IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Suggested comment resolution for CID 2548 on REMmd D2.0 | | | | |
| Date: 2019-07-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Marc Emmelmann | Self | Berlin, Germany |  | emmelmann@ieee.org |
| Hitoshi Morioka | SRC Sorftware | Fukuoka, Japan |  | hmorioka@src-soft.com |
| Hiroshi Mano | KDTI | Tokyo, Japan |  | mano@koden-ti.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Abstract

This submission presents a suggested comment resolution for CID(s) 2548 on REVmd D2.0

Table of Contents

[Abstract 1](file:////Users/mem/Documents/Privat/Projects/802.11-TGm/REVmd-D2-Fils_comments/11-19-1252-00-000m-Suggested%20comment%20resolution%20for%20CID%202548%20on%20REMmd%20D2.0.docx#_Toc14081721)

[Comment 3](#_Toc14081722)

[Discussion 3](#_Toc14081723)

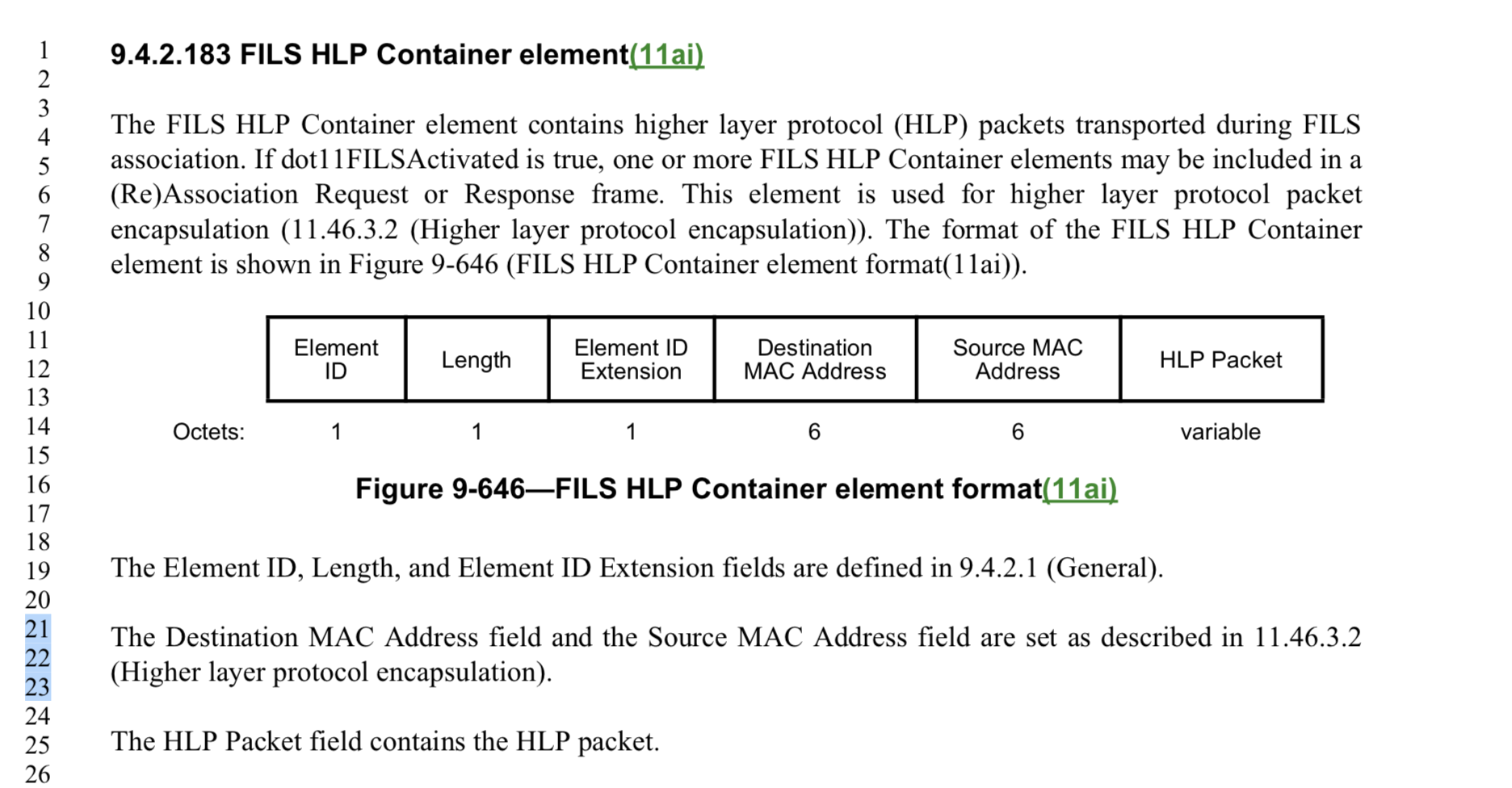
[Proposed Resolution 4](#_Toc14081724)

