is one possibility. The point is to have a changing value that can be known by the AP and the station.

Q; On the first straw poll: it seems obvious to limit the number of calls, so why asking for it?

A: Because some contributions may propose different mechanisms for each parameter and create additional computation overhead.

Q: What is the difference between reset and mask?

A: Mask based mechanism is to keep data continuity while reset completely reset the data. For reset based mechanism, the internal data is changed.

C: If it is a static mask, it will not improve privacy of our link since this can be determine.

A: The mask is static but only for one Epoch. This provides protection across epoch but we can still track within one Epoch.

C: This will force to have very small epoch to have a guaranty of privacy.

A: I agree.

Q: for SP 2: do you mean that we use different offset for different link?

A; yes, you are right.

C: if we agree on having an offset, it would be better to indicate “offset” in your SP text. But I am ok with current wording.

Q: for SP 1: I am not sure we can generate AID so I would like to remove AID from the SP.

A: OK, I understand, So You prefer to have an AID computed in another way.

Q: you are just adding a derived value to the PN right? So, you are not stopping the tracking.

A: The idea is to generate a random mask that obfuscate the SN and PN during transition from one Epoch to another.

C: Changing the PN is dangerous with regard to encryption, so unless we solve a real problem, we shouldn’t change PN.

A: The PN sequence is used to identify client so we need to obfuscate it. This is important when we apply the obfuscation procedure to recover the PN for instance to keep continuity, but as other CPE parameters, we also have to obfuscate it.

Q: In slide 5, we can compute the encryption in many different ways. Not sure the PRF you describe is implemented.

A: This mechanism is already implemented to generate the cryptographic key. It is a good candidate because we know the performance of this algorithm, but I am open to have other standardized algorithm to allow a same computation on both AP and STA side.

A: let’s take it offline

C: I think we should add the usage of those parameters to future revision of this contribution, not only how to compute it.

A: yes, thank you for the advice.

Q: I think for instance, that we can also mask the scrambler seed. Can you remind me the difference between reset a and mask?

A: mask obfuscate but internal value remains the same while a reset changes internal value.

Q: I think AID will collide easily with this proposal, so let’s continue discussing to find a robust mechanism

A: ok.

Q: For the MAC address the possibility of duplication is rare but exists, so how do you deal with that?

A: Some previous contribution presented a mechanism to deal with the duplication (for instance 11-23/0336r1). The AP knows that there will be a collision and indicate to the station to change its colliding address. Such message exchange will be very rare.

C: I’d like to bring clarification on previous questions. There is another contribution (11-23/1883r0) scheduled for tomorrow that explain why using a temporal reference as changing parameter of the PRF is a good idea. So, let’s discuss this point after this presentation.

C: Concerning the obfuscation, we already discussed in the group that tracking will be possible within an Epoch, but not across Epoch.

C: This presentation is an extension from single link to multi-link, and this is ok. But I have a concern on the general approach. I think that each parameter should be handled separately, and more details are needed on how to apply those parameter values. In addition, all station changing at the same time gives a pointer so those are general concerns on the mechanism.

A: this contribution is just saying it is a good think to compute all parameters at once, but you are right that the way to obfuscate this parameter (how to apply mask) is not described here. Here we are not dealing with how or when to apply the new values.

Q: On slide 8: An MLD can have more than 2 affiliated STA, even if what you present is just an example, I think we have to consider having more links that we can compute in one call to the PRF.

A: Yes, we can have more than 2 links and need more computed bits. So, in that case, we may have to run several calls. Currently the biggest PRF generation is more than 2000 bits. This is high, but if we go upper than this limit, we will have to increase the number of calls.

C: To obfuscate the SN and PN, it should be easier to change the value since the station should already be able to do it.

Q: Are you going to propose a per link AID?

A: No, AID will be at MLD level.

Q: So, if we use AID at MLD level, why do we use SN and PN per link?

A: good point

C: CPE parameters should change but we need more details. Since this contribution covers several requirements, more discussion is necessary. We also need to consider extension for mass rotation for instance.

Author then requested to run 2 straw polls.

