IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Text for IRM  |
| Date: 2023 - March |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |
| Kurt Lumbatis | ARRIS/CommScope | Suwanee, GA, USA |  | Kurt.lumbatis@commscope.com |

Abstract

Proposed text for the IRM scheme.

R0: Written such that IRM co-exists with Device ID

R1: Incorporate the comments and additions from Jay, Kurt, etc.

This version has the following additions:

* PASN
* Status field
* MIB
* MLME

R2 Edits by Carol.

R3 corrected heading.

R4 Edited text related to PASN.

R5 Corrected “PSAN” to “PASN”

R6 Added NOTE to 12.2.12.2

Introduction:

The following provides the instructions for inserting the new text into Draft 0.2.

Instructions:

802.11 bh Draft 0.2 is base

*Add following Acronym to 3.4.*

IRM Indentifiable Random MAC address

*At 4.5.4.10, edit last sentence to read:*

Such a STA, when reconnecting to a network, can exchange a device ID that allows the network to recognize the device and/or use a MAC address that it was previously provided to the network, but protects the information from third parties.

***Clause 6.3 Edit as indicated:***

**6.3.7 Associate**

**6.3.7.2 MLME-ASSOCIATE.request**

**6.3.7.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-ASSOCIATE.request(

….

CDMG Capabilities,

CMMG Capabilities,

GLK-GCR Parameter Set,

MSCS Descriptor,

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.3.7.3 MLME-ASSOCIATE.confirm**

**6.3.7.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-ASSOCIATE.confirm(

…..

GLK-GCR Parameter Set,

MSCS Descriptor,

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.3.7.4 MLME-ASSOCIATE.indication**

**6.3.7.4.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-ASSOCIATE.indication(

….

MSCS Descriptor,

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.3.7.5 MLME-ASSOCIATE.response**

**6.3.7.5.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-ASSOCIATE.response(

…

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.3.8 Reassociate**

**6.5.8.2 MLME-REASSOCIATE.request**

**6.5.8.2.1 Function**

This primitive requests a change in association to a specified new peer MAC entity that is in an AP or PCP.

**6.5.8.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-REASSOCIATE.request(

…

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.5.8.3 MLME-REASSOCIATE.confirm**

**6.5.8.3.1 Function**

This primitive reports the results of a reassociation attempt with a specified peer MAC entity that is in an AP

or PCP.

**6.5.8.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-REASSOCIATE.confirm(

…

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.5.8.4 MLME-REASSOCIATE.indication**

**6.5.8.4.1 Function**

This primitive indicates that a specific peer MAC entity is requesting reassociation with the local MAC

entity, which is in an AP or PCP.

**6.5.8.4.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-REASSOCIATE.indication(

…

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

**6.5.8.5 MLME-REASSOCIATE.response**

**6.5.8.5.1 Function**

This primitive is used to send a response to a specific peer MAC entity that requested a reassociation with

the STA that issued this primitive, which is in an AP or PCP.

**6.5.8.5.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-REASSOCIATE.response(

…

Device ID,

IRM,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| IRM | IRMelement | As defined in9.4.2.xx (IRM element) | Specifies the IRM for therequesting STA. Optionally present if dot11FILSActivated is true and IRM is active, otherwise notpresent. |

*At 9.3.3.5 Association Request frame format*

*Insert new row in Table 9-62 Association Request frame body P23:*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |

*At 9.3.3.6 Assocaition Response frame format*

*Insert new row in Table 9-63 Association Response frame body P1031:*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |

*Insert new row in Table 9-64 Reassociation Request frame body:*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |

*Insert new row in Table 9-65 Reassociation Response frame body:*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| <ANA> | IRM | The IRM element is optionally present when using FILS authentication; otherwise, it is not present |

*At 9.4.2.1 Insert new row in Table 9-128 Element IDs P23:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| Device ID (see 9.4.2.x (Device ID element)) | 255 | <ANA> | No | No |
| IRM (see 9.4.2.xx IRM element) | 255 | <ANA> | No | No |

*At 9.4.2.241 Insert new row in Table 9-363 Extended Capabilities field, P24:*

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | Device ID Active | The STA sets the Device ID Active field to 1 when dot11DeviceIDActivated is true to indicate Device ID is active. Otherwise, the STA sets the Device ID Active field to 0. |
| <ANA> | IRM Active | A STA sets IRM Active subfield to 1 when dot11IRMActivated is true to indicate IRM is active. Otherwise, the STA sets the IRM Active field to to 0.  |

