IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bi – Support for rotating MAC addresses while associated in MLO and non-MLO cases |
| Date: September 13, 2022 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Antonio de la Oliva | Interdigital Ltd, UC3M |  |  | aoliva@it.uc3m.es |
| Joseph Levy | Interdigital Ltd, |  |  |  |
| Others |  |  |  |  |
|  |  |  |  |  |

 Abstract

This submission tackles the required modifications to the standard to support modification of the A2 MAC Address while the STA is associated.

This contribution tackles MLD and non-MLD cases, and PV0 frames. Baseline for this document is REVme\_D2.0.

**Note for understanding this contribution:**

Any EP frame may be addressed to a STA which is protecting its receiving address. Therefore, the frame may be addressed to an otaMAC (over the air MAC address) used to mask the address of the receiving STA. Through this contribution, we refer to this address as receiving otaMAC.

The same EP frame or a different EP frame, may be send by an STA which is protecting its transmitting address. Therefore, the frame uses an otaMAC as transmitting address. We refer to this address as transmitting otaMAC in this contribution.

The anonymization of frames depends on a pre-established DSMAC (MAC address used for association and authentication) and otaMAC binding. This document assumes a single RSNA between transmitting and receiving DSMACs, which is used to encrypt and decrypt frames even if the frames use associated transmitting and receiving otaMACs.

In the case of MLO, the transmitting and receiving MLD MAC addresses play the same role as the DSMAC for each peer of the communication. In the following clause, we introduce language to include this idea in the specification.

Proposed contribution

**Changes to standard text are marked in red**

**3 Definitions**

otaMAC: over the air medium access control address

*NOTE -- A temporal MAC address used in frames transmitted over the air. The purpose of the otaMAC is to keep private the DSMAC of the STA.*

DSMAC: Distribution System MAC Address (MAC used for association and authentication)

*NOTE -- The DSMAC corresponds to the MAC address used for the association and authentication process between the AP and the STA and is the one indexed in the RSNA. This MAC address is used to set up the RSNA, for routing traffic to the STA on the DS network segment and it is also the one used for mobility related operations such as Fast Transition mechanisms.*

**4.9.6 Reference model for multi-link operation (MLO)**

MLO defines a set of procedures allowing communication over multiple links between MLDs. An MLD manages such communication over multiple links. Communication across links using different frequency bands or channels can occur simultaneously or not depending on the capabilities of both the AP MLD and the non-AP MLD (see 35.3.16.3 (Simultaneous transmit and receive (STR) operation) and 35.3.16.4 (Nonsimultaneous transmit and receive (NSTR) operation)).

The MLO procedures (see 35.3 (Multi-link operation)) allow a pair of MLDs to discover, synchronize, (de)authenticate, (re)associate, disassociate, and manage links and other resources with each other on any common bands or channels that are supported by both MLDs.

Each MLD has a single MAC-SAP. Each AP affiliated with an AP MLD has a MAC address different from any other AP affiliated with the AP MLD, and each non-AP STA affiliated with a non-AP MLD has a MAC address different from any other non-AP STA affiliated with the non-AP MLD.

An example of an AP MLD with two affiliated APs (Link 1 and Link 2) is shown in Figure 4-30a (Example MLD and the affiliated STA communication system). The figure shows an AP MLD with MLD MAC address M and the MLD lower MAC sublayers of two affiliated APs (AP1 with MAC address w and AP2 with MAC address x). The AP MLD is associated with a non-AP MLD with MLD MAC address P and the MLD lower MAC sublayers of two affiliated STAs (STA1 with MAC address y and STA2 with MAC address z) are shown. Link 1 is established between AP1 and STA1 and link 2 is established between AP2 and STA2. In general, the MAC address of an MLD and the MAC addresses of the STAs affiliated with the MLD are all different (e.g., M, P, w, x, y, and z have different values).

However, the architecture supports an implementation where M could equal either w or x, and where P could equal y or z.

In case of Enhanced Privacy (EP) operation in the MLO, the MLD MAC address (M and P in Figure 4-30a (Example MLD and the affiliated STA communication system)) play the role of DSMAC addresses. Addresses w, x, y and z are considered otaMAC addresses and are subject to change during the operation of the MLO.



**5.1.5 MAC data service architecture**

**5.1.5.1 General**

When transparent FST is not being used, the MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 5-1 (MAC data plane architecture). When transparent FST is being used, the MAC data plane architecture is shown in Figure 5-2 (MAC data plane architecture (transparent FST).