**SP#1** requested by Julien:

**SP#1 initial text**: “*Do you support that MLD Level Parameters and Link Level Parameters are generated with a single execution of a standardized PRF?*”

Y / N / A: / need more info:

Discussion:

Q: we discussed that some parameters may be difficult to generate with others, can you consider reducing the scope of the SP?

A: this is just a SP; we can run it like that.

**SP#1 results:** 10Y / 10N / 6A / 5 need more info / 4 no answer

**SP#2**: requested by Julien

**SP#2: initial text**: “*Do you support a per-link mask-based obfuscation procedure for SN, PN and TID?*”

Discussion:

C: I think we don’t need SN / PN since we have a MLD AID, this is why I will vote no but I understand you want to gather opinion.

C: I think this is a good choice to have this per link parameters and we can find solution to raised issue like AID.

**SP#2 results**: 11Y/ 11N/ 2A/ 8 need more info / 4 no answer

* 1. [11-23/2049r0](https://mentor.ieee.org/802.11/dcn/23/11-23-2049-00-00bi-a1-filtering-spec-text.docx) -- A1 filtering spec text -- Antonio

Presentation made by Antonio.

The contribution also contains MIB element to deal with the EDP and especially the list of MAC addresses used for reception.

* + 1. Discussion

Q: I just want to avoid confusion that we are not changing inside the MSDU. The only thing we want to change is the address field. So please consider my proposed text:

“*In case of an EP (Enhanced Privacy) STA, using Frame Anonymization (FA), address filtering on the Address 1 field in each individually addressed MPDU contained in a PPDU is performed by comparing the value of the Address 1 field to all values in the dot11RxAddressesTable*.”

C: I think we should indicate “in addition” instead of “In case of” to avoid adding confusion, right?

A: OK.

Q: Can we just say TBD value in the table because we did not converge on the number of MAC addresses per STA.

A: This table supports whatever number so I think this is OK.

C: I think TBD address this point.

Q: Procedural question: Can we add “TBD” and come back later?

A: (technical editor) Yes, we can do that: keep a “TBD” for D0.1 and we will have to remove any TBD for D1.0.

Q: Clarification question: Let say the group decides to use only one new MAC address and one old, so the table will contain 2 entries during transition period and then after, only one address?

A: yes.

Author to clean it and come back with a new revision

Chair reminds next meeting tomorrow PM2.

1. Chair adjourned the meeting at 09:39 EDT

**2nd slot: Tuesday November 14th 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 16:05 Local time.

Agenda slide deck: [11-23-1696r2](https://mentor.ieee.org/802.11/dcn/23/11-23-1696-02-00bi-november-plenary-agenda-tgbi.pptx):

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. Review of policies and procedures.

IEEE individual process slides were presented.

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

No questions

1. **Discussion of agenda 11-23-1696r2 (slide #15)**
   1. Discussion on agenda

Document 23/1982r0 is deferred to tomorrow.

* 1. Adoption of agenda by unanimous consent (18 participants, 9 in the room).

1. **Administrative**
   1. Approval of Telecon minutes and Plenary session minutes – Motion #34
      1. Approved by unanimous consent (17 online, 9 in the room)
   2. Remaining Meetings:

* Wednesday PM2
* Thursday PM1

1. **Technical Submissions**
   1. [11-23/1983r0](https://mentor.ieee.org/802.11/dcn/23/11-23-1983-00-00bi-epoch-start-time-setting.pptx) – Epoch Start Time Setting: Stéphane.

Presented by Stéphane.

Contribution proposes a solution to handle both group and Individual pseudo recurrent Epoch start time and computation of CPE parameters based on a time reference.

* + 1. Questions:

Q: Is this pseudo random variation really needed since station will not immediately send data at epoch start time, but rather when they will have data to transmit.

A: Statistically, in a crowded environment, station will have data queued waiting for transmission, so it is likely that the first transmission with a new MAC will occur immediately after the Epoch start time. So, to make thing more difficult to eavesdropper to determine start time of the Epoch, a pseudo random variation is required.

Q: For group variation, I don’t see a big interest since a lot of STA will change at the same time, so it is easy to determine starting time.

