IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Suggestions for remaining “fix-ups” in TGbh D0.1 | | | | |
| Date: 2022-05-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Mark Hamilton | Ruckus/CommScope |  |  | [Mark.hamilton2152@gmail.com](mailto:Mark.hamilton2152@gmail.com) |
|  |  |  |  |  |

Abstract

This submission provides discussion and suggestions to complete (“fix-up”) the remaining clauses not currently covered in TGbh D0.1.

Overview (clause 1):

* Insert the following bullet as part of the “This standard…” list in subclause 1.3:
  + Defines a mechanism to enable private identification of IEEE 802.11 STAs that use a randomized or changing MAC address.

Normative References (clause 2):

* None appear to be needed. The new Annex mentions AES-SIV-256 and AES-SIV-512, but these are not newly added, and we have references to supporting RFCs for AES, already.

Definitions (clause 3):

* None seem to be needed. Perhaps, one for “device identification (ID)” could be imagined, but I suspect it will turn into a rat-hole discussion, and does not seem to be required. The Device ID element (and the Device ID KDE) explicitly states that it carries an “opaque identifier”, which seems clear enough as simple words.
* One could imagine listing “ID” as an acronym for “identifier” in subclause 3.4, but we have had that acronym used in many other contexts for years without doing so.

Clause 4:

* Many amendments add a short subclause (a few paragraphs, often) to describe the features/facilities supported, to the general description of 802.11 in clause 4. The feature(s) in our draft seem too small to be worth a new section. However, we can add to the existing subclause on MAC privacy enhancements. For example:
  + To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks. Such a STA, when returning to a previously connected network, can opt-in to exchange a device identifier that allows the network to recognize the device but protects the information from third parties.

Clause 6:

* The Device ID added to Association Request/Response needs to be added to the parameter list for the corresponding MLME primitives:
  + In 6.3.7.2.2, 6.3.7.3.2, 6.3.7.4.2 and 6.3.7.5.2 add the parameter “Device ID” at the end of the primitive parameter list, and add a row in the parameter description table:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| Device ID | Device ID element | As defined in 9.4.2.296a | Specifies the Device ID for the requesting STA. Optionally present if Device ID is supported, otherwise not present. |

* + NOTE: If desired, the phrase “Device ID is supported” can be replaced by a check for a MIB attribute being true. However, the MIB attribute usage recommendations in 11-15/0535r13, §S 3.6, seem clear that this is not necessary.

TBDs:

* One in Z.1, one in Z.3. I think these are referring to the new 12.2.11 (in which case the “Privacy Protection procedures” in Z.1 should change to “Device ID procedures”, also).