IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbh SA Ballot CIDs on IRM | | | | |
| Date: 2024 - May | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

CIDs related to IRM.

3001, 3024, 3031, 3033, 3034, 3045, 3046, 3047, ~~3048~~, 3050, 3056, 3057, 3058, 3059, 3071, 3073, 3077, 3078, 3079, 3080, 3081, 3083, 3085, 3086, 3088, 3089, 3090, 3094, 3096, 3097, 3103, 3195, 3196, 3197.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3085 | 17.13 | 3.2 | Per definition of IRM (“A MAC address that can be used by a non-access point (non-AP) station (STA) to identify itself to a network”), any MAC address that can be used by such a STA to identify itself to a network is (“by definition") an IRM. This definition is inconsistent with the draft. Note that a definition-like sentence in 12.2.12.2 (“"An IRM is a MAC address that is constructed from the locally administered address space.”) is also inadequately limited. In fact, given that the “R” in IRM stands for “random”, the concept of randomness should be included in the definition. | Create a definition with a meaningful limitation, including the requirement for randomness; e.g. : "A MAC address selected randomly from among the Administratively Assigned local identifiers specified in IEEE Std 802 and used by a non-access point (non-AP) station (STA) to identify itself to a network." | Revised  at 38.24 make following change  “An IRM is a random MAC address that is constructed from the locally administered address space. A non-AP STA ~~should~~ shall construct randomized IRMs according to IEEE Std 802-2014 and IEEE Std 802c-2017.”  Note to commentor:  This change follows the current baseline in Rev me, subclause 12.2.10. and should follow any changes made in TGme.  And at 17.13 change IRM definition as follows:  *“A random local MAC address provided by a non-access point (non-AP) station (STA)*  *to identify itself to a network*.” |
| 3024 | 27.40 | 9.4.2.316 | The Device ID Length field is not a length; it's a field. | Change to "The Device ID Length field is set to the number of octets in the Device ID field." ("is set to" or "indicates"; I prefer "is set to" because indicates is not specific on the encoding) | Revise  Change cited text to “The Device ID Length field is set to the number of octets in the Device ID field." |
| 3086 | 28.45 | 9.4.2.317 | The text indicates that the IRM field contains a MAC address, without limitation. In fact, only specific forms are permitted, per 12.12. It would be helpful to refer the reader to this fact. The same comment also applies elsewhere (e.g., P31L24). | Change to "The IRM field contains an IRM, as specified in 12.2.12.2, when sent from a non-AP STA to an AP." | Reject  The IRM is a MAC address and convention in clause 9 is to define the content of frame fields.  The IRM MAC address form is specified in the operational procedures. |
| 3071 | 18.14 | 4.5.4.10 | "To mitigate this sort of traffic …." could be improved. | Change "To mitigate this sort of traffic..." to "To mitigate traffic analysis and tracking…" | Accept |
| 3078 | 38.32 | 12.2.12.2 | Poor use of terminology | Change "… that IRM as its TA for any probes," to "that IRM as a TA for any Probe Request frames," | Revise  Change  "… that IRM as its TA for any probes,"  to  "…that IRM as the TA for any Probe Request frames,"  Note to editor, P38.32 |
| 3097 | 34.9 | 12.2.12 | This looks like incorrect use of "may" (an optional requirement). It seems to be stating an objective for this clause. | Delete sentence. Change first sentence of next paragraph to "When a non-AP STA is randomly changing it's MAC address while not associated (see 4.5.4.10 (MAC privacy enhancements)) this presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information (“shared identity state”) from the previous association to the current association (see 12.2.10). | Revise  4.5.4.10 says  “To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its  MAC addresses….”  Hence propose to use “can” in place of “may”.  Revise  At 39.9 replace “a non-AP STA may randomly…”,  with  “a non-AP STA can randomly…” |
| 3096 | 34.21 | 12.2.12 | "A may then report back to the AP during a future association or PASN authentication" is a rather vague statement of a requirement, which I think is meant to be an informative, not normative, statement. This appears to be stating a possibility, not an optional requirement (in which case some additional information is needed to implement the option). In this case "will" is more correct as that is how this first scheme is intended to work. | change "may" to "will" | Revise  At P34.20  Change  “may then report back”  To  “then reports back”. |