*Insert following subclause after 9.4.2.296a “Device ID element” P 24:*

9.4.2.x IRM element

The IRM element contains a determined MAC address. The format of the IRM element is shown in Figure 9-y.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | IRM status | IRM |

 Octets 1 1 1 1 6

**Figure 9-y IRM element**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

**The IRM Status field indicates the current status of the IRM.**

**When sent from a non-AP STA to an AP, the IRM Status field is reserved.**

**When sent from an AP to a non-AP STA, the IRM Status field contains one of the following values:**

|  |  |  |
| --- | --- | --- |
| **IRM Status** | **Name** | **Meaning** |
| **0** | **Recognized** | **Indicates the IRM was recognized by the AP.** |
| **1** | **Not Recognized** | **Indicates the IRM was not recognized by the AP.** |
| **2-255** | **Reserved** |  |

The IRM field is 48-bit MAC address when sent from a non-AP STA to an AP.

The IRM field is reserved when sent from AP to non-AP STA.

**12. Security**

*Add the following new subclause after 12.2.10 (i.e., immediately before 12.3)*

**12.2.11 Changing MAC address**

To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10). For some services, however, it may be desirable by the user that the non-AP STA is identified by the AP and network services.

An AP may provide a device ID to a non-AP STA to allow any AP in the ESS to recognize the non-AP STA when it returns to that ESS even if the non-AP STA changes its MAC Address. The non-AP STA may provide that device ID to any AP in the same ESS upon a new association. Exchanges of the device ID are protected from third parties.

When using IRM, a non-AP STA may provide a random MAC address to AP either when it associates or when it performs PASN authentication. The non-AP STA may then use that IRM MAC address as its TA when it returns to that ESS or AP such that the non-AP STA may be identified pre-association.

Device ID and IRM may be used together.

***Renumber Device ID indication clause 12.2.11 as 12.2.11.1.***

Note to Editor: This a reprint of 22/1329r17 but first para is deleted and added to 12.2.11 above as the second paragraph.

**12.2.11.1 Device ID indication**

A non-AP STA indicates activation of device ID for a particular ESS by setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.241 - RSNExtension Element) in (Re)Association Request frames sent to any AP in the ESS. An AP indicates activation of Device ID by setting the Device ID Active field to 1 in the Extended RSN Capabilities field in Beacon, (Re)Association Response, and Probe Response frames. All APs in a given ESS shall set this field to the same value.

A STA shall not send a device ID to any STA that does not indicate Device ID is active.

A non-AP STA shall send a device ID when required by the procedures described below via the following frames (known as“non-AP STA Identity frames”):

1. When using FILS authentication in the Device ID element in the (Re)Association Request frame.
2. When not using FILS authentication in the Device ID KDE in message 2 of the 4 way handshake.

An AP shall send a device ID when required by the procedures described below via the following frames (known as “AP Identity frames”):

1. When using FILS authentication in the Device ID element in the (Re)Association Response frame.
2. When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

A non-AP STA that is associating with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP and the non-AP STA has not previously associated with any AP in the ESS, shall not send a device ID in the non-AP STA Identity frame. Similarly, if the non-AP STA is associating with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP but the non-AP STA no longer has a device ID for that ESS for implementation-specific reasons (for example, configuration changes have lost the device ID, or sufficient time has passed since the last association to the ESS so that the device ID has been deleted), then the non-AP STA shall not send a device ID in the non-AP STA Identity frame.

A non-AP STA that is associating with any AP in an ESS with Device ID active for both the non-AP STA and the AP and the non-AP STA has a saved device ID for the ESS shall send the most recently received device ID for that ESS in the non-AP STA Identity frame.

When an AP with Device ID active receives a non-AP STA Identity frame from a non-AP STA with Device ID active and the received device ID is recognized, the AP shall perform one of the following actions:

1. Send a zero-length device ID and set Identifier Status to “Recognized” in the appropriate AP Identity frame.
2. Assign a new device ID to the non-AP STA, send the device ID, and set Identifier Status to “Recognized” in the appropriate AP Identity frame.

When a non-AP STA receives an AP Identity frame with Identifier Status equal to “Recognized” it can 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 non-AP STA’s current MAC address.

