IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Text for CIDs 7, 21, 114 | | | | |
| Date: 2023- 08 | | | | |
| 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”

**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.

**Option 1 is to ignore it**. If AP sees duplicate and flags it. Then next time either STA associates, then AP will return “IRM not recognized” and ‘starts again’.

**Option 2 is to add status code**

**4w HS**

Option #A – keep IRM KDE with new IRM in msg 4.

If duplicate, STA associates, then AP sends Action frame with IRM status “Duplicate”, STA sends Action frame with new “IRM”.

Option #B – move IRM KDE with new IRM to msg 2,

Then, if duplicate, AP sends Status in msg 3 “duplicate”, STA sends another IRM in msg 4.  No Action frame required.

**FILS**

STA sends IRM IE with new IRM in Association Request (as now)

Option#A - AP sends IRM status “duplicate” in Association Response

STA then sends Action frame with a new IRM.

Option #B – AP does not send IRM status in Association Response,

If duplicate, STA associates, then AP sends Action frame with IRM status “Duplicate”, STA sends Action frame with new “IRM”.

**PASN**

STA sends new IRM in Auth msg 3

If duplicate, then AP sends Action frame with IRM status “Duplicate”, STA sends Action frame with new “IRM”.

To keep the process the same, i.e., in case of duplicate, AP sends action frame “duplicate”, propose for **4w HS Option #A and FILS Option #B?**

**Proposals:**

**Option 1**

**At 33.8 as amended re CID 135, 224**

When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, the AP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication, including an IRM element in the Association Request frame. If the AP recognizes the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 0 to indicate that the AP recognizes the IRM and the IRM field is not present. If the AP does not recognize the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 1 to indicate that AP does not recognize the IRM and the IRM field is not present. The non-AP STA, on receipt of an IRM Status field of value 1, indicating the AP has not recognized the IRM, may either continue to associate to the AP and provide a new IRM in an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication, including an IRM element in the Association Request frame, ~~in~~ or disassociate. If an AP has stored the same IRM for two non-AP STAs, then if a STA uses that IRM to associate or authenticate then AP shall set the IRM status field to 1 indicating “Not Recognized”.

Note 1: An AP might set an IRM status field to 1 indicating “Not Recognized” for any reason if the AP cannot unequivocally identify the non-AP STA shared identity state.

**Option 2 – Add 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. The reason is that for FILS and PASN it is considered that restarting the association/authentication is not defined behavior.

DISCUSSION:

STRAW POLL – Option 1 or 2?

**REVISED**

***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 | IRM Duplicate |
| 1 | New IRM |
| 2-255 | Reserved |

**9.6.aa.2 IRM Duplicate**

The IRM Status Action 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 IRM Status Action field is shown in Figure 9-ccc.

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

Octets: 1 1

**Figure – 9-ccc – IRM Duplicate 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 IRMK Response Action frame is transmitted from a non-AP STA to an AP in response to an IRM Duplicate Action 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 P32.58, make following edits:***

When associating to an AP that advertises support for IRM, the non-AP STA ~~may~~ shall ~~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~~ shall ~~allocate~~ provide a new IRM ~~MAC address~~ to the AP by including the IRM element in the third PASN frame. If the AP determines that the new IRM is a duplicate of an IRM that another STA has previously provided to the AP, then, after association or authentication using PASN, the AP shall send an IRM Duplicate Action 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 shall then respond with a New IRM Action frame (see 9.6.aa.3) which provides a new IRM to the AP.

NOTE: A duplicate IRM should be an extremely rare occurrence if non-AP STAs select their IRMs randomly.