The dotted line box labeled “Role-specific behaviors” is replaced by one of several options, depending on the role of the STA. See the following subclauses

During transmission, an MSDU goes through the processes shown in the left-hand side of Figure 5-1 (MAC data plane architecture). When transparent FST is used, an MSDU first goes, as shown in Figure 5-2 (MAC data plane architecture (transparent FST), through an additional transparent FST entity that contains a demultiplexing process that forwards the MSDU down to the selected TX MSDU Rate Limiting process and from there to MAC data plane processing as described in the previous sentence. IEEE Std 802.1X-2010 may block the MSDU at the Controlled Port before the preceding processing occurs. Otherwise, at some point, the Data frames that contain all or part of the MSDU are queued per AC/TS.

A transmitting EP (Enhanced Privacy) STA shall include the block “EP anonymization” and may modify the Address 1 (e.g., from AP to non-AP STA transmission) and/or the Address 2 (e.g., from non-AP STA to AP transmission) in an MPDU, replacing the transmitting and/or receiving DSMACs by the transmitting and/or receiving otaMACs currently in use by the intended receiver of the EP MPDU (Address 1) and/or the current transmitter of the EP MPDU (Address 2).

During reception, a received Data frame goes through the processes shown in the right-hand side of of Figure 5-1 (MAC data plane architecture). Then, one or more MSDUs are delivered to the MAC SAP or, via the DSAF, to either the DS or an IEEE 802.1Q bridge port. When transparent FST is used, MSDUs originating from different PHY SAPs go, as shown in Figure 5-2 (MAC data plane architecture (transparent FST)), through a final step of a transparent FST entity that contains a multiplexing process before delivering the MSDU. The IEEE 802.1X -Controlled/Uncontrolled Ports discard any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame.

A receiving EP STA shall include the block “EP de-anonymisation” and may modify the Address 1 (e.g., from AP to non-AP STA transmission) and/or Address 2 (e.g., from non-AP STA to AP transmission) in an MPDU by replacing the otaMAC with the DSMAC.

NOTE—Many of the processes shown in Figure 5-1 (MAC data plane architecture) also apply to MMPDU flows for the MAC control plane architecture, and the processes shown at the bottom also apply to Control and Extension frames.

When transparent FST is used, the same security keys and PN counters are used by the MAC data plane to encrypt the MPDU prior to and following an FST, and the same security keys and replay counters are used to check the integrity and perform the protection of MPDUs. When nontransparent FST is used, independent RSNAs, security keys, replay counters, and PN counters have to be established for each MAC data plane to be used prior to and following an FST. When transparent FST is used, a single MAC SAP at each peer is presented to the higher layers of that peer for all of the frequency bands/channels that are identified by the same MAC address at that peer. When nontransparent FST is used, different MAC SAPs are presented to higher layers since different MAC addresses are used prior to and following an FST.



Figure 5-1 – MAC data plane architecture

The “EP anonymization” block (in transmission) may be located before the “MPDU Encryption” block, therefore modifying the MPDU before undergoing CCMP encapsulation, or after this block, modifying the frame after the encapsulation is done.

The “EP de-anonymization” block (in reception) may be located after “MPDU Decryption and Integrity” block or it may be located (and its function performed), after the “Address 1 address filtering” block. In the latter case, the modification of the MPDU is done before the decryption process is performed.

**12.5.2.3 CCMP cryptographic encapsulation**

**12.5.2.3.1 General**

The CCMP cryptographic encapsulation process is depicted in Figure 12-18 (CCMP encapsulation block diagram).

1. For secure PV0 MPDUs, CCMP encrypts the Frame Body field of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

1) Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key.

NOTE 1—Retransmitted MPDUs are not modified on retransmission. For MLO, MPDUs are not encapsulated with a new PN when retransmitted on another link.

2) Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD.

MPDU header fields that may change when retransmitted are muted by being masked to 0 or being set to a known value when calculating the AAD as described in 12.5.2.3.3 (Construct AAD).

