IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Text for MAAD for TGbh Draft 0.2 | | | | |
| Date: 2022-07 | | | | |
| 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 MAAD MAC scheme as per 22/0737r2

Device ID indication and MAAD will then be covered.

AP and STA can advertise support for either or both. No selection, computations or calculations are required. Recommended that AP supports either or both dependent upon its Use Case or upper layer application. STA should support both.

Device ID – AP sends ID in msg 3, STA sends ID back in msg 2 on every associaition

MAAD – AP sends MAAD MAC in msg 3 on every association, STA uses MAAD MAC as TA on next association.

See 22/0908r1 for detailed discussion on how the schemes simply co-exist.

Introduction:

The MAAD scheme uses an ID allocated by an AP during a previous RSN association as the TA for a new association. The TA is changing every association.

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.***

MAAD MAC Address Designation

***At 4.5.4.10, edit last sentence to read***

Such a STA, when reconnecting to a network, can opt-in to exchange a device identifier that allows the network to recognize the device and/or use a MAC address that has been allocated by the network, whilst still protecting the information from third parties.

***Clause 6.3***

***We will need an “MLME-RCM” primitive so that the SME can instruct the MLME to set up which supported schemes device ID and/or MAAD. Work in ARC and TGme will probably change the way this is written. The primitive will consist of a single MLME-RCM.request.***

***Note to editor: The MAAD element has not been added to the 6.3 clause Associate. It is assumed that the MAAD is dealt with at the MLME and therefore is not required in the primitive.***

***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> | MAAD | The MAAD 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> | MAAD | The MAAD 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> | MAAD | The MAAD 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> | MAAD | The MAAD 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 |
| MAAD (see 9.4.2.xx MAAD 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 support | The STA sets the Device ID Support field to 1 to indicate support for Device ID indication. Otherwise, the STA sets the Device ID field to 0. |
| <ANA> | MAAD Capability | A STA sets MAAD Capability subfield to 1 to indicate support for MAAD and sets to 0 if MAAD is not supported. |

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

9.4.2.x MAAD element

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

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | MAAD MAC |

Octets 1 1 1 6

**Figure 9-y MAAD element**

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

The MAAD MAC field is a 48-bit MAC address.

**12. Security**

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

**12.2.11 Mitigation of random and changing MAC (RCM) 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 to the user that the non-AP STA is identified by the AP and network services. Device ID indication and MAAD may be used to identify the non-AP STA whilst still being unidentifiable to a third party.

When using device ID indication, an AP may provide a device ID, contained in a device ID KDE in message 3 of the 4-way handshake, to a non-AP STA and the non-AP STA may provide that same device ID, in a device ID KDE in message 2 of the 4-way handshake, to any AP in the same ESS to allow the network to recognize the same non-AP STA when it returns to the ESS even if it changes its MAC address.

When using MAAD, an AP may provide a random MAC address (MAAD MAC address) contained in a MAAD KDE in message 3 of the 4-way handshake, to a non-AP STA when it associates, and the non-AP STA may then use that MAAD MAC address as its TA when associating the next time to that ESS or AP. Hence, that AP or ESS can also recognize that non-AP STA pre-association.

A non-AP STA and an AP may indicate support for device ID indication and MAAD either individually or in combination. An MLME-RCM.request may be used to set which scheme(s) the STA supports

Note: An AP may indicate support for device ID and/or MAAD as required by an upper layer application. A non-AP STA may indicate support for device ID and MAAD to be compatible with different AP/networks.

**12.2.11.1 Device ID indication**

~~An AP may provide an identifier to a non-AP STA and the non-AP STA may opt-in to providing that identifier to any AP in the same ESS to allow the network to recognize the same non-AP STA when it returns to the ESS even if it changes its MAC address. Exchanges of this identifier information are protected from third parties to limit the tracking capability to the APs in an ESS~~.

A non-AP STA indicates support for this capability in the Device ID Support subfield in the Extended RSN Capabilities field (see 9.4.2.241 (RSN Extension Element)). An AP shall not send an identifier to a non-AP STA that does not indicate support for this capability.

When using FILS authentication, the non-AP STA sends the identifier, if it has one and opts-in to using it, in the Association Request frame and the AP sends a new identifier in the Association Response frame. When using FT, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial mobility domain association the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4; the identifier or a new identifier are not exchanged during the FT protocol reassociations within the same ESS. For other cases, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial 4-way handshake in the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4. When the non-AP STA sends the opaque identifier, it shall send the most recently received value from an AP in the ESS without modification.

**12.2.12.2 MAC Address Designation (MAAD) operation**

A STA advertises support for MAAD by setting the MAAD Capability subfield to 1 in the Extended Capabilites element in Probe Response, Association Response and Reassociation Response frames.

Each time the non-AP STA associates to the AP/ESS, it receives a new MAAD MAC address during the RSN association. The non-AP STA may then use that MAAD MAC address as its TA the next time it probes or requests association to that same AP/ESS.

When the associating non-AP STA advertises support for MAAD, during the initial mobility domain association the AP may allocate a new MAAD MAC address to the non-AP STA by including a MAAD KDE in EAPOL-Key message 3/4, or, when using FILS authentication, including the MAAD element in the Association Response frame.

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

Note 1: Allocating a new MAAD MAC during each association ensures that the non-AP STA will use a different TA for each association and hence that non-AP STA is unidentifiable to a third party.

The MAAD MAC address is a 48-bit address that is constructed from the locally administered address space (see 12.2.10). The non-AP STA may then store this address and use it as the TA in the next association request to that same AP. An AP should generate the MAAD 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. A list of MAAD MACs and respective non-AP STAs shall be stored by the AP and used as an identifier for each non-AP STA. A non-AP STA should store the latest MAAD MAC received from a particular AP such that the next time the non-AP STA associates to that AP, the AP can identify the non-AP STA.

When a non-AP STA sends an Association Request using an allocated MAAD MAC address as the TA, to the AP that allocated that address, then that AP can identify the non-AP STA before association is started or completed. A non-AP STA that has been allocated a MAAD MAC address, may use that address when directly probing the AP or ESS that 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. A non-AP STA that has been allocated a MAAD MAC address, may use that address in an ANQP packet so that the AP may identify the non-AP STA, if that non-AP STA had previously associated with that AP.

* 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> | MAAD KDE |

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

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

|  |
| --- |
| MAAD MAC |

Octets 6

Figure 12-48b—MAAD KDE format

The MAAD MAC field contains a MAAD MAC address.

* EAPOL-Key frame notation

***Insert following text after OCI KDE (shown for reference)***

OCI KDE is a KDE containing operating channel information

Device ID KDE is a KDE containing a device identifier

MAAD KDE is a KDE containing a MAAD MAC

* 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], MAAD KDE} or {RSNE, GTK[N], OCI KDE, MAAD KDE} or   
{RSNE, GTK[N], RSNXE, MAAD KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, MAAD KDE} or  
{RSNE, GTK[N], MAAD KDE} or {RSNE, GTK[N], OCI KDE, MAAD KDE} or   
{RSNE, GTK[N], RSNXE, Device ID, MAAD KDE} or   
{RSNE, GTK[N], OCI KDE, RSNXE, Device ID, MAAD KDE})

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

* 4-way handshake message 3

***At P 28 Modify 12.7.6.4.4 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 a MAAD 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.