C: For individual it is more interesting to hide the starting time so in that case a randomization may be useful.

Q: If it is a constant random, I think this can be easily determined by eavesdropper.

A: in this contribution, the variation is computed at each epoch so the variation changes at each epoch

Q: Do you consider changing the duration of the epoch rather than the starting time?

A: I think those are two sides of the same coin, since epoch are one after the other, so if you change randomly the starting time, you change the duration, and vice versa.

C: ok, but let consider the random duration as an alternative to the starting time duration

C: Maybe we should close first if it is important to hide or not the rotation boundary, and if having synced rotation helps or not on hiding the identity.

A: ok I will prepare a SP to close this question.

C: concerning SP 2: There is an issue related to the AID if you change per link, because today the AID is at MLD level. We can also consider changing some links together.

C: The traffic may be different per link, so the instant of change may not be suitable for every links at the same time.

C: we learnt from 11be that it is difficult to synchronize things among different links.

C: Concerning the SP#2 related to time, I think time is good since it is important for a STA to be prepared for change and it is easily synchronized.

Q: When do you plan to run those SPs?

A: on Thursday

* 1. [11-23/0031r4](file:///\\nas-1\project\VSDN\Standard\802.11bi\Secretary\Proposed%20spec%20texts%20for%20802.1X%20authentication%20utilizing%20authentication%20frame) – Proposed spec texts for 802.1X authentication utilizing authentication frame: Po-kai Huang.
     1. Questions

Q: on field 10 – 11 page 3 : About the authentication frame body: do you put encapsulation in an IE?

A: no in this document, I put it in a field.

SP #1 requested by chair:

“Does anyone as any objection to direct technical editor to add the text of 31r4 into our baseline?”

* + 1. Discussion on SP #1:

Q:is it a motion?

A: this is a SP. We used SP to add material to our future draft, we will have a motion once the document will be populated.

SP#1 received no objection.

* 1. [1664r0](https://mentor.ieee.org/802.11/dcn/23/11-23-1664-00-00bi-proposed-spec-texts-for-pmkid-requirement.docx) -- Proposed spec texts for PMKID requirement Po-kai Huang.
     1. Discussion

PMK caching will likely goes with RCM

Q: In which frame is transmitted the PMKId?

A: it has to be in authentication frame.

Q: you say “shall randomized MAC address”. This is not during Assoc, but before right ?

A: Right.

Q: PMKID is sent in RSNE IE, in Assoc or Authentication frame, or during the 4-way handshake. So, the ID is good. But you need to use random MAC.

A: Right but if you don’t change your MAC why do we need to change the PMKID?

C: It is more like a 11bh random MAC that is different from the 11bi.

A: I see your point, and yes, we can discuss how to generate it.

C: Protection of association has nothing to see with RCM.

C:I think we may change the wording to avoid mentioning the randomization. Rather use a different MAC address.

Q: while indicating is confusing. We should use applying pmk caching.

A:ok I see

C:I think we don’t need to mandate if the MAC address is not changing, so, we rather need to write a note with it .

A: ok the note is already there so we could remove the 2 first paragraphs.

Q: I see some value in those sentences and makes sense for an EDP station that you have to change your MAC address.

A: ok

C: “shall” language may be for deriving a new PMKID instead of shall change MAC address.

Author will come back with a new revision after offline discussion.

Chair reminds next meeting tomorrow PM2.

1. Chair adjourned the meeting at 17:58 EDT

**3rd slot : Wednesday November 15th 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 16:08 Local time.

Agenda slide deck: [11-23-1696r3](https://mentor.ieee.org/802.11/dcn/23/11-23-1696-03-00bi-november-plenary-agenda-tgbi.pptx):

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. Review of policies and procedures.

IEEE individual process slides were presented.

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

No questions

1. **Discussion of agenda 11-23-1696r3 (slide #15)**
   1. Discussion on agenda

No discussion

* 1. Adoption of agenda by unanimous consent (21 participants, 13 in the room).

