IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for CIDs 7, 21, 114  |
| Date: 2023- 09 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Proposed text for the Identifiable Random MAC scheme to cover the case when a duplicate IRM is provided by the STA.

Rev 1 – Added option for “Not Recognized”.

Rev 2 – edits

Rev 3 – added clause 6 edits to Action frame option.

Rev 4 – meeting 9/12/2023. Decision to go with Action Frames

Rev 5 – meeting 9/13/2023. Resolved

**Background on Duplicate IRM**

**Probabilities:** 100 stored IRMs - 1 in 14 billion

 1000 stored IRMs – 1 in 141 million

 10000 stored IRMs – 1 in 1.4 million

Doing it twice? Astronomical.

What do these probabilities mean?

* If AP has 1000 STAs registering per day, and 1000 stored IRMs, how long before 0.5 chance of duplicate? – 192 YEARS
* 10,000 stored addresses and 1000 STAs per day? – 1.92 years

So, need to solve this is very dependent upon how many STAs do we expect an ESS to store, BUT there is a rare possibility.

**Action frames.**

On each association or PASN authentication, the STA provides a new IRM to the AP. If the STA provides an IRM that is already being stored by the AP (for another STA) then there is a “Duplicate”. Although this should be an extremely rare event, in order for the AP to indicate this to the STA, and for the STA to be able to provide a new IRM, it is proposed to add two IRM Action frames.

**REVISED**

***Insert new line in Table 6.1 MLME SA Interface***

Service Name MLME-XXX Type Reference Comments

IRM Duplicate IRMDUPLICATE 1 9.6.aa 12.2.11.2

***Insert new line in 9.4.1.11, Table 9-79***

Code Meaning See subclause Robust Group addressed privacy

33 IRM Action 9.6.aa Yes No

~~33~~34-125Reserved

***Insert new clause at end of 9.6 Action frame format details:***

**9.6.aa IRM Action frame details**

**9.6.aa.1 General**

Two Action frame formats are defined for IRM purposes. These frames are identified by the single octet IRM Action field, which follows immediately after the Category field. The values of the IRM Action field are defined in Table 9-bbb (IRM Action field).

**Table 9-bbb – IRM Action field**

|  |  |
| --- | --- |
| Action field value | Meaning |
| 0 | Duplicate IRM  |
| 1 | New IRM  |
| 2-255 | Reserved |

**9.6.aa.2 Duplicate IRM**

The Duplicate IRM frame is transmitted by an AP to a non-AP STA that associated or authenticated using PASN to the AP and provided a new IRM that the AP already has stored for another STA. The format of the Duplicate IRM Action field is shown in Figure 9-ccc.

|  |  |
| --- | --- |
| Category | IRM Action |

 Octets: 1 1

**Figure – 9-ccc – Duplicate IRM Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

**9.6.aa.3 New IRM**

The New IRM frame is transmitted from a non-AP STA to an AP in response to a Duplicate IRM frame. The format of the New IRM Action field is shown in Figure 9-ddd.

|  |  |  |
| --- | --- | --- |
| Category | IRM Action | IRM |

 Octets: 1 1 6

**Figure – 9-ddd – New IRM Action field format**

The Category field is defined in 9.4.1.1.1(Action field)

The IRM Action field is defined in Table 9-bbb in 9.6.aa.1 (General).

The IRM field is a 48 bit MAC Address.

***At P32.54, make following edits:***

When associating to an AP that advertises support for IRM, the non-AP STA may ~~allocate~~ provide a new IRM ~~MAC address~~ to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication, including the IRM element in the Association Response frame. When using PASN, the non-AP STA may ~~allocate~~ provide a new IRM ~~MAC address~~ to the AP by including the IRM element in the third PASN frame.

If the new IRM is already in use within the IEEE 802 LAN, or identical to a most recently received IRM for another non-AP STA, then, after association or authentication using PASN, the AP may send a Duplicate IRM frame (see 9.6.aa.2) to the non-AP STA indicating to the STA that the provided IRM is a duplicate. The non-AP STA may then respond with a New IRM frame (see 9.6.aa.3) which provides a new IRM to the AP.

***Add a Class 1a frame under subsection 11.3.3 Frame filtering based on STA state in 802.11az-2022 as follows:***

b) Class 1a framesIn an infrastructure BSS when PTKSA from PASN authentication exists.1) Protected Fine Timing frames (9.6.34)2) Unicast SA Query (11.13)3) IRM Action frame (9.6.aa)