| 3083 | 34.26 | 12.2.12 | There has been confusions during offline discussion that IRM can be used to change MAC address during association. Although the description for the IRM specifies that it is used during the "next preassociaiton exchanges...", but I think the confusion is whether the "next" is applied to all the description. Suggest to add next for all the following descriptions. | change "during its next preassociation exchanges, PASN authentication, and/or association and associated exchanges with that AP." as "during its next preassociation exchanges, next PASN authentication, and/or next association and next associated exchanges with that AP." | Accept |
| 3073 | 34.31 | 12.2.12 | Both mechanisms require the dot11PrivacyActivated is equal to true. Otherwise the device uses its universal MAC address. | At 34.30, insert the following sentences at the beginning of the paragraph: "MAC privacy enahancements is required in order to use the device ID mechanism or the IRM mechanism. non-AP STA shall set dot11PrivacyActivated equal to true to use either of these mechanisms." | Accept |
| 3094 | 34.38 | 12.2.12 | The Note starting on line 35 is ambiguous:  The IRM mechanism and the device ID mechanism are independent. IRM allows an AP to recognize a non-AP STA prior to and while it is associated. Device ID allows an AP to identify a non-AP STA while it is associated. A device ID is allocated by an AP, and an IRM is selected by a non-AP STA. If an AP and a non-AP STA both have both IRM and device ID activated, the non-AP STA might provide both an IRM and a device ID during association or PASN authentication.[262,107, 36, 230] | The IRM mechanism and the device ID mechanism are independent. IRM allows an AP to recognize a non-AP STA prior to and while it is associated. Device ID allows an AP to identify a non-AP STA while it is associated. A device ID is allocated by an AP, and an IRM is selected by a non-AP STA. If an AP and a non-AP STA both have the IRM and device ID activated, the non-AP STA may provide an IRM and a device ID during association or PASN authentication. | Reject  It's a Note, hence "might" not "may" |
| 3081 | 35.35 | 12.2.12.2 | This set of requirements is silent of the use of IRM with FT. However I don't see why IRM cannot be used in FT initial Association. | Insert the following sentence after the first sentence of the paragraph at 38.55: "A non-AP STA may indicate the IRM mechanism is activated in an association request frame as part of an initial mobility domain association." | Revise  Insert the following sentence after the first sentence of the paragraph at 38.55:  "A non-AP STA may indicate the IRM mechanism is activated in an association request frame as part of an initial mobility domain association."  Relative to REVme D6.0 edits as follows:  Include 13.4.2 in the TGbh draft.  At 3185.52 for EAPOL Message 2, change  "MDE, FTE" to "MDE, FTE [, Device ID KDE]"  At 3185.55 for EAPOL  Message 3, change  "[, WIGTK(R, WIPN)]" to ""[, WIGTK(R, WIPN)] [, Device ID KDE] [, IRM KDE]"  At 3185.57 for EAPOL  Message 4, change "{}" to "{[IRM KDE]}" |
| 3197 | 36.2 | 12.2.12.2 | Don't all the "may"s in this para need to be shoulds or shalls? | More generally the following "may" look suspect to me:  The following look suspect to me:  it may proceed with the assumption [discussed elsewhere]  An AP may set a Device ID Status field to 1 indicating “Not Recognized” if the AP cannot unequivocally identify the non-AP STA shared identity state.  … that it may transmit …  … may either continue to associate or authenticate using PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication optionally provide an IRM element in the Association Request frame, or when using PASN authentication optionally provide an IRM element in the third PASN frame, else disassociate/ deauthenticate.  An AP may set an IRM status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.  … such that the AP may identify the non-AP STA  … such that APs in that ESS may identify the non-AP STA | Revise  See proposed changes at end of this document for CID 3197 |
| 3057 | 38.20 | 12.2.12.2 | I think it needs to be clarified within the note that the IRM is distributed throughout the APs in the ESS and not the ESS itself. | Change "distribute IRMs throughout the ESS" to "distribute IRMs throughout the APs in the ESS" | Revise  At cited sentence change to  “distribute IRMs to the APs in the ESS"  And at 35.18 |