1. **Administrative**
   1. Remaining Meetings:

Thursday PM1

1. **Technical Submissions**
   1. [11-23/1982](https://mentor.ieee.org/802.11/dcn/23/11-23-1982-00-00bi-epoch-group-management.pptx) -- EPOCH Group Management -- Patrice

Presented by Patrice.

Proposes to allow creation of several groups of stations for mass rotation to solve resource issues (especially AID limited resources)

* + 1. Discussion

Q: How many groups do you really want to have?

A: It depends on the number of STA and it can be implementation dependent.

Q: The AP provides the value, so the AP make sure that it doesn’t assign more than the available values. So, you always have the same issue?

A: having only one group double the number of required AIDs, and having few spare AID will drive the size of the group to a numerous small group.

Q: I think the epoch boundaries doesn’t make sense; you cannot force a station to send data.

A: I think we need a discussion on the mandatory versus not mandatory application of the new parameters after the Epoch boundary.

Q: In your mind, what is the Epoch duration?

A: I think it could be around 10 minutes. But, if you are multiplying the number of groups, you may have a reduced duration.

Q: what will drive the number of groups?

A: Mainly the number of stations.

Q: In this presentation, you indicate “Mass change”. So, all the STA will change at the same time. For individual, it is less likely that we will have the issue, right?

Q: yes.

Q: how does the AP decides which stations will belong to each group.

A: today I didn’t determine how an AP set groups.

C: I think we need to address this problem and you are in the right direction.

C: In this scenario the AP wants to coordinate the change of STA. But previous commenter says we should not force a station. I think the station can indicate the AP it will not follow the group. This can be a solution to the problem.

Chair ask for people to make a contribution to trigger the discussion on the mandatory versus non mandatory change of parameters.

Discussion then derived on AID aspects.

Q: why do we need to change the AID, why can’t we just obfuscate it?

A: you will have the same resource issue, because the number of bit to encode the AID is the same.

C: Agree about resource issue but changing the AID or obfuscate it is different.

A: AID is used in beacon while station is sleeping, if you obfuscate it in anyway, the STA and AP needs to be aware of that. I prefer to change the AID.

* 1. [11-23/2059r2](https://mentor.ieee.org/802.11/dcn/23/11-23-2059-02-00bi-epoch-definition.pptx) Epoch-definiton -- Stephen Rodriguez

Presented by Stephen

* + 1. Discussion

Q: I wonder for simplicity, why not setting everything to 5 minutes

A: I try to keep it open

Q: your value is upper bound. so can we say 5 minutes or less

A: yes, you can.

C: For security point of view the AP will have to keep track of the security status of the STA, why not indicating 5 minutes.

Q: Those numbers came from dictionary attacks, right?

A: yes

C: we have different approach for the frequency here to avoid tracking, not considering the security aspects. And we also have to take into account power consumption that is quite low, so we may end up with a more frequent change to cope with your constraints.

Q: can we consider those value as a recommended maximum value for the AP.

A: yes

Q:is it the station that says the AP about this value

A: yes.

Author then requested to run 2 straw polls.

**SP#1** requested by Stephen:

**SP#1 initial text**: “Would you support using AKM based/network trust level, for Epoch definition?”

Y / N / A: / need more info:

Discussion on SP#1 :

Q: If vote yes what does it mean?

A: This is how the AKM is used to set Epoch.

Q: Is it maximum duration or Epoch duration?

A: This would be the maximum duration of the Epoch.

C: I can support maximum value, but not definition of the Epoch using AKM. This is too restrictive to me.

C: Epoch cannot be defined by AKM, so can you change the wording

**SP#1 New text proposal**: “Would you agree to take into account the AKM when determining the epoch duration?”

Q: Can you elaborate on the sunset timer. Is it like the transition period?

A: yes

Q: You define it very precisely 5\*Dtim. Why that value?

A: we need to have a time to stop. Otherwise, an attacker can replay a message and listen who will answer to track it.

C: I don’t like this much, because if you consider the AP based on that, you do not consider station application needs.

