IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FT 4-way handshake | | | | |
| Date: 2016-01-21 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes changes to the description of the FT 4-way handshake to clarify the applicability of the rules to all cases in which 4-way handshake can be used with FT (i.e., in addition to the existing initial mobility domain association, also the PTK rekeying during an association started with FT protocol needs to be covered). These changes address a comment that I filed in REVmc/D5.0 SB recirculation letter ballot. That comment identifies an interoperability issue with deployed FT implementations.

Rev 1: “the Message” 🡪 “this Message”

# Comment:

Clause 13.4.2 page 2072 line 40

comment:

The page 2072 lines 33-51 is the only place in the standard where the contents of the FTE and MDE in EAPOL-Key messages 2 and 3 of the 4-way handshake is described. The title of this subclause is "FT initial mobility domain association in an RSN" which is not exactly ideal for describing 4-way handshake behavior since that handshare is used both in the initial mobility domain association and also in cases where FT protocol authentication is used. For the latter, 4-way handshake is used to rekey PTK either by AP or non-AP STA request, e.g., due to a configured maximum lifetime for the PTK (or EAP authentication; EAP re-authentication is followed by 4-way handshake).

An interoperability issue has come up in this area since there are deployed AP devices that do not follow these FTE/MDE expectations for the case where 4-way handshake is initiated on an association that used the FT protocol. This results in the association getting dropped when trying to go through the exchange.

It would be good for the standard to be clearer on how the 4-way handshake works in all FT cases.

It should also be noted that the final paragraph of this subclause discusses one case of PTKSA lifetime expiration detected by the non-AP STA based on TIE[KeyLifetime]. This is also a bit unclear on whether this is supposed to apply only for the initial mobility domain association (likely not) or also FT protocol cases. It is possible that

there was an intent to not allow EAPOL exchanges at all in an association started with FT protocol. If that is indeed the case, this is not described completely enough (and those example deployed APs speak on this..). If the group decides that this is the approach to use here, the proposed change in the comment should be replaced with such description that makes it clear that neither the AP nor the non-AP STA shall initiate an EAPOL frame exchange after the initial 4-way handshake in the initial mobility domain association or in association started with FT protocol. It should be noted that this would break TKIP counter measures since the non-AP STA would have no means for notifying the AP of a receipt of a Michael MIC failure (e.g., when using TKIP as the

group cipher).

proposed change:

A minimal change to address this would be to add a note at page 2072 line 52 stating that these rules apply to all 4-way handshake cases in FT: "NOTE--The exceptions described above apply to both the initial mobility domain association and also to use of 4-way handshake in an association started with FT protocol."

A more complete change would be to move this description of 4-way handshake (starting from "The EAPOL-Key frame notation.." on page 2072 line 21 and ending at the end of the current 13.4.2).

# Proposed changes to the REVmc draft

**12.7.6.3 4-way handshake message 2**

*Change the EAPOL-Key Key Data construction in REVmc/D5.0 page 2010 line 13 through page 2010 line 15 as shown:*

Key Data =

* included RSNE – the sending STA’s RSNE for PTK generation or peer RSNE for the current operationg band, and when this Message 2 is part of a fast BSS transition Initial Mobility Domain Association or an association started through FT protocol, the PMKR1Name calculated by the S1KH according to the procedures of 12.7.1.7.4 (PMK-R1) is included in the PMKID field of the RSNE and the FTE and MDE are also included, or;

*Change the EAPOL-Key reception process in REVmc/D5.0 page 2010 line 38-55 as shown:*

On reception of Message 2, the Authenticator checks that the key replay counter corresponds to the outstanding Message 1. If not, it silently discards the message. Otherwise, the Authenticator:

1. Derives PTK.
2. Verifies the Message 2 MIC.
3. If the calculated MIC does not match the MIC that the Supplicant included in the EAPOL-Key frame, the Authenticator silently discards Message 2.
4. If the MIC is valid and this Message 2 is part of a fast BSS transition Initial Mobility Domain Association or an association started through FT protocol, the Authenticator checks that all fields of the RSNE other than the PMKID field bitwise matches the fields from the (Re)Association Request frame and that the FTE and MDE are the same as those provided in the AP’s (Re)Association Response frame. If the MIC is valid and this Message 2 is not part of a fast BSS transition Initial Mobility Domain Association or an association started through FT protocol, the Authenticator checks that the RSNE bitwise matches that from the (Re)Association Request frame.
5. If these are not exactly the same, the Authenticator uses MLME-DEAUTHENTICATE.request primitive to terminate the association.
6. If they do match bitwise, the Authenticator constructs Message 3.

**12.7.6.4 4-way handshake message 3**

*Change the EAPOL-Key Key Data construction in REVmc/D5.0 page 2011 line 59 through page 2012 line 2 as shown:*

Key Data =

* For PTK generation for the current operating band, the AP’s Beacon/Probe Response frame’s RSNE for the current operating band, and, optionally, a second RSNE that is the Authenticator’s pairwise cipher suite assignment for the current operating band, and, if a group cipher has been negotiated, the encapsulated GTK and the GTK’s key identifier (see 12.7.2 (EAPOL-Key frames)) for the current operating band, and if management frame protection is negotiated, the IGTK KDE, and when this Message 2 is part of a fast BSS transition Initial Mobility Domain Association or an association started through FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.7.4 (PMK-R1) in the PMKID field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK key lifetime in the TIE[KeyLifetime]; or

*Change the EAPOL-Key reception process in REVmc/D5.0 page 2012 line 57 through page 2013 line 2 as shown:*

On reception of Message 3, the Supplicant silently discards the message if the Key Replay Counter field value has already been used or if the ANonce value in Message 3 differs from the ANonce value in Message 1. The Supplicant also:

a) Verifies the RSNE. If this Message 3 is part of a fast BSS transition Initial Mobility Domain Association or an association started through FT protocol, the Supplicant verifies that the PMKR1Name in the PMKID field of the RSNE is identical to the value sent in this Message 2 and all other fields of the RSNE are identical to the fields in the RSNE present in the Beacon or Probe Response frames and that the FTE and MDE are the same as in the (Re)Association Response frame. Otherwise, the Supplicant verifies that the RSNE is identical to that the STA received in the Beacon or Probe Response frame. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant uses the pairwise cipher suite specified in the second RSNE or deauthenticates.

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

*REVmc/D5.0 page 2072 lines 32-51:*

The message sequence is described in 12.7.6 (4-way handshake).