IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for 11be D1.0 AAD and Nonce CIDs |
| Date: 2021-11-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGbe comment collection 36 (TGbe Draft 1.0).

* CIDs: 6718, 6720 (2 CIDs)

Revisions:

* Rev 0: Initial version of the document.
1. **Introduction**

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 TGbe Draft. The introduction and the explanation of the proposed changes are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe Draft (i.e. they are instructions to the 802.11be editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Clause  | Page.Line | Comment | Proposed Change | Resolution |
| 6718 | Rojan Chitrakar | 12.5.3.4.1 | 217.25 | "In addition, if dot11MultiLinkActivated is true, either or both of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD,..." The receiving MLD needs to check many fields of the MPDU and also check whether the transmitting STA is affiliated with an MLD in order to decide what addresses to use in AAD and Nonce. The decapsulation logic will be greatly simplified if the transmitting STA directly signaled in the MPDU (e.g. using 1 bit in the CCMP header) if MLD MAC Address were used for the construction of AAD and Nonce. | If a transmitting STA uses MLD MAC Address during the construction of AAD and Nonce, it will set one reserved bit in the CCMP header of the MPDU to 1. During depcapsulation, the crypto engine in the STA of the receiving MLD can simply use this bit to decide whether to use the MLD MAC Address or the Address fields of the MPDU to construct the AAD and Nonce. Commenter will bring related submission. | **Revised.**Agree with the comment that if a protected Data frame carries an indication that the MLD MAC Addresses were used during the CCMP encapsulation of the frame, the decision whether to use MLD MAC Addresses or A1/A2/A3 addresses during the CCMP decapsulation will be greatly simplified. TGbe editor to make the changes shown in IEEE 802.11-21/1279r0 under all headings that include CID 6718. |
| 6720 | Rojan Chitrakar | 12.5.5.4.1 | 217.45 | "In addition, if dot11MultiLinkActivated is true, either or both of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD,..." The receiving MLD needs to check many fields of the MPDU and also check whether the transmitting STA is affiliated with an MLD in order to decide what addresses to use in AAD and Nonce. The decapsulation logic will be greatly simplified if the transmitting STA directly signaled in the MPDU (e.g. using 1 bit in the CCMP header) if MLD MAC Address were used for the construction of AAD and Nonce. | If a transmitting STA uses MLD MAC Address during the construction of AAD and Nonce, it will set one reserved bit in the CCMP header of the MPDU to 1. During depcapsulation, the crypto engine in the STA of the receiving MLD can simply use this bit to decide whether to use the MLD MAC Address or the Address fields of the MPDU to construct the AAD and Nonce. Commenter will bring related submission. | **Revised.**Agree with the comment that if a protected Data frame carries an indication that the MLD MAC Addresses were used during the GCMP encapsulation of the frame, the decision whether to use MLD MAC Addresses or A1/A2/A3 addresses during the GCMP decapsulation will be greatly simplified. TGbe editor to make the changes shown in IEEE 802.11-21/1279r0 under all headings that include CID 6720. |

**Discussion:**

As of 11be\_D1.3, during the encapsulation/decapsulation of individually addressed data frames between two MLDs, MLD MAC Addresses are used for the construction of AAD and Nonce:

Figure from 21/1609r0 (Po-kai)



Address 1 replaced with MLD MAC Address of the **receiving MLD**

Address 2 replaced with MLD MAC Address of the **transmitting MLD**

11be\_D1.3 describes the CCMP decapsulation as:



For an AP MLD, to decide whether to use MLD MAC Addresses, or the A1/A2/A3(/A4) fields of a protected data frame for the construction of the AAD and nonce during CCMP decapsulation, the CCMP decapslation block in the AP MLD needs to know whether the transmitter is a STA affiliated with an associated MLD (in which case MLD MAC Addresses are used for the construction of the AAD and nonce), or it is an associated non-MLD STA (in which case the A1/A2/A3(/A4) fields of the frame are used for the construction of the AAD and nonce). While the other information required to make the decision of whether to use MLD MAC Addresses, or the A1/A2/A3 fields for the construction of the AAD and nonce, can be obtained from the MAC header of the frame itself, **the frame doesn’t indicate whether the transmitter is a STA affiliated with an MLD**. This is especially relevant if the AP MLD implements the External key-holder security architecture (see 20/1545r0).

|  |
| --- |
|  |
| Figure from 20/1545r0 (Gaurav Patwardhan) |

Taking a simplified example of an AP MLD that supports a throughput of 30 Gbps (see 11be PAR) and assuming each Data frame is 11,454 octets (maximum MPDU size), **the AP MLD could be required to decapsulate upto 2,500,000 frames per second**! **Any simplification in the decapsulation logic to avoid confusions in the MAC Address selection during the construction of AAD and Nonce would be beneficial**.