| 3031 | 38.31 | 12.2.12.2 | association is not requested | Change "the next time it requests association to any AP in that same ESS" to "the next time it associates with an AP in that same ESS" | Revised  At 38.31 replace:  “The non-AP STA may  then use that IRM as its TA the next time it requests association to any AP in that same ESS”  With  “The non-AP STA may  then use that IRM as its TA the next time it associates with any AP in that same ESS” |
| 3033 | 37.50 | 12.2.12.2 | "Identifiable random MAC address (IRM) operation" in the title but "IRM mechanism" elsewhere. | Change title to "Identifiable random MAC address (IRM) mechanism". At 48.28, change "IRM operation" to "IRM mechanism" | Revise  Change title to "Identifiable random MAC address (IRM) mechanism". At 48.38, change "IRM operation" to "IRM mechanism" |
| 3195 | 37.54 | 12.2.12.2 | "A non-AP STA that has dot11IRMActivated equal to true indicates the IRM mechanism is active by setting the IRM Active field to 1 in either the Extended RSN Capabilities field in (Re)Association Request frames or the first PASN frame that is sent to any AP that advertises activation of the IRM mechanism." is confusing because it suggests that if the STA wants to do it with PASN the AP has to advertise it, but if the STA wants to do it with extended caps the AP doesn't have to support it. Also the IRM Active field is always in ext caps so "either" is misplaced | Change to "A non-AP STA that has dot11IRMActivated equal to true indicates the IRM mechanism is active by setting the IRM Active field to 1 in the Extended RSN Capabilities field in either the (Re)Association Request frame or the first PASN frame that it sends to an AP that advertises activation of the IRM mechanism." and put para break before. Similarly at 34.61 | Revise  Change to "A non-AP STA that has dot11IRMActivated equal to true indicates the IRM mechanism is active by setting the IRM Active field to 1 in the Extended RSN Capabilities field in either the (Re)Association Request frame or the first PASN frame that it sends to an AP that advertises activation of the IRM mechanism." and put para break before. Similarly at 34.51 |
| 3088 | 38.24 | 12.2.12.2 | The paragraph "An IRM is a MAC address that is constructed from the locally administered address space. A non-AP STA should construct randomized IRMs according to IEEE Std 802-2014 and IEEE Std 802c-2017.” has several problems. | If the IRM is defined precisely in the definition section, then this sentence may be unnecessary. Alternatively, change to: “An IRM is selected randomly from among the Administratively Assigned local identifiers specified in IEEE Std 802.” See also comments targeted to P38L27 and P38L28 for additional changes proposed to this material. | Revised  Note to editor, same resolution as CID 3085  At 38.24 make following change  “An IRM is a random MAC address that is constructed from the locally administered address space. A non-AP STA ~~should~~ shall construct randomized IRMs according to IEEE Std 802-2014 and IEEE Std 802c-2017.”  Note to commentor:  This change follows the current baseline in Rev me, subclause 12.2.10. and should follow any changes made in TGme.  And at 17.13 change IRM definition as follows:  *“A random local MAC address provided by a non-access point (non-AP) station (STA)*  *to identify itself to a network*.” |
| 3034 | 38.27 | 12.2.12.2 | "When associating or authenticating using PASN for the first time" is ambiguous (one does not associate using PASN). | Change to "When associating for the first time or authenticating using PASN for the first time..." | Accept |
| 3056 | 38.27 | 12.2.12.2 | The text "When associating or authenticating using PASN for the first time to an ESS", is incorrect as associations are between peer STAs. | Change the cited text to "When associating or authenticating using PASN for the first time to an AP in an ESS" | Revise  Change to "When associating for the first time or authenticating using PASN for the first time to an AP in an ESS" |
| 3089 | 38.27 | 12.2.12.2 | The notion of a “first time” association or authentication is problematic. It seems clear that a such a circumstance should occur even if it’s not the first time; e.g., if the device has been fully reset, and probably in other cases as well. Those cases are not addressed in the draft. | Change “for the first time to an ESS, the non-AP STA” to “, a non-AP STA without an IRM that it has previously provided to the ESS”. See also comments targeted to P38L24 and P38L28 for additional changes proposed to this material. | Reject  The point here is that this deals with the intiial first time association (or authenication using PASN). The STA can use any MAC address, including its real one. Re-defining “first time” as “without an IRM” might cause confusion. Also Note 2 (39.20) refers to this first connection case and the use of the “not recognized” procedure. Text is considered to be clear on this point. |