Considering the discussion, author **defers its SP#1.**

* 1. [11-23/1818r4](https://mentor.ieee.org/802.11/dcn/23/11-23-1818-04-00bi-ota-mac-address-derivation.pptx) -- OTA Mac address derivation -- Stephen Rodriguez

Presented by Stephen.

* + 1. Discussion

C: I would recommend to read previous contribution since this has mainly be already proposed and we have much more parameter s.

Q:What is FTM

A: it is Fine Time measurement.

Q: what is relationship between FTM and TSF.

A: I am not sure.

C: In general FTM should be known by the AP and the STA.

Q: Is FTM mandatory in 802.11?

A: No, but I think here we are referring to TSF.

Q: for multiple MAC address changes, you can do it on one shot to reduce computation right?

A: yes

C: originally, I thought we can compute a set of param each time, but I can consider computing several sets in advance.

C: This is first time I see FTM in a key derivation.

C: I don’t think it makes a lot of sense to go thru FTM to generate a new value.

Q: What do you mean by validating?

A: The AP need to validate if we are out of sync for instance.

C: Not sure we need a kind of validation if we are confident in the new value generation.

A: this is also to avoid spoofing and determine that the sender is a bad actor.

C: I think this is better to use KDK rather than PMK. This is what KDK is made for.

A: ok.

No more questions.

* 1. [11-23/2049r1](https://mentor.ieee.org/802.11/dcn/23/11-23-2049-01-00bi-a1-filtering-spec-text.docx) -- A1 filtering spec text -- Antonio de la Oliva

Cleaned version of the r0 presented yesterday.

* + 1. Discussion

Q: What is the link with the change of MAC addresses?

A: This is the A1 filtering only.

Q: I don’t see the change here, since we always check A1?

A: in existing spec we have only one A1 MAC address, here we check against the content of a table.

Q: Do we have a rxtable today?

A: No, this is addition of the text.

Q: do you indicate how to add, or remove addresses? Or how many values is handled by the table?

A: No we do not have decided the mechanism yet, and the number of addresses is TBD.

C: I think we need more discussion on the mechanism.

A: agree, but this doesn’t preclude other text to define the mechanism.

No more question.

Author proposes to include that in the future 11bi spec text.

Chair ask if anybody is opposed to the inclusion.

Some members express their opposition.

Author request a SP on the inclusion of document 11-23/2049r1

**SP#1** requested by Antonio:

**SP#1 initial text** : “Do you approve adding the text in 2049r1 to the D0.1 Draft?”

Y / N / A:

Discussion:

Q: Do you want to add “need more info”

A: No.

C: This is a small section and you propose few words, so maybe you need the “need more info” choice

A: ok add this option.

C: I think we should have discussion on the maximum number of value and it should be 2. Otherwise, this opens the door to let say 10 MAC addresses.

A: This is why I add “TBD” for this value.

**SP#1 results:** 8Y / 5N / 6A / 1 need more info / 4 No answer

Chair reminds next meeting tomorrow PM1.

1. Chair adjourned the meeting at 17:57 EDT

**4th slot : Wednesday November 16th 2023, 13:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 16:08 Local time.

Agenda slide deck: [11-23-1696r4](https://mentor.ieee.org/802.11/dcn/23/11-23-1696-04-00bi-november-plenary-agenda-tgbi.pptx):

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. Review of policies and procedures.

IEEE individual process slides were presented.

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

No questions

1. **Discussion of agenda 11-23-1696r4 (slide #15)**
   1. Discussion on agenda

Potential contribution by Javier is deferred to allow offline discussion

* 1. Adoption of agenda by unanimous consent (19 participants, 13 in the room).

1. **Administrative**
   1. Teleconference plan

Proposed time: 10:00 ET

Proposed dates: 2023/11/30, 2023/12/7, 2023/12/14, 2024/1/4, and 2024/1/11.

1. **Technical Submissions**
   1. [11-23/2088r0](https://mentor.ieee.org/802.11/dcn/23/11-23-2088-00-00bi-analysis-simultaneous-mac-address-change.pptx) -- Analysis simultaneous MAC address change -- Antonio de la Oliva

Presented by Antonio

Contribution shows device profiling mechanism and indicates that the 11bi current scope will not overcome the profiling problem.