3) In case of a secure PV0 MPDU that is an individually addressed Data frame to be encrypted by an MLD, construct the CCM nonce block as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN, transmitting MLD MAC address (a transmitting EP MLD shall use the MLD MAC as DSMAC) and the priority value of the MPDU. In case of a secure PV0 MPDU that is an individually addressed EP Data frame in a non-MLD, construct the CCM nonce block as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN, transmitting DSMAC, and the priority value of the MPDU. Otherwise, construct the CCM nonce block as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN, A2, and the priority value of the MPDU where A2 is MPDU Address 2. If the Type field of the Frame Control field is 10 (Data frame) and there is a QoS Control field present in the MPDU header, the priority value of the MPDU is equal to the value of the TID subfield of the QoS Control field (bits 0 to 3 of the QoS Control field). If the Type field of the Frame Control field is 00 (Management frame) and the frame is a QMF, the priority value of the MPDU is equal to the value in the ACI subfield of the Sequence Number field. Otherwise, the priority value of the MPDU is equal to the fixed value 0.

NOTE 2—For MLO, AAD and CCM Nonce construction for Management frames follows 12.5.2.3.4 (Construct CCM nonce) and uses the MPDU header fields to be transmitted over the affiliated STA link.

4) Construct the CCMP header as defined in 12.5.3.3.5 (Construct CCMP header for PV0 MPDUs).

5) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and the encrypted MIC. This step is known as CCM originator processing.

NOTE 3 – For EP frames, the SME keeps and RSNA association between the AP and non-AP STAs’ DSMAC addresses. The temporal key is therefore associated to the pair of DSMAC addresses used in the communication.

6) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and the encrypted MIC, as described in 12.5.3.2 (CCMP MPDU format



**Figure 12- 18 – CCMP encapsulation block diagram**

**12.5.2.3.3 Construct AAD**



**Table 12-3 – AAD length for PV0 MPDUs**

|  |  |  |
| --- | --- | --- |
| **AAD length for PV0 MPDUs** |  |  |
| **QC field** | **A4 field** | **AAD length (octets)** |
| Absent | Absent | 22 |
| Present | Absent | 24 |
| Absent | Present | 28 |
| Present | Present | 30 |

a) For PV0 MPDUs, the format of the AAD is shown in Figure 12-19 (AAD construction for PV0 MPDUs). The length of the AAD for PV0 varies depending on the presence or absence of the QC and A4 fields and is shown in Table 12-3 (AAD length for PV0 MPDUs).

The AAD is constructed from the MPDU header. The AAD includes neither the Duration/ID field nor the HT Control field because the contents of these fields might change during normal operation (e.g., due to a rate change preceding retransmission). The HT Control field might also be inserted or removed during normal operation (e.g., retransmission of an A-MPDU where the original A-MPDU included an MRQ that has already generated a response). For similar reasons, several subfields in the Frame Control field are masked to 0. For PV0 MPDUs, AAD construction is performed as follows:

1) FC – MPDU Frame Control field, with

 i) Subtype subfield (bits 4 5 6) in a Data frame masked to 0

 ii) Retry subfield (bit 11) masked to 0

 iii) Power Management subfield (bit 12) masked to 0

 iv) More Data subfield (bit 13) masked to 0

 v) Protected Frame subfield (bit 14) always set to 1

 vi) +HTC subfield (bit 15) as follows:

 — Masked to 0 in all Data frames containing a QoS Control field

 — Unmasked otherwise vii) Other subfields are not modified

2) A1 is set as follows:

* If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD (EP or not EP), then A1 is set to the MLD MAC address of the intended receiver.
* If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0 or 1, and the MPDU is an individually addressed EP Data frame, then A1 is set to the DSMAC of the intended receiver.

 — otherwise, Al is set to the MPDU Address 1 field.

3) A2 is set as follows:

* If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD (EP or not EP), then A2 is set to the MLD MAC address of the transmitting MLD.
* If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0 or 1, and the MPDU is an individually addressed EP Data frame, then A2 is set to the DSMAC of the intended transmitter.
* otherwise, A2 is set to the MPDU Address 2 field.

4) If dot11MultiLinkActivated is true, the MPDU Address 3 field is the BSSID and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then:

—A3 is set to the MLD MAC address of the AP MLD.

—Otherwise, A3 is set to the MPDU Address 3 field.

5) SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked to 0. The Fragment Number subfield is not modified.

6) A4, if present, is set as follows:

- if dot11MultiLinkActivated is true, MPDU Address 4 field is a BSSID, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then A4 is set to the MLD MAC address of the AP MLD(#13167).

