IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbh CIDs on Shared Identity State | | | | |
| Date: 2024-06-18 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java Dr  Sunnyvale, CA 94089 | +1.303.818.8472 | [mark.hamilton2152@gmail.com](mailto:mark.hamilton2152@gmail.com) |

Abstract

R0: TGbh Initial SA CIDs related to Shared Identity State (subclause 12.2.12.1), CIDs 3134, 3200.

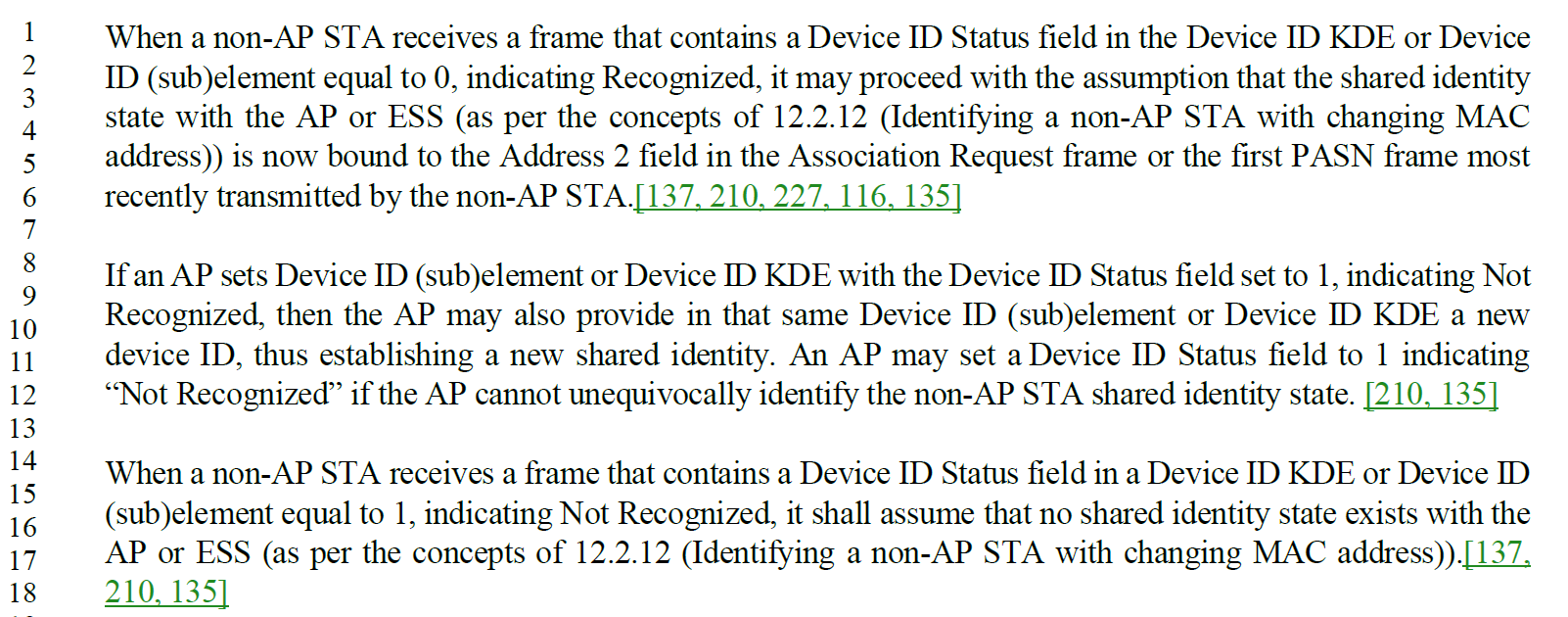
R1: Added CID 3048

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3134 | 36.2 | 12.2.12.1 | what does the non-AP STA do with this binding?It assumes there's a binding…but what does it do with that knowledge? How does it use this binding? | define what the binding implies and how knowledge of the binding is used or get rid of the paragraph | Revised |
| 3200 |  | 12.2.12.1 | "may proceed with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.10) is now bound to the TA field in the Association Request frame" -- it is not clear what the implications/consequences of this assumption are | MarkH clarified that the intent was "It’s not that “something bad will happen”, but that something good (optimization) was hoped for, will not happen. The non-AP STA will not be recognized, and any state that had previously been established will need to be re-established. Or, in the case of this phrase, when things do work correctly, the AP and non-AP STA may proceed with the assumption that this state is still established, and they don’t need to take effort to re-establish it." so express that somehow | Revised |