When a non-AP STA receives an AP Identity frame with the Identifier Status equal to “Not Recognized”, it must assume that no shared identity state exists with the AP or ESS (as per the concepts of 12.2.10) and the non-AP STA must (re)establish any desired, shared identity state per the procedures previously described.

***Insert following new sub clause:***

**12.2.12.2 Identifiable Random MAC address (IRM) operation**

A non-AP STA indicates activation of IRM for a particular ESS by setting the IRM Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.241 - RSNExtension Element) in (Re)Association Request frames sent to any AP in the ESS. An AP indicates activation of IRM by setting the IRM Active field to 1 in the Extended RSN Capabilities field in Beacon, (Re)Association Response, and Probe Response frames. All APs in each ESS shall set this field to the same value.

Each time the non-AP STA associates with an AP/ESS, it provides a new IRM MAC address to the AP/ESS during the RSN association. The non-AP STA may then use that IRM MAC address as its TA the next time it requests association to that same AP/ESS. The non-AP STA may also use that IRM MAC address as its TA for any probes, directed or broadcast, public action frame, authentication and (re)association frame, that it may transmit when it intends to be identified.

When associating to an AP that advertises support for IRM, the non-AP STA may allocate 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 a new IRM MAC address to the AP by including the IRM element in the third PASN frame.

The IRM Status field in the IRM KDE or IRM element is reserved when transmitted by the non-AP STA.

The non-AP STA should store the newly allocated IRM MAC address as an identifier for use with that AP/ESS and the AP/ESS should store that IRM MAC address as an identifier for that non-AP STA. The non-AP STA then may use that allocated IRM MAC address as its TA when it next associates or uses PASN to preassociate with that same AP or another AP in the same ESS. In so doing, the AP/ESS will identify the non-AP STA.

NOTE: Allocating a new IRM MAC during each association or PASN preassociation ensures that the non-AP STA will use a different TA for the next association or PASN preassociation, and hence that non-AP STA is unidentifiable to a third party.

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 Response frame. If the AP recognizes the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 1 and the IRM field is reserved. If the AP does not recognize the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 0 and the IRM field is reserved. The non-AP STA, on receipt of an IRM Status field of value 1 may either continue to associate to the AP or disassociate.

NOTE: In the case of an initial association to an AP/ESS, the AP will indicate that the non-AP STA is not recognized, but the non-AP STA would ignore that.

An IRM MAC address is a 48-bit address that is constructed from the locally administered address space (see 12.2.10). A non-AP STA should generate the IRM MAC addresses on a random basis such that a returning non-AP STA cannot be identified by a third party from the TA it is using.

When a non-AP STA sends an Authentication Request using an IRM MAC address as the TA to the AP that was allocated that address, then that AP can identify the non-AP STA before association is started or completed. A non-AP STA may use that address for direct or broadcast probing for an AP or ESS that was allocated that address, such that the AP may identify the non-AP STA and note that that particular non-AP STA is within range of the WM, but only if the non-AP STA wants to be identifiable at that time. A non-AP STA that has allocated an IRM MAC address to an AP/ESS, may use that address in a public action frame (e.g., ANQP frame) such that the AP/ESS may identify the non-AP STA, if that non-AP STA had previously associated or used PASN to preassociate with that AP/ESS.

NOTE: In States 1 and 2, the IRM MAC address is recommended to be used only in authentication and association frames. To ensure good STA privacy, a non-AP STA is recommended to change its IRM MAC Address in every 4-way handshake.

* EAPOL-Key frames

*Add a new row into Table 12-10 (KDE selectors) P26 as shown below:*

|  |
| --- |
| * KDE selectors
 |
| OUI | Data type | Meaning |
| 00-0F-AC | <ANA> | Device ID KDE |
| 00-0F-AC | <ANA> | IRM KDE |

*Make following additions for the new KDE at the end of 12.7.2 as shown below:*

The format of the IRM KDE is shown in Figure 12-48b (IRM KDE format).

|  |  |
| --- | --- |
| IRM Status | IRM |

 Octets 1 6

Figure 12-48b—IRM KDE format

**The IRM Status field indicates the current status of the IRM.**

**When sent from a non-AP STA to an AP, the IRM Status field is reserved.**

**When sent from an AP to a non-AP STA, the IRM Status field contains one of the following values:**

|  |  |  |
| --- | --- | --- |
| **IRM Status** | **Name** | **Meaning** |
| **0** | **Recognized** | **Indicates the IRM was recognized by the AP.** |
| **1** | **Not Recognized** | **Indicates the IRM was not recognized by the AP.** |
| **2-255** | **Reserved** |  |

The IRM field is 48-bit MAC address when sent from a non-AP STA to an AP.

