IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of some MAC comments | | | | |
| Date: 2021-09-09 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission addresses the CIDs under the “Dan Harkins” tab of 11-21/0793r4 with the exception of CID 205 which has been resassigned to Mark Rison and CID 591 which has been reassigned to Stephen McCann.

**CID 154**

Comment: It would be helpful to explain the columns in Table 9-51.

Proposed Change: Reference 12.2.7 and 11.12 (or maybe 12.5.3.1, et al?) for explanations of the "Robust" and "Group Addressed Privacy" columns in Table 9-51.

Discussion: Both 11.12 and 12.2.7 refer back to Table 9-51 but having a forward reference (thus making a circle!) would seem helpful to the reader for more information on the significance of the values in these columns.

Proposed Resolution: Revised, instruct editor to modify section 9.4.1.11 as indicated:

**9.4.1.11 Action field**

The Action Details field contains the details of the action. The details of the actions allowed in each category are described in the appropriate subclause referenced in Table 9-51 (Category values). Robust Action frames are defined in 12.2.7 (Requirements for management frame protection) and group addressed privacy is defined in 11.12 (Group addressed management frame protection procedures).

**CID 461**

Comment: "If no MLME-SA-QUERY.confirm primitive for the STA is received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall allow a subsequent association process with the STA to be started without starting an additional SA Query procedure" -- should it allow this indefinitely? It might be better to have some kind of timeout, though it's not clear what this should be. Ditto in 11.3.5.5

Proposed Change: As it says in the comment

Discussion: Comments that suggest a change of “as it says in the comment” are inappropriate, especially when the comment to which it refers say “it’s not clear what [the change] should be.” It’s not clear what the commenter wants and it’s not clear how to satisfy the comment. “Ditto in 11.3.5.5”? Well it’s not clear what the change should be everywhere, not just 11.3.5.5.

Proposed Resolution: Reject, there is no change proposed that could satisfy the comment.

**CID 344**

Comment: "direct hashing" (technique) should be referred to as "hash-to-element" (11x) so a single term is used throughout. Ditto "directly hashing" should be canonicalised (2x)

Proposed Change: As it says in the comment

Discussion: Another, proposed change of “as it says in the comment”. The hash-to-element procedure uses direct hashing, as opposed to looping. This is nice descriptive text that should not change. A single term would result in a tautology and ridiculousness. Suggesting bulk editing changes (“(11x)…(2x)”) is inappropriate as it assumes that the assignee can identify each of these locations, presumes to be the accurate total number of such references, and does not include any context surrounding any of these locations which might make application of the bulk editing change wrong.

Proposed Resolution: Reject, there is no problem identified, no justification for the change, and the change would not be correct.

**CID 340**

Comment: It would be good if some of the RSNE examples showed counts greater than 1

Proposed Change: As it says in the comment

Discussion: Again with the “as it says in the comment”. Further demonstration of the inappropriate and unprofessional nature of these kinds of comments. The comments says “it would be good if….” There is no justification to describe the benefit that would be realized if this thing that is said in the comment is done. It’s like saying, “it would be good to know how many commas are in the REVme draft…as it says in the comment” and then expect an assignee to go spend time doing it as if people on the comment resolution committee are at the beck-and-call of random commeters and will go do busy work on command.

Proposed Resolution: Reject, inappropriate and unprofessional comment.

**CID 204**

Comment: There are 12 locations where the SME is required to "delete any PTKSA, GTKSA, IGTKSA, BIGTKSA and temporal keys held for communication". Any TPKSA also needs to be deleted too (except maybe for reassociation to the same AP?)

Proposed Change: Add ", TPKSA" after ", GTKSA" in each of the 12 locations

Discussion: Another form of inappropriate comment. There is no page or line number associated with this comment. It alleges that there are 12 occurances (in a 4600 page document) of something and to go do a blanket edit at each place. This assumes that the assignee will identify each of the 12 places that the commenter could not be bothered to list in the comment, and it assumes that there are exactly 12 places, no more and no less. Such an editing might be appropriate at some of the occurances, it might even be appropriate at 12 occurances, it might be appropriate at 14 occurances only 7 of which are in the commenter’s 12, or some places might not need such an edit. Blanket edits ignore context that might make an individual edit incorrect at a certain location. Without an explicit listing of each of the places where a change is being proposed it is not possible to determine whether the change would be correct. And it’s unprofessional to instruct an assignee to do a task that the commenter could not be bothered to do.

Proposed Resolution: Reject, inappropriate and unprofessional comment.

**CID 167**

Comment: "16 replay counters per PTKSA/GTKSA/" has a spurious trailing /. But actually all entries in the table are missing TPKSA

Proposed Change: Change "PTKSA/GTKSA[/]" to "PTKSA/GTKSA/TPKSA" throughout Table 9-152--PTKSA/GTKSA replay counters usage (including caption). At 3841.33 change "Specifies the number of PTKSA replay counters per association:" to "Specifies the number of PTKSA replay counters per association and the number of TPKSA replay counters per TDLS link:"

Discussion: A comment that states the exact change desired at the exact location! Huzzah!

Resolution: Accept.

**CID 162**

Comment: In Table 9-43--Action frame body and Action No Ack frame body, 11.12 Group addressed management frame protection procedures, 12.5.3(.1) CTR with CBC-MAC protocol (CCMP), 12.5.5(.1) GCM protocol (GCMP) it is not sufficiently clear that "Group addressed privacy" only applies in the context of an MBSS

Proposed Change: In 11.12 change "For group addressed Management frames that" to "In an MBSS, for group addressed Management frames that". Add "(MBSS only)" in each of the other locations

Discussion: It’s not sufficiently clear why 12.5.3 and 12.5.5 (or “each of the other locations”) need clarification for their reference to a table. Indeed, if the rows in the referred table currently only apply to mesh that is something that can be determined by checking the table. Putting a linkage in the general description of a cipher mode that directs its specific usage seems wrong, and likely to cause trouble if the referred table ever changes in the future. But the text in 11.12 does reference the MGTK so that text might be in need of clarification.

Resolution: Revised, instruct the editor to modify section 11.12 as indicated:

**11.12 Group addressed management frame protection procedures**

For group addressed Management frames in an MBSS that are specified with Yes in the Group Addressed Privacy column of Table 9-51 (Category values), the group addressed frame protection service shall take the following actions:

* The frames shall be encapsulated and protected with the MGTK using the group cipher negotiated during the AMPE exchange.

**CID 119**

Comment: The currently defined rules for processing received Robust Management frames do not seem to explicitly disallow processing of group addressed frames in cases where only an individually address frame would be used. While the group addressed frame is not defined in the standard as a valid case, it would be better to make the receiver rules more explicit to avoid undesired security issues (potential for insider attacks due to the shared IGTK being used for the group addressed frames). It may not be appropriate to describe a generic rules for all Robust Action frames since there might be cases using group addresses from. As such, this comment might require going through all possible Robust Action frames and identify the correct constraint separately for each.. The proposed change here is addressing only the SA Query case which can have security implications. Similar rules to force group addressed frames to be discarded should likely be added for some other cases (e.g., DelBA) to avoid similar security issues.

Proposed Change: Add a new item to the "none of the following are true" list (P2302 L5):

-- The SA Query Request frame was sent to a group address.

Add the following new paragraph at P2302 L24:

"If a STA receives a group addressed SA Query Response frame, it shall deem the response as invalid and discard it."

Discussion: The comment is specific enough to be acted upon. Its request for a more thorough going over of the specification and enhancement of the proposed change by including separate constraints for each robust action frame is declined though.

Proposed Resolution: Accept.

**References: 11-21/0793r4**