IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed resolutions to some LB270 comments | | | | |
| Date: 2022-11-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses and proposes resolutions to the following LB270 (REVme/D2.0) comments:

* CID 3135

r1: updates based on 2022-11-14 PM2 discussion / ready for motion

r2: update Clause 13 language to set the new MIC Length subfield as appropriate

**CID 3135**

P2910 L24 12.7.3

Comment:

The recently added AKM 00-0F-AC:25 (FT/SAE with variable key length) made parsing of the first Authentication frame in the FT protocol case inconvenient since the AP receiving this frame may not have been part of the SAE authentication exchange with the non-AP STA and as such, it does not yet know which finite cyclic group was used with SAE and as such, does not know the length of the MIC field. However, this AP needs to be able to parse the FTE in this frame and, in particular, find the subelements from the FTE after the variable length MIC field. This cannot be done robustly without knowing the length of the MIC field (and the 8 octet length of the likely first subelement makes this even more inconvenient since that happens to be the difference between possible MIC field lengths).

Proposed Change:

Specify the length of the MIC field in the FTE for the new AKM:  
- at P1037 L8 (Figure 9-418), add a new subfield "MIC Length" for B1..B3 (3 bits), leaving B4..B7 (4 bits) as the new size for Reserved  
- at P1037 (was 1036) L18 add a new paragraph:  
 "The MIC Length subfield defines the length of the MIC field when using AKM 00-0F-AC:25. The value of this subfield is not applicable for other AKMs. Table 9-<new> defines the available values for this."  
- at P1037 (was 1036) L18 add a new table "Table 9-<new>--MIC length" with columns "Value" and "MIC field length in octets" and values "0 = 16 or not applicable", "1 = 24", "2 = 32", "3-7 = Reserved".

Discussion:

The comment is on the last row of this table:



The identified issue has been identified in an early implementation of the new AKM and the proposed change addresses the identified parsing issue, but has couple of editorial issues that are addressed in the following redline version.

Proposed Resolution:

REVISED. Add the proposed subfield with some editorial cleanup by incorporating changes under the “Changes for CID 3135” header in document <this document>.

**Changes for CID 3135**

*Modify 9.4.2.47 (D2.0 P1037 L8-18) as shown:*

**9.4.2.47 FTE**

The fast BSS transition element (FTE) includes information needed to perform the FT authentication

sequence or FILS authentication during a fast BSS transition in an RSN. This element is shown in Figure 9-

417 (FTE format).



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

The MIC Control field is 2 octets and is defined in Figure 9-418 (MIC Control field format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0 | B1 B3 | B4 B7 | B8 B15 |
|  | RSNXE Used | MIC Length | Reserved | Element Count |
| Bits: | 1 | 3 | 4 | 8 |

**Figure 9-418—MIC Control field format**

The RSNXE Used subfield of the MIC Control field is used in the third and fourth messages of the FT

authentication sequence to indicate whether the STA transmitting the frame containing the FTE includes an

RSNXE in other frames. This subfield is set to 0 in other frames.

When using AKM 00-0F-AC:25, the MIC Length subfield defines the length of the MIC field, as defined in Table 9-<new>. This subfield is reserved for other AKMs.

**Table 9-<new>—MIC Length subfield values**

|  |  |
| --- | --- |
| **Value** | **MIC field length in octets** |
| 0 | 16 |
| 1 | 24 |
| 2 | 32 |
| 3-7 | Reserved |

The Element Count subfield of the MIC Control field contains the number of elements that are included in

the message integrity code (MIC) calculation.

When the Element Count subfield has a value greater than 0, the MIC field contains a MIC. Otherwise, the

MIC field is set to 0.

The length of the MIC field depends on the negotiated AKM selector and the value of the MIC Length subfield, when not reserved, and is specified in Table 12-11 (Integrity and key wrap algorithms) and Table 9-<new>.

The ANonce field contains a value chosen by the R1KH.

The SNonce field contains a value chosen by the S1KH.

**13.4.2 FT initial mobility domain association in an RSN**

*Modify 13.4.2 (D2.0 P2969 L11) as shown:*

…

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities of the AP, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTE shall have a MIC element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0. The RSNXE Used subfield of the MIC Control field shall be set to 0. When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.

**13.8.2 FT authentication sequence: contents of first message**

*Modify 13.8.2 (D2.0 P2990 L32) as shown:*

…

If present, the FTE shall be set as follows:

* R0KH-ID shall be the value of R0KH-ID obtained by the FTO during its FT initial mobility domain association exchange.
* SNonce shall be set to a value chosen randomly by the FTO, see 12.7.5 (Nonce generation) for a recommended procedure.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* All other fields shall be set to 0.

**13.8.3 FT authentication sequence: contents of second message**

*Modify 13.8.3 (D2.0 P2990 L61) as shown:*

…

If present, the FTE shall be set as follows:

* R0KH-ID shall be identical to the R0KH-ID provided by the FTO in the first message.
* R1KH-ID shall be set to the R1KH-ID of the target AP, from dot11FTR1KeyHolderID.
* ANonce shall be set to a value chosen randomly by the target AP, see 12.7.5 (Nonce generation) for a recommended procedure.
* SNonce shall be set to the value contained in the first message of this sequence.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* All other fields shall be set to 0.

**13.8.4 FT authentication sequence: contents of third message**

*Modify 13.8.4 (D2.0 P2991 L27) as shown:*

…

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in the RSNXE; otherwise this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* When the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.

…

* All other fields shall be set to 0.

**13.8.5 FT authentication sequence: contents of fourth message**

*Modify 13.8.5 (D2.0 P2992 L36) as shown:*

…

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the target AP includes an RSNXE in its Beacon and Probe Response frames; otherwise this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC capability, the Authenticator shall include FT OCI subelement in FTE.

…

* All other fields shall be set to 0.