IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbh CIDs on Shared Identity State |
| Date: 2024-06-19 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java DrSunnyvale, CA 94089 | +1.303.818.8472 | 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

R2: Provided proposed resolution changes, based on feedback from the TGbh group during the Sunnyvale ad hoc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |
| 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 |

**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 identity 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 identity state is needed/desired, it much re-estastablish such identity.

The suggestion is to clarify the value/purpose of the shared identity state, and the value of being able to logically match a returning STA to such previous established shared identity state (including in clause 4, where it is mentioned that the network would like to “recognize” a returning STA, but not that this recognition is related to the shared identity state concept).

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

**Proposed Resolution (both CIDs):**

Revised

In 4.5.4.10, after the sentence:

“Either approach allows the network to recognize the STA while providing protection against third party tracking or traffic analysis.”

add:

“When the network can recognize the STA, it can map already established shared identity state (see 12.2.12) to this STA, which allows the network to help with network acquisition steering and selection, or connect transactional information such as preasociation or prior association activity to a post-association device.”

In 12.2.12, after the sentence:

“The two mechanisms both allow the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA.”

add:

“When the STA is successfully recognized by the network, it can proceed knowing that its prior shared identity state is established and re-used by its applications, higher-layer control plane (such as the network allowing access to the LAN and WAN, etc.), and also for layer 2 control plane (pre-/non-association identity for access and steering, etc.). Alternatively, when the STA fails to be successfully recognized, it knows that where such shared identity state is needed/desired, it will have to be re-estastablished through additional protocol exchanges. Both mechanisms also provide for the non-AP STA to opt-in (typically under user-control) to participating in the recognition mechanism, so that sensitive user information can be kept confidential unless the network is trusted.”

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.