Proposal is rather to use several MAC addresses to transmit the streams.

* + 1. Discussion

C: Thank you for this interesting document. I agree that 11bi do not address the traffic profiling issue, but I am ok with that. I think we should focus on 11bi scope that is already quite large.

Q: Can we consider given advice on how to handle your traffic? Or Can we consider average packet size as a CPR param and randomize it a t MAC address change?

A: This is a possibility. Here I just want to highlight the fact that current 11bi direction can address this issue by using several MAC addresses.

Q: I agree we need to do something. For the moment we are focusing on device traffic, should we focus on traffic identification? This is an open question.

C: I think that increasing the number of MAC address may make things worse, since all MAC addresses are coming form the same physical location and create a fingerprint.

C: I do not promote to expand our scope significantly and rather complete correctly our current goal.

A: There are things that we can do for instance having several MAC addresses.

C: If you look at time of arrival or others, this will not change anything. And using several MAC addresses will some much more expensive that I do not recommend going that way.

C: You propose to change more MAC address, but the problem is still there since the traffic will looks like the same.

A: I am not proposing a solution but rather say that we may have things to consider like not changing all MAC address at the same time.

Q: The problem you raise is like extremely enhanced privacy. But I think if we go that way we will need to go to the physical layer as well.

A: everything we do has an impact on performance this is always a question of trad off

C: On a general perspective, when initiating our TIG, we worked on that, but it depends on how much money and energy an attacker put to track people.

C: We can propose mechanism to obfuscate packet size. But application can be more careful of it if they really want to hide

Q: Our scope is addressing privacy and not performance. Our task is to improve the privacy so we should take some time to study a little this problem.

C: We have a requirement document that list a set of thinks we could obfuscate in addition to the MAC address, and traffic profiling is something we should work on but probably keep it for the next 11bi generation. First focus on MAC and do a good job and we still have lot to do.

C: I think the amount of work to cope with this problem will prevent us to finish our work in our timeline. Currently we have a good compromise.

C: Multiple MAC addresses will open new type of attacks, so I am not sure this solves the problem, because you can profile this multiplicity of MAC addresses.

No more questions.

* 1. 11-23/1983r1 – Epoch start time setting – Stéphane Baron

Presented by Stéphane.

Stéphane presented the difference with revision R0 presented on Tuesday this week (mainly the added slide 13).

Presenter also briefly presented the different SP texts.

* + 1. Questions

C: Even if I agree on the general direction, I think we need time to run the SP.

A: Those SP are there to trigger discussion and find agreement on elements that needs to be decided in order to be able to draft a spec text.

A: I agree and to allow next contribution presentation I prefer to run the SP during next telecon to let people think on it.

Chair indicate she will schedule the SPs for the next teleconference.

* 1. 11-23/2098r0 -- Frame Anonymization (FA) normative text for 11bi -- Phil Hawkes/Duncan Ho

Presented by Phil

Phil presents r1 of this large document (25 pages).

Presenter introduced the structure of the document and the terminology it introduces.

He also quicky go thru the different new frames introduced.

* + 1. Questions

C: Even if I agree on the general direction, I think we need to work on open items

Q: About AID collision, how could this happen since this assigned by the AP.

A: The point is that AP may have retransmissions including AID, especially for individually addresses trigger frame. So, we may need to take care on potential transmission just before the Epoch.

Q: Do we decided that EDP will only be available for MLO?

A: We have a general agreement in the group on this.

C: This is a very detailed things, but we received previous presentation having different proposal, like for instance in the MAC address generation using KDK rather than PTK.

A: it seems to have consensus on this approach.

Q: Is there any reason to use AID as a parameter to generate the MAC address?

A: No, the more parameter we have the better it is.

C: There are still some elements to discuss but thank you for the huge work.

Chair: I think we cannot directly integrate that into the draft so we will have to go section by section. Chair request people to check their agenda to prepare contribution on dedicated topics.

Chair remind the timeline and the target to generate a D0.1 in January.

1. Chair adjourned the meeting at 15:28 EDT.