As for non-AP MLDs, today individually addressed data frames (To DS = From DS = 0) transmitted in a single link TDLS direct link between two non-AP MLDs follow the baseline rule for the construction of AAD and Nonce (i.e., MLD MAC Addresses are not used). However the individually addressed data frames received from the associated AP MLD will be encapsulated using the MLD MAC Addresses. **This opens up the possibility of confusions in the MAC Address selection during the construction of AAD and Nonce for non-AP MLDs** as well.

**Proposal:**

CCMP/GCMP cryptographic encapsulation

During the CCMP/GCMP cryptographic encapsulation, the transmitter sets **a bit in the CCMP Header (proposing the LSB of the 3rd octet, called MLD subfield) to indicate whether the MDPU Address fields or the** **MLD MAC Addresses are used for the construction of the AAD and nonce**. The MLD subfield is set to 1 if MLD MAC Addresses are used for the construction of the AAD and nonce, otherwise it is set to 0. Example for CCMP is shown below:



CCMP/GCMP cryptographic decapsulation

During the CCMP/GCMP cryptographic decapsulation, **the receiver uses only the MLD bit in the CCMP Header to decide whether to use the MDPU Address fields or the MLD MAC Addresses for the construction of the AAD and nonce**. If the MLD subfield is set to 1, MLD MAC Addresses are used for the construction of the AAD and nonce, otherwise the the MDPU Address fields are used.

Baselines are 11REVme\_D0.4 and 11be\_D1.3.

SP: Do you agree to incorporate the changes proposed in IEEE 802.11-21/1279r0 to the lastest 11be draft for the following CIDs?

CID: 6718, 6720

12.5.3.2 CCMP MPDU format (CIDs 6718)

***TGbe editor: Replace Figure 12-16 with the below figure (Track Change On):***

****

**Figure 12-16—Expanded CCMP MPDU**

***TGbe editor: Modify the following paragraphs as below (Track Change On):***

For secure PV0 MPDUs, CCMP-128 processing expands the original MPDU size by 16 octets, 8 octets for the CCMP Header field and 8 octets for the MIC field. CCMP-256 processing expands the original MPDU size by 24 octets, 8 octets for the CCMP Header field, and 16 octets for the MIC field. The CCMP Header field is constructed from the PN, MLD, ExtIV, and Key ID subfields. PN is a 48-bit PN represented as an array of 6 octets. PN5 is the most significant octet of the PN, and PN0 is the least significant.

The MLD subfield (bit 0) of the Options octet signals whether MLD MAC Addresses are used for the construction of AAD and Nonce. The MLD subfield is set to 1 if MLD MAC Addresses are used for the constructions of AAD and Nonce, otherwise it is set to 0. The MLD subfield is always set to 0 when the transmitting STA is not affiliated with an MLD.

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header by a total of 8 octets, compared to the 4 octets added to the MPDU header when WEP is used. The ExtIV bit (bit 5) is always set to 1 for CCMP.

12.5.3.3 CCMP cryptographic encapsulation (CIDs 6718)

12.5.3.3.3 Construct AAD

***TGbe editor: Modify the subclause as below (Track Change On):***

## Change the first paragraph as follows:

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 fol- lows:

FC – MPDU Frame Control field, with

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

Retry subfield (bit 11) masked to 0

Power Management subfield (bit 12) masked to 0

More Data subfield (bit 13) masked to 0

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

~~A1 – MPDU Address 1 field.~~ For a transmitting STA, if dot11MultiLinkActivated is true, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to:

* the MLD MAC address of the intended receiver MLD of the MPDU.
* otherwise, Al is set to MPDU Address 1 field.

For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then A1 is set to the MLD MAC address of the intended receiver MLD of the MPDU. Otherwise, Al is set to MPDU Address 1 field.

~~A2 – MPDU Address 2 field.~~ For a transmitting STA, if dot11MultiLinkActivated is true, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to:

* the MLD MAC address of the transmitting MLD of the MPDU.
* otherwise, A2 is set to MPDU Address 2 field.

For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then A2 is set to the MLD MAC address of the transmitting MLD of the MPDU. Otherwise, A2 is set to MPDU Address 2 field.