| 3077 | 38.28 | 12.2.12.2 | The sentence looks to be specific to PASN, but I don't think it is. Also, there are restrictions on what MAC address can be used. | Change "When associating or authenticating using PASN for the first time to an ESS, the non-AP STA may use any MAC address." to "When associating to an AP in an ESS or authenticating using PASN for the first time, the non-AP STA may use any Local MAC address." | Line in spreadsheet is wrong. Correct line is Line 28.  STA can use any MAC Address, including its own.  Revise  Change cited text to  “When associating to any AP in an ESS or authenticating using PASN for the first time, the non-AP STA may use any local or its universal MAC address." |
| 3090 | 38.28 | 12.2.12.2 | The text "the non-AP STA may use any MAC address” is problematic. Does it mean that any possible identifier that meets the conditions (e.g., per IEEE Std 802) to be used as an IEEE 802 MAC address is an eligible MAC address in this circumstance? For example, could it be a a multicast address? Could be be an EUI under an OUI assigned to an entity who does not condone this use? The answer to these questions needs to be “no”. | Join with the prior paragraph, using the resolution proposed in the comments targeted to P38L24 and P38L27, so that the first two sentence of the combined paragraph are replaced by: "When associating or authenticating using PASN, a non-AP STA without an IRM that it has previously provided to the ESS may use any IRM selected randomly from among the Administratively Assigned local identifiers specified in IEEE Std 802." | Should not restrict it to locally addressed.  Revise  When associating for the first time, the STA can use any MAC address, including its universal one.  Change cited text to  “When associating to any AP in an ESS or authenticating using PASN for the first time, the non-AP STA may use any local or its universal MAC address.". |
| 3001 | 38.32 | 12.2.12.2. | The sentence is confusing because the phrase "directed or broadcast" is not a member of the list frames where the non-AP STA can use the IRM, but a description of the types of probe frames | Rephrase as "The non-AP STA may also use that IRM as its TA for any directed or broadcast probe frames, public Action frames, Authentication frames, and (Re)Association frames that it may transmit when it intends to be identified." | Revise  "The non-AP STA may also use that IRM as its TA for probe frames (directed or broadcast), public Action frames, Authentication frames, and (Re)Association frames that it may transmit when it intends to be identified." |
| 3103 | 38.30 | 12.2.12.2 | "The non-AP STA may then use that IRM as its TA the next time it requests association to any AP in that same ESS."  This isn't entirely clear that it is trying to say the IRM is going to be used some time in the future. The next sentence is even worse. | Suggest adding "after it leaves the ESS (disassociates) and then the next time (some time later) when it returns and requests association to any AP in the same ESS, including Authentication and Association frames." Change the next sentence to "The non-AP STA may also use that IRM after it disassociated from the ESS, for any probes, directed or broadcast, or public Action frames sent to any AP in the ESS. | Revise  Ref CID 3001  (First change does not appear to me to be needed. I do however agree with the second change.)  Change the next sentence to "The non-AP STA may also use that IRM as its TA for probe frames (directed or broadcast), public Action frames, Authentication frames, and (Re)Association frames that it may transmit when it intends to be identified." |
| 3196 | 38.30 | 12.2.12.2 | "may then use that IRM as its TA" -- shouldn't it be more than a "may"? | Change to "shall use that IRM as its TA […] if it wants to be recognised". In the next sentence change "may also use" to "shall also use" and "that it may transmit" to "that it transmits" | IRM is optional not mandatory.  Revise (ref CID 3001)  At cited location, change to:  "The non-AP STA may also use that IRM as its TA for probe frames (directed or broadcast), public Action frames, Authentication frames, and (Re)Association frames that it may transmit when it intends to be identified." |