# Comment

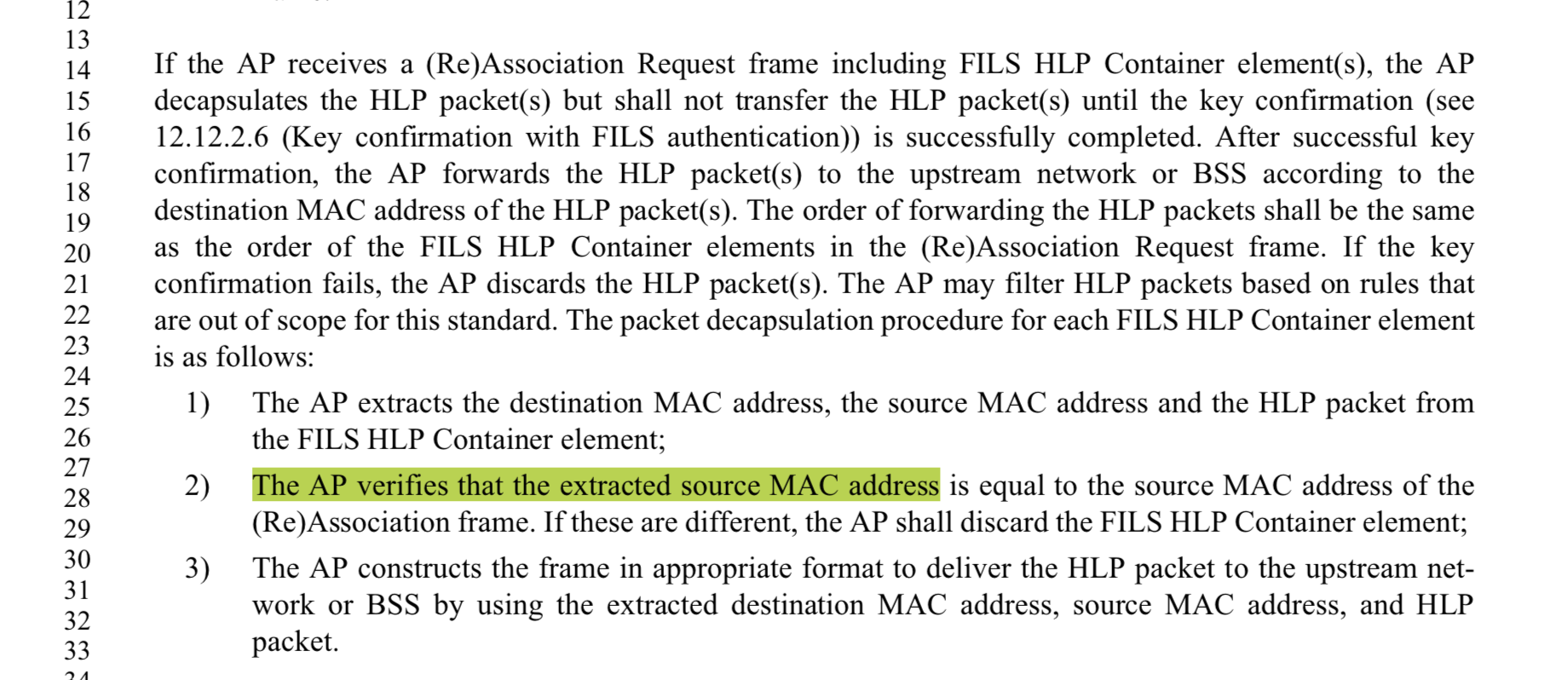
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CID** | **LB** | **Draft** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** |
| 2548 | 236 | 2 | 1351.00 | 1 | 9.4.2.183 | "The AP verifies that the extracted source MAC address is equal to the source MAC address of the (Re)Association frame. If these are different, the AP shall discard the FILS HLP Container element;" -- so there's no point passing the source MAC address, since the transmitter will always ensure they are the same (why bother sending something you know the other end will discard?). CID 1543 rejected this because "the FILS HLP Container element is reused in other situations, in which the source address field is required. Instead of defining another (new) element, the existing is reused (e.g. see D1.4 P 2461 L55)." This makes no sense as the whole point of this comment is that the source address is necessarily going to match, so adds no value | Make the changes proposed in CID 1543 |

# Discussion

Context of the comment (D2.0 P1351)



The comment does not directly refer to text in this clause but in the referenced cls. 11.46.3.2



The sentence " The AP verifies that the extracted source MAC address is equal to the source MAC address of the (Re)Association frame. If these are different, the AP shall discard the FILS HLP Container element;" is required because of the following security reason.

If the AP does not filter by the source address, a malicious non-AP STA can send fake frames to the network.

# Proposed Resolution

Reject.

The FILS HLP Container element is reused in association responses, in which both the source and destination address fields are required and may not match the addresses of the AP or STA. Instead of defining another (new) element, the existing is reused (e.g. see D1.4 P 2461 L55).