The IRM field is reserved when send from AP to non-AP STA.

* EAPOL-Key frame notation

*Insert following text after device ID KDE (shown for reference)*

 OCI KDE is a KDE containing operating channel information

 Device ID KDE is a KDE containing a device identifier

 IRM KDE is a KDE containing IRM MAC addresses.

* 4-way handshake
* General

*Modify 12.7.6.1 P27 as shown below:*

RSNA defines a protocol using EAPOL-Key frames called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID})

Message 2: Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or {RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE} or {RSNE, OCI KDE, RSNXE} or {RSNE, Device ID KDE} or {RSNE, OCI KDE, Device ID KDE} or {RSNE, RSNXE, Device ID KDE} or {RSNE, OCI KDE, RSNXE,Device ID KDE})

Message 3: AuthenticatorSupplicant:
EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or
{RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or
{RSNE, GTK[N], OCI KDE, RSNXE} or
{RSNE, GTK[N], Device ID KDE} or {RSNE, GTK[N], OCI KDE, Device ID KDE} or
{RSNE, GTK[N], RSNXE, Device ID KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, Device ID KDE} or

{RSNE, GTK[N], IRM KDE} or {RSNE, GTK[N], OCI KDE, IRM KDE} or
{RSNE, GTK[N], RSNXE, IRM KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, IRM KDE})

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{IRM KDE}).

**12.7.6.4 4-way handshake message 3**

*Modify 12.7.6.4 as shown below:*

* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
* Additionally, may include a Device ID KDE
* Additionally, may include an IRM KDE.
* The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.

**12.7.6.5 4-way handshake message 4**

Key Data Length = length of Key Data field in octets

Key Data = Additionally, includes an IRM KDE when dot11IRMActivated is true, otherwise, none required(#1954); RSNEs and Multi-band elements shall not be included(#1962)

 *Modify 12.12.3.2 as shown below:*

**12.12.3.2 PASN Frame Construction and Processing**

**Otherwise the STA begins the construction the third PASN frame** as follows:

— 9.4.1.1 (Authentication Algorithm Number field) set to 7 (PASN Authentication)

— 9.4.1.2 (Authentication Transaction Sequence Number field) set to 3

— Status code indicating success

….

— If dot11RSNAOperatingChannelValidationActivated is true, including an OCI Element containing an OCI element as defined in 9.4.2.236 (OCI element)

— If dot11IRMActivated is true, including a IRM element containing an IRM as defined in (9.4.2.X IRM element), if any. The IRM element shall be encrypted with the cipher suite of AES-128-CMAC.

— 9.4.2.118 (A MIC element) with MIC computed as specified in 12.12.8 (MIC computation for PASN third frame)

*Make following changes in Annex C.3*

*Insert in dot11StationConfigentry*

Dot11StationConfigEntry ::= SEQUENCE

{

dot11StationID MacAddress,

dot11MediumOccupancyLimit Unsigned32,

dot11CFPollable TruthValue,

dot11CFPPeriod Unsigned32,

dot11CFPMaxDuration Unsigned32,

dot11AuthenticationResponseTimeout Unsigned32,

dot11PrivacyOptionImplemented TruthValue,

dot11PowerManagementMode INTEGER,

dot11DesiredSSID OCTET STRING,

dot11DesiredBSSType INTEGER,

.

.

.

dot11UnsolicitedPADActivated TruthValue,

dot11MACPrivacyActivated TruthValue,

dot11GASExtensionImplemented TruthValue,

dot11LocallyAdministeredMACConfig Unsigned32,

dot11BeaconProtectionEnabled TruthValue,

dot11MSCSActivated TruthValue,

dot11LocalMACAddressPolicyActivated TruthValue,

dot11BSSMaxIdlePeriodIndicationByNonAPSTA TruthValue,

dot11DeviceIDActivated TruthValue,

dot11IRMActivated TruthValue

*Insert at end of dot11StationConfigEntry*

dot11IRMActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity or the SME.

Changes take effect as soon as practical in the implementation.

This attribute, when true at a non-AP STA, indicates that the STA might

send an IRM.

This attribute, when true at an AP indicates that the AP

supports IRM."

DEFVAL { false }

::= { dot11StationConfigEntry <ANA> }