IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D0.4 Capability bit for DS MAC Address |
| Date: 2025-01-06 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes capability bit for DS MAC address

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.7 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.7 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

**Discussion:**

There are feedbacks that to enable address mapping based on DS MAC address, additional implementation efforts are required.

The original intention of DS MAC address is to allow changing OTA MAC address during reassociation. Without support of DS MAC address, privacy is still improved for the initial connection.

To preserve the intention of allowing progressive privacy improvement, this document proposes capability bit for the support of DS MAC address.

**Proposed Texts:**

**TGbi Editor: *Modify 9.4.2.240 as shown below***

* RSNXE

***Insert the following new rows to Table 9-373 while maintaining the numerical order and updating the reserved range (not all lines shown):***

* Extended RSN Capabilities field

|  |  |  |
| --- | --- | --- |
| Bit | Information | Notes |
| … |  |  |
| <ANA> | DS MAC Address Support | The DS MAC Address Support field is set to 1 when dot11DSMACAddressActivated is true and is set to 0 otherwise.  |

**TGbi Editor: *Modify 9.3.3.5 as shown below***

* Association Request frame format

***Insert new rows to Table 9-64 in numeric order (not all lines shown):.***

* Association Request frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| <Last assigned+1> | DS MAC Address | The DS MAC Address element is present if the Association Request frame is encrypted, dot11DSMACAddressActivated is true, and the peer supports DS MAC Address; otherwise, it is not present. |

**TGbi Editor: *Modify 9.3.3.7 as shown below***

* Reassociation Request frame format

***Insert new rows to Table 9-66 in numeric order (not all lines shown):.***

* Reassociation Request frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| <Last assigned+1> | DS MAC Address | The DS MAC Address element is present if the Reassociation Request frame is encrypted, dot11DSMACAddressActivated is true, and the peer supports DS MAC Address; otherwise, it is not present. |

**TGbi Editor: *Modify 12.16.6 as shown below***

* (Re)Association Request/Response Frame Encryption(#1488)

This subclause defines rules to encrypt the Frame Body field of the (Re)Association Request/Response frame and to include a DS MAC Address element in the encrypted (Re)Association Request frame.

* Non-MLO(#1416)

An EDP non-AP STA that sets the (Re)Association Frame Encryption(#1488) Support field in the RSNXE to 1 may indicate a pairwise cipher, establish a(#1444) PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the (Re)Association Frame Encryption(#1488) Support field in the RSNXE to 1.

An EDP non-AP STA shall randomize its over-the-air MAC address during a BSS transition(#Ed) if the BSS transition procedure uses an(#1455) encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP STA and a temporal key (TK) is derived during Authentication frame exchange between the EDP non-AP STA and an EDP AP, (#1445)the EDP non-AP STA shall encrypt the (Re)Association Request frame transmitted to the EDP AP using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange.

If dot11DSMACAddressActivated is true and the EDP AP sets the DS MAC Address Support field in the RSNXE to 1, the EDP non-AP STA shall include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP for the mapping to the DS.

The EDP non-AP STA may randomize the DS MAC address. To construct a random DS MAC address, the EDP non-AP STA shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP STA shall use the same DS MAC address for the duration of its connection across an ESS.(#1462)

The EDP AP shall decrypt the (Re)Association Request frame received from the EDP non-AP STA using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange. If the decryption fails, then the EDP AP shall reject the association.(#1463)

The EDP AP shall encrypt the (Re)Association Response frame transmitted to the EDP non-AP STA in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange.

If the FILS authentication and the(#1455) FT protocol are not used, the EDP AP shall include a Key Delivery(#1447) element in the (Re)Association Response frame.

If a Key Delivery element is included in the (Re)Association Response frame, the EDP AP shall construct the Key Delivery element indicating the current GTK PN in the RSC subfield, with the GTK KDE, with the IGTK KDE if management frame protection is enabled, with the BIGTK KDE if beacon protection is enabled, and(#1460) with the(#1448) WIGTK KDE if WUR frame protection is enabled.

The EDP non-AP STA shall decrypt the (Re)Association Response frame received from the EDP AP using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange. If the decryption fails, then the EDP AP shall reject the association.(#1463)

If FT protocol is not used and in the (Re)Association Response frame the RSNE fields are not identical to the corresponding RSNE fields in the Beacon and Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response.(#1143)

If FT protocol is not used and the (Re)Association Response frame includes the RSNXE, the EDP non-AP STA shall verify that this element is identical to the RSNXE included in the Beacon and Probe Response frames received from the EDP AP. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP STA shall discard the response.(#1143)

On a successful (re)association,

* The EDP non-AP STA shall process the Key Delivery element in the (Re)Association Response frame if present.(#1127)
* The EDP non-AP STA shall install(#1452) the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true.(#1127)
* The EDP AP and the EDP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)).(#1449)
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP non-AP STA shall use the indicated DS MAC address for the EDP non-AP STA to EDP AP mapping to the DS rather than the MAC address of the EDP non-AP STA.
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP AP shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP STA to EDP AP mapping to the DS rather than the MAC address of the EDP non-AP STA.

NOTE 1— If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP STA are set to the DS MAC address, which is the identity of the non-AP STA known by the DS.(#1512)

On a failed (re)association, the(#1125) established PTKSA shall be irretrievably deleted.