~~A3 – MPDU Address 3 field.~~ For a transmitting STA, if dot11MultiLinkActivated is true, MPDU Address 3 field is BSSID and the MPDU is an individually addressed Data frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then:

* (#4924)A3 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD.
* (#4924)Otherwise, A3 is set to the MPDU Address 3 field.

For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then A3 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD. Otherwise, A3 is set to the MPDU Address 3 field.

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.

~~A4 – MPDU Address field, if present.~~A4, if present, is set as follows:

* For a transmitting STA, if dot11MultiLinkActivated is true, MPDU Address 4 field is a BSSID, and the MPDU is an individually addressed Data frame (#4924)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, where the corresponding AP with the BSSID is affiliated with the AP MLD. Otherwise A4, if present, is set to the MPDU Address 4 field.
* For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then A4 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD. Otherwise A4, if present, is set to the MPDU Address 4 field.

12.5.3.3.4 Construct CCM nonce

***TGbe editor: Modify the sixth paragraph as below (Track Change On):***

For a transmitting STA, if dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed Data frame, then the STA Or MLD MAC Address Identified By A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ STA Or MLD 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)).

***TGbe editor: Add a new paragraph after the sixth paragraph as below (Track Change On):***

For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then the STA Or MLD MAC Address Identified By A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the STA Or MLD 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)).

12.5.3.3.5 Construct CCMP header for PV0 MPDUs

***TGbe editor: Modify the subclause as below (Track Change On):***

The format of the 8-octet CCMP header is given in 12.5.3.2 (CCMP MPDU format). The header encodes the PN, Key ID, and ExtIV field values used to encrypt the MPDU. The MLD subfield is set as described in 12.5.3.2 (CCMP MPDU format).

12.5.3.4 CCMP decapsulation

12.5.3.4.1 General

***TGbe editor: Modify the paragraph as below (Track Change On):***

For secure PV0 MPDUs, CCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:

The encrypted MPDU is parsed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values. In addition, if dot11MultiLinkActivated is true, and the MLD subfield in the CCMP header is equal to 1, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values.

12.5.5 GCM protocol (GCMP) (CIDs 6720)

12.5.5.2 GCMP MPDU format

***TGbe editor: Replace Figure 12-16 with the below figure (Track Change On):***

****

**Figure 12-26—Expanded GCMP MPDU**

***TGbe editor: Modify the following paragraphs as below (Track Change On):***

GCMP processing expands the original MPDU size by 24 octets, 8 octets for the GCMP Header field and 16 octets for the MIC field. The GCMP Header field is constructed from the PN, MLD and Key ID subfields. The 48-bit PN is represented as an array of 6 octets. PN5 is the most significant octet of the PN, and PN0 is the least significant.

The MLD subfield (bit 0) of the Options octet signals whether MLD MAC Addresses are used for the construction of AAD and Nonce. The MLD subfield is set to 1 if MLD MAC Addresses are used for the constructions of AAD and Nonce, otherwise it is set to 0. The MLD subfield is always set to 0 when the transmitting STA is not affiliated with an MLD.

The ExtIV subfield (bit 5) of the Key ID octet is always set to 1 for GCMP.

Bits 6–7 of the Key ID octet are for the Key ID subfield. The remaining bits of the Key ID octet are reserved.

12.5.5.3.4 Construct GCM nonce

***TGbe editor: Modify the second paragraph as below (Track Change On):***

For a transmitting STA, f dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed Data frame, then the A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ A2 subfield shall contain the Address 2 field from the MAC header.

***TGbe editor: Add a new paragraph after the second paragraph as below (Track Change On):***

For a receiving STA, if dot11MultiLinkActivated is true, and the MLD subfield in the GCMP header is equal to 1, then the A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the A2 subfield shall contain the Address 2 field from the MAC header.

12.5.5.3.5 Construct GCMP header

The format of the 8-octet GCMP header is given in 12.5.5.2 (GCMP MPDU format). The header encodes the PN and Key ID field values used to encrypt the MPDU. The MLD subfield is set as described in 12.5.5.2 (GCMP MPDU format).

12.5.5.4 GCMP decapsulation

12.5.5.4.1 General

***TGbe editor: Modify the paragraph as below (Track Change On):***

For secure PV0 MPDUs, CCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:

The encrypted MPDU is parsed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values. In addition, if dot11MultiLinkActivated is true, and the MLD subfield in the GCMP header is equal to 1, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values.