- otherwise A4, if present, is set to the MPDU Address 4 field.

7) QC – QoS Control field contains the MSDU priority, if present. The QC TID is used in the construction of the AAD. When in a non-DMG BSS and both the STA and its peer have their SPP A-MSDU Capable fields equal to 1, bit 7 (the A-MSDU Present field) is used in the construction of the AAD. The remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDU Type bit 8 are used in the construction of the AAD, and the remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 9 to 15)

**12.5.2.3.4 Construct CCM nonce**

The CCM nonce is shown in Figure 12-21 (CCM nonce). The structure of the CCM Nonce Flags field of the CCM nonce is shown in Figure 12-22 (CCM Nonce Flags field).





The Priority subfield shall be set to the priority value of the MPDU (see 12.5.2.3.1 (General)).

The Management subfield shall be set to 1 if the MPDU is a Management frame and management frame protection is negotiated; otherwise, it shall be set to 0.

The PV1 subfield shall be set to 1 for a PV1 frame; otherwise, it shall be set to 0.

The Zeros subfield shall be set to 0.

If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and the MPDU is an individually addressed Data frame between an AP MLD and a non-AP MLD associated with the AP MLD, then the STA MAC Address Identified By A2 subfield shall contain the MLD MAC address of the transmitting MLD.

If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0 or 1, and the MPDU is an EP MPDU, then the STA MAC Address Identified by A2 subfield is set to the DSMAC of the transmitting STA.

Otherwise, the STA MAC Address Identified By A2 subfield shall contain the Address 2 field from the MAC header for PV0 MPDUs and the MAC address identified by the A2 field in the MAC header for PV1 MPDUs (see 9.8.3.2 (Address fields))

The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

A transmitter shall not use an MSDU or A-MSDU priority if this would cause the total number of priorities used during the lifetime of the SA to exceed the number of replay counters supported by the receiver (for a pairwise SA) or all the receivers (for a group SA) for that SA. The transmitter shall not reorder CCMP protected frames that are transmitted to the same RA within a replay counter, but may reorder frames across replay counters. One possible reason for reordering frames is the MSDU or A‑MSDU priority.

The transmitter shall preserve the order of protected robust Management frames that are transmitted to the same DA without the QMF service. When the QMF service is used, the transmitter shall not reorder robust IQMFs within an AC when the frames are transmitted to the same RA.

A CCMP protected individually addressed robust Management frame shall be protected using the same TK as a Data frame.

**12.5.2.4 CCMP decapsulation**

**12.5.2.4.1 General**

Figure 12-23 (CCMP decapsulation block diagram) depicts the CCMP decapsulation process and is described as follows.

1. For secure PV0 MPDUs, CCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:
2. The encrypted MPDU is parsed to construct the AAD (see 12.5.2.3.3 (Construct AAD)) and nonce (see 12.5.2.3.4 (Construct CCM nonce)) values. In case the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see 12.5.2.3.3 (Construct AAD)) and nonce (see 12.5.2.3.4 (Construct CCM nonce)) values. In case the To DS and From DS bits of the MAC header are not both set to 1 or 0, and the MPDU is an individually addressed EP MPDU, then the transmitting and receiving DSMACs are passed to construct the AAD (see 12.5.2.3.3 (Construct AAD)) and nonce values (see 12.5.2.3.4 (Construct CCM nonce)).
3. The MIC is extracted for use in CCM integrity checking.
4. CCM recipient processing uses the temporal key, AAD, nonce, encrypted MIC, and MPDU cipher text data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU plaintext data.

NOTE X – For EP frames, the SME keeps and RSNA association between the AP and non-AP STAs’ DSMAC addresses. The temporal key is therefore associated to the pair of DSMAC addresses used in the communication.

1. The received MPDU header and the MPDU plaintext data from CCM recipient processing are concatenated to form a plaintext MPDU.
2. The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session(#193), and TID (for Data frames) or ACI (for QMFs).

See 12.5.2.4.2 (CCM recipient processing) to 12.5.2.4.4 (PN and replay detection) for details of this processing.

When the received frame is a CCMP protected individually addressed robust Management frame or PV1 Management frame, contents of the MMPDU body after protection is removed shall be delivered to the SME via the MLME primitive designated for that MMPDU or PV1 Management frame rather than through the MA‑UNITDATA.indication primitive.



**Figure 12- 23 – CCMP decapsulation block diagram**