* MLO

A non-AP MLD that sets the (Re)Association Frame Encryption(#1488) Support field in the RSNXE to 1 may indicate a pairwise cipher, establish a(#1444) PTKSA, and derive(#1445) a temporal key (TK) through Authentication frame exchange with an EDP AP MLD if APs affiliated with the EDP AP MLD set the (Re)Association Frame Encryption(#1488) Support field in the RSNXE to 1.

NOTE 1—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

An EDP non-AP MLD shall randomize its over-the-air MAC address (including the STA MAC addresses of its affiliated STAs and its MLD MAC address)(#Ed) during a(#Ed) BSS transition if the BSS transition procedure uses an(#1455) encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP MLD and a TK is derived during Authentication frame exchange between the EDP non-AP MLD and an EDP AP MLD, then the EDP non-AP MLD shall encrypt the (Re)Association Request frame transmitted to the EDP AP MLD using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange.

The (Re)Association Request frame shall:

* Have (#1457)the Address 1 field equal to (#1457)the Address 1 field of the Authentication frame used by the non-AP MLD to establish a(#1444) PTKSA
* Have (#1457)the Address 2 field equal to (#1457)the Address 2 field of the Authentication frame used by the non-AP MLD to establish a(#1444) PTKSA
* Include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP MLD for the mapping to the DS if dot11DSMACAddressActivated is true and the APs affiliated with the EDP AP MLD set the DS MAC Address Support field in the RSNXE to 1,.

An EDP non-AP MLD may randomize its DS MAC address. To construct a random DS MAC address, the EDP non-AP MLD shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP MLD shall use the same DS MAC address for the duration of its connection across an ESS.(#1462)

The EDP AP MLD shall decrypt the (Re)Association Request frame received from the EDP non-AP MLD using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange. If the decryption fails, then (#1463)the EDP AP MLD shall reject the association.

The EDP AP MLD shall encrypt the transmitted (Re)Association Response frame transmitted to the EDP non-AP MLD in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange.

If the FILS authentication and the(#1455) FT protocol are not used, the EDP AP MLD shall include a Key Delivery element in(#1458) the (Re)Association Response frame.

If a Key Delivery(#1447) element is included in the (Re)Association Response frame, the EDP AP MLD shall construct the Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled, and with the PGTK KDE if EDP epoch is supported by both AP MLD and non-AP MLD.(#1001)

The EDP non-AP MLD shall decrypt the (Re)Association Response frame received from the EDP AP MLD using the TK and the pairwise cipher indicated(#1446) in the Authentication frame exchange. If the decryption fails, the EDP AP MLD shall reject the association(#1463).

If FT protocol is not used and in the (Re)Association Response frame the RSNE fields corresponding to each link are not identical to the corresponding RSNE fields of the link in the Beacon and Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD, the EDP non-AP MLD shall discard the response.(#1144)

If FT protocol is not used and the (Re)Association Response frame includes the RSNXE, the EDP non-AP MLD shall verify that the RSNXE corresponding to each link is identical to the corresponding RSNXE of the link in the Beacon and Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP MLD shall discard the response.(#1144)

On successful (re)association,

* The(#1450) EDP non-AP MLD shall process the Key Delivery element in the (Re)Association Response frame if present. (#1127)
* The(#1450) EDP non-AP MLD shall install(#1452) the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and PGTK if EDP epoch is supported by both AP MLD and non-AP MLD. (#1127, #1001)
* The EDP AP MLD and the EDP non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)). (#1449)
* If the DS MAC Address element is included in the (Re)Association Request frame,,the EDP non-AP MLD shall use the indicated DS MAC address for the EDP non-AP MLD to EDP AP MLD mapping to the DS rather than the MLD MAC address of the non-AP MLD.
* If the DS MAC Address element is included in the (Re)Association Request frame,,the EDP AP MLD shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP MLD to EDP AP MLD mapping to the DS rather than the MLD MAC address of the EDP non-AP MLD.

NOTE 2— If the DS MAC Address element is included in the (Re)Association Request frame,,the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP MLD are set to the DS MAC address, which is the identity of the non-AP MLD known by the DS.(#1512)

On failed (re)association, the(#1125) established PTKSA shall be irretrievably deleted.

* **TGbi Editor: *Modify C.3 as shown below***MIB detail(#1499)

***Insert new entry to "Dot11StationConfigEntry" as follows (not all lines shown):***

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11StationConfig TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Dot11StationConfigEntry ::= SEQUENCE

 {

 …….

 dot11EPDPKEActivated TruthValue,

 dot11GroupEpochActivated TruthValue,

 dot11EpochStartTimeMargin Unsigned32,

 dot11EpochTransitionTime Unsigned32,

 dot11EDPRobustIndividuallyAddressedManagementFrameActivated

 TruthValue,(#1497)

 dot11EDPCapabilitiesAndOperationParametersRequestResponseActivated

 TruthValue,(#1497)

 dot11EDPReAssociationFrameEncryptionSupportActivated TruthValue,(#1497)

 dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated

 TruthValue,(#1497)

 dot11EDPPMKSACachingPrivacySupportActivated TruthValue,(#1497)

 dot11DSMACAddressActivated TruthValue

}

***Insert the following at the end of the dot11StationConfig TABLE:***

…(existing texts)….

dot11DSMACAddressActivated 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 for the next MLME-START.request primitive or MLME-JOIN.request primitive. This attribute, when true, indicates the capability to support DS MAC Address is enabled. The capability is disabled otherwise."

 DEFVAL { false }

 ::= { dot11StationConfigEntry <ANA> }

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* End of dot11StationConfig TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*