**Context:**

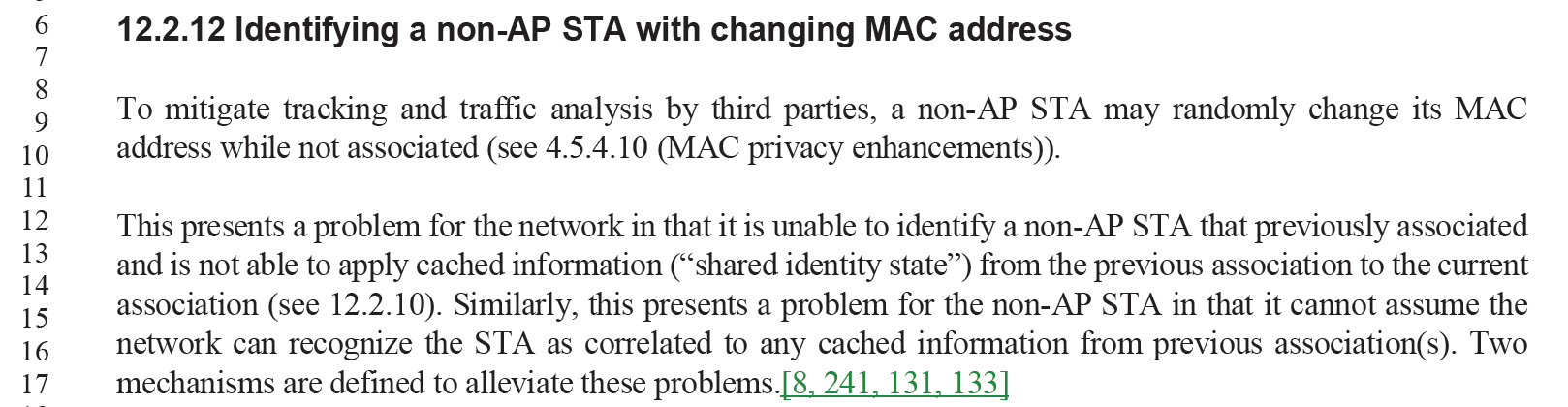
12.2.12.1, P36.1:





**Discussion:**

The root concept of this “binding” and “assumption” is the *shared identity state*. This term comes from here (12.2.12, P34.12):





We need to (better?) connect the discussion on page 36 with the concept introduced on page 34. There is also the explicit cross-reference, but apparently that is not enough to clarify the intent.

Two views of this:

* When successful (“Recognized”, per 12.2.12.1 text quoted above), the non-AP STA knows/assumes that the shared identity state is established and re-used. It can proceed knowing the shared state is established for use by its applications, higher-layer control plane (access to the LAN and WAN, etc.), and for layer 2 control plane (pre-/non-association identity for steering, etc.)
* BUT… When not successful (“Not Recognized”, per third paragraph of 12.2.12.1 above), the non-AP STA knows that where such shared state is needed/desired, it much re-estastablish such identity.

The question is how much of the discussion just above is use case justification and potentital uses within the end device implementation that the Standard should/needs to explain?

(Also, a minor nit, but the second occurrenace on page 36 left off the word “state” in the term.)

**Proposed Resolution:**

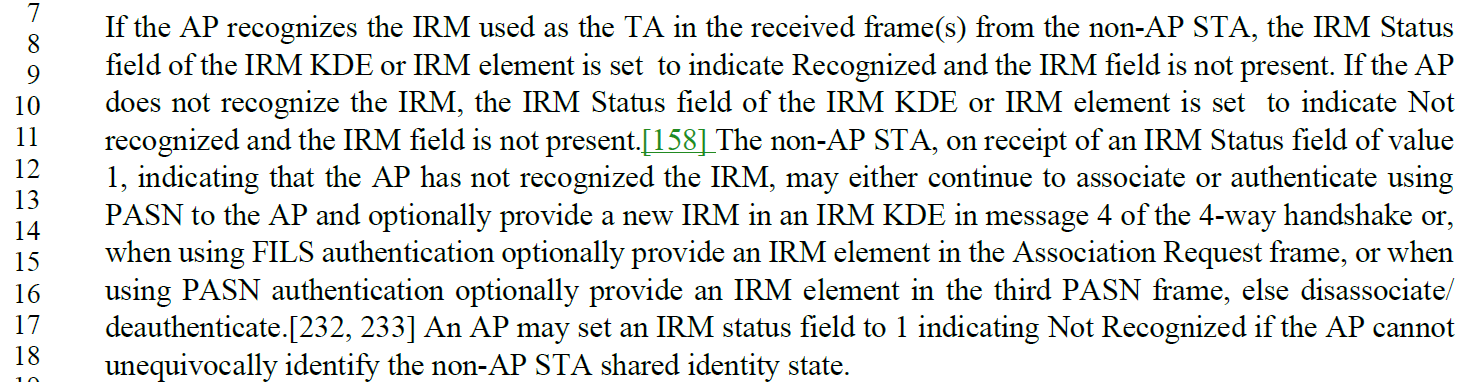
<To be discussed>

At P36.11, replace “new shared identity” with “new shared identity state”.

**CID 3048:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | ??? |

**Context:**



**Discussion:**

The term, per discussion above (for CIDs 3134 and 3200) is “shared identity state”, for the cached information that the network can re-use (only) when it can recognize the returning non-AP STA. In this case, the network cannot identify the non-AP STA, so it cannot identify the *shared identity state* that corresponds to the STA.

**Proposed Resolution:**

Rejected.

The term “shared identity state” is specifically defined in 12.2.12 (D4.0, P34.12), for the cached information that the network can re-use (only) when it can recognize the returning non-AP STA. In this case, the network cannot identify the non-AP STA, so it cannot identify the *shared identity state* that corresponds to the STA.