### IEEE P802.11Wireless LANs

|  |
| --- |
| 11be D1.0 PDT for fast ML transition |
| Date: 2021-06-01 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation | 2200 Mission College Blvd, Santa Clara, CA 950542200  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |
| Daniel F Bravo |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes spec texts for the following motions:

802.11be supports to reuse existing frame exchange of over-the-air fast BSS transition (FT) for fast ML transition in R1.

[Motion 131, #SP197, [58] and [200]]

For a non-AP MLD and an AP MLD in a FT initial mobility domain operation, use non-AP MLD address as S1KH-ID and S0KH-ID and AP MLD address as R1KH-ID. Use AP MLD address and non-AP MLD address to compute PMKID, PTK, and PTKName.

For a non-AP MLD and a target AP MLD in an over-the-air FT operation, use non-AP MLD address as S1KH-ID and AP MLD address as R1KH-ID. Use AP MLD address and non-AP MLD address to compute PMKID, PTK, and PTKName.

NOTE – It is an R1 feature.

[Motion 131, #SP203, [58] and [201]]

For a non-AP MLD and an AP MLD in a FT initial mobility domain operation, different GTK/IGTK/BIGTK of different setup links are delivered in one FT 4-way handshake.

For a non-AP MLD and a target AP MLD in an over-the-air FT operation, different GTK/IGTK/BIGTK of different setup links are delivered in FTE of reassociation response of the over-the-air FT protocol.

NOTE – It is an R1 feature.

[Motion 131, #SP204, [58] and [201]]

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 TGbe D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D1.0 Draft (i.e. they are instructions to the 802.11 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.***

**Discussion:** *None.*

**Propose:**

*TGbe editor: Change Clause 3.1* *as follows (track change on):*

**3.1 Definitions**

**authenticator address (AA):** The medium access control (MAC) address of the IEEE 802.1X
Authenticator’s STA or MLD.

**Supplicant address (SPA):** The medium access control (MAC) address of the IEEE 802.1X Supplicant’s
STA or MLD.

*TGbe editor: Modify Clause 4.5.3.2* *as follows (track change on):*

* Mobility types

***Change the first paragraph as follows:***

The three transition types of significance to this standard that describe the mobility of STAs within a net-work are as follows:

* ***No-transition:*** In this type, two subclasses that are usually indistinguishable are identified:
* Static—no motion.
* Local movement—movement within the PHY range of the communicating STAs, i.e., movement within a basic service area (BSA).

***BSS-transition:*** This type is defined as follows:

* a STA movement from one BSS in one ESS to another BSS within the same ESS.
* A non-AP MLD movement from being associated with one AP MLD in one ESS and each non-AP STA affiliated with the non-AP MLD being in one BSS to be reassociated with another AP MLD within the same ESS and each non-AP STA affiliated with the non-AP MLD after reassociation be in another BSS.
* A non-AP MLD movement from being associated with one AP MLD in one ESS and each non-AP STA affiliated with the non-AP MLD being in one BSS to be a non-AP STA that is reassociated with an AP within the same ESS and the non-AP STA be in another BSS, where the MLD MAC address of the non-AP MLD is the same as the MAC address of the non-AP STA.(#2236)
* A non-AP STA movement from being associated with one AP in one ESS and the non-AP STA be in one BSS to be a non-AP MLD that is reassociated with an AP MLD with the same ESS and each non-AP STA affiliated with the non-AP MLD be in another BSS, where the MAC address of the non-AP STA is the same as the MLD MAC address of the non-AP MLD.(#2236)

A fast BSS transition is a BSS transition that establishes the state necessary for data connectivity before the reassociation rather than after the reassociation.

* ***ESS-transition:*** This type is defined as STA movement from a BSS in one ESS to a BSS in a different ESS. This case is supported only in the sense that the STA might move. Maintenance of upper-layer connections cannot be guaranteed by IEEE Std 802.11; in fact, disruption of service is likely to occur.

**4.5.3.4 Reassociation**

*TGbe editor: Modify 4.5.3.4 Reassociation (track change on)*

***Change the last paragraph as follows:***Only the fast BSS/ transition facility can move an RSNA during reassociation. Therefore, if FT is not
used, the old RSNA is deleted and a new RSNA is constructed.

*TGbe editor: Modify 9.4.1.5 as follows (track change on)*

**9.4.1.5 Current AP Address field
*Change as follows:***If the current association is between a non-AP STA and an AP, ~~T~~the Current AP Address field is the MAC address of the AP with which the STA is currently associated. If the current association is between a non-AP MLD and an AP MLD, then the Current AP Address field is the MLD MAC address of the AP MLD with which the non-AP MLD is currently associated. The length of the Current AP Address field is 6 octets. The Current AP Address field is shown in Figure 9-87 (Current AP Address field format).

*TGbe editor: Replace every instance of “BSS/ML transition” with “BSS transition” in the following figure or clauses:*

*Figure 11-17*

11.3.4.2 Authentication—originating STA or MLD

**11.3.5.4 Non-AP, non-AP MLD, and non-PCP STA reassociation initiation procedures**

**11.3.5.5 AP, AP MLD, or PCP reassociation receipt procedures**

*TGbe editor: Modify 35.3.4.3 as follows (track change on)*

**35.3.4.3 Non-AP behavior**

(…existing texts….)

A non-AP MLD shall be able to discover an AP MLD when it receives a Neighbor Report element carried in a Management frame. If the Basic variant Multi-Link element is present in the Neighbor Report element for a reported AP, then the reported AP is affiliated with an AP MLD. The non-AP MLD shall be able to obtain, based on the contents of the Common Info field of the Basic variant Multi-Link element, the MLD information for the AP MLD with which the reported AP is affiliated. A non-AP MLD may use the information it receives from a Neighbor Report element to make a decision on performing multi-link (re)setup (see 35.3.5 (Multi-link (re)setup)) or BSS transition (see 4.5.3.2 Mobility types). A non-AP MLD shall be able to determine that two or more APs reported in different Neighbor Report elements are affiliated with the same AP MLD if the MLD MAC address of the reported APs are the same.

*TGbe editor: Change the title of 9.4.2.47* *as follows (track change on):*

* Fast BSS Transition element (FTE)

*TGbe editor: Change the first paragraph* *as follows (track change on):*

The 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 9-356 (FTE format).

*TGbe editor: Change the fourth paragraph* *as follows (track change on):*

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 or the STA affiliated with the MLD transmitting the frame containing the FTE includes an RSNXE in other frames. This subfield is set to 0 in other frames.

*TGbe editor: Change Table 9-181* *as follows (track change on):*

|  |
| --- |
| Table 9-181 Subelement IDs |
| Value | Contents of Data field |
| 0 | Reserved |
| 1 | PMK-R1 key holder identifier (R1KH-ID) |
| 2 | GTK |
| 3 | PMK-R0 key holder identifier (R0KH-ID) |
| 4 | IGTK |
| 5 | Operating Channel Information (OCI) |
| 6 | BIGTK |
| 7 | MLO GTK |
| 8 | MLO IGTK |
| 9 | MLO BIGTK |
| 10–255 | Reserved |

*TGbe editor: Change the 19th paragraph* *as follows (track change on):*

When sent by a non-AP STA or a non-AP MLD through an affiliated non-AP STA, the R0KH-ID indicates the R0KH with which the S0KH negotiated the PMK‑R0 it is using for this transition. When sent by an AP or an AP MLD through an affiliated AP, the R0KH-ID indicates the R0KH that the S0KH will be using to generate a PMK-R0 security association. It is encoded following the conventions from 9.2.2 (Conventions).

*TGbe editor: Change the following paragraphs at the end of 9.4.2.47* *as follows (track change on):*

The MLO GTK subelement contains the GTK for a link, which is encrypted (see procedures in 13.8.5 (FT authentication sequence: contents of fourth message)) and is defined in Figure xx1 (MLO GTK subelement format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Key Info | Link Info | Key Length | RSC | Wrapped Key |
| Octets: | 1 | 1 | 2 | 1 | 1 | 8 | 24–40  |
|  | Figure XX1 - MLO GTK subelement format |

The MLO GTK subelement Link Info subfield is defined in Figure XX2 (MLO GTK subelement’s Link Info subfield format).

|  |  |