| 3045 | 38.42 | 12.2.12.2 | For checking whether the IRM is already in use within the ESS a note needs to be added to the effect of “Mechanism to synchronize the storage of IRMs throughout an ESS is out of scope for this standard.” Alternatively, add this point to the Note 1 on the same page at L21. | as in comment | Reject  We have note 1 at P38.20. Why say twice? |
| 3079 | 38.42 | 12.2.12.2 | It's the new IRM. | Change "If a newly provided IRM" to "If a new IRM" | Revised  Change cited text to  "If a newly provided IRM is already in use by any STA in the ESS” |
| 3058 | 38.42 | 12.2.12.2 | I think it needs to be clarified that the IRM is used by APs within the ESS and not the ESS itself. | Change "If a newly provided IRM is already in use within the ESS" to "If a newly provided IRM is already in use by an AP of the ESS" | Revised  Change cited text to  "If a newly provided IRM is already in use by any STA in the ESS" |
| 3080 | 38.44 | 12.2.12.2 | If there's a duplicate, which STA should the AP send the Duplicate IRM frame to? | Change  "the AP should send a Duplicate IRM frame (see 9.6.36.2) to the non-AP STA indicating to the STA that the provided IRM is a duplicate. The non-AP STA may then respond with a New IRM frame (see 9.6.36.3 ), which provides a new IRM to the AP." to "the AP should send a Duplicate IRM frame (see 9.6.36.2) to the non-AP STA that provided the new IRM indicating that the new IRM is a duplicate of another Local MAC address. The non-AP STA may then respond with a New IRM frame (see 9.6.36.3 ) to provide an updated new IRM to the AP." | The first part of the sentence explains when the AP sends the duplicate frame.  Revise  “the AP should send a Duplicate IRM frame (see 9.6.36.2) to the non-AP STA that provided the new IRM indicating that the provided IRM is a duplicate. The non-AP STA may then respond with a New IRM frame (see 9.6.36.3 ), to provide a new IRM to the AP.” |
| 3046 | 38.53 | 12.2.12.2 | Remove the sentence “In so doing, the AP identifies the non-AP STA” as it provides no value here. | as in comment | Accept |
| 3047 | 39.8 | 12.2.12.2 | Instead of “… and the IRM field is not present.”, it should be “… and the IRM field is present.” | as in comment | Reject  The IRM field is never present when sent by the AP. |
| 3048 | 39.18 | 12.2.12.2 | Remove the word ‘state’ at the end of the sentence as it changes the meaning of the sentence. | as in comment | Assigned to Mark H  See also CIDs 3134, 3200  Reject  How to express this idea was argued long over how to say this.  At top of 12.2.12 we do discuss what the shared identity state is. |
| 3050 | 39.27 | 12.2.12.2 | Sentence does not read well. Reword to “A non-AP STA may use that address for active scanning for an AP in that ESS.” I think we have already established in the prior subclause text that the IRM is distributed to APs across the ESS. | as in comment | Revised  Change cited text to  “A non-AP STA may use that address when actively scanning for any AP in that ESS, such that the AP may identify the non-AP STA.” |
| 3059 | 39.28 | 12.2.12.2 | I think it needs to be clarified that the IRM is used by APs within the ESS and not the ESS itself. | Change "A non-AP STA that has provided an IRM to an ESS" to "A non-AP STA that has provided an IRM to an AP within the ESS" | Revised  Change cited text to  "A non-AP STA that has provided an IRM to any AP in the ESS" |

CID 3197

Revised

At 36.2 Change “may proceed” to “proceeds”

At 39.7 make changes as follows:

If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the AP shall set the IRM Status field of the IRM KDE or IRM element ~~is set~~ to indicate Recognized and the IRM field is not present. If the AP does not recognize the IRM, the AP shall set the IRM Status field of the IRM KDE or IRM element ~~is set~~ to indicate Not recognized and the IRM field is not present.[158] An AP shall set the IRM status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state. The non-AP STA, on receipt of an IRM Status field of value 1, indicating that the AP has not recognized the IRM, ~~may~~ shall either continue to associate or authenticate using PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication optionally provide an IRM element in the Association Request frame, or when using PASN authentication optionally provide an IRM element in the third PASN frame, else disassociate/deauthenticate.[232, 233] ~~An AP may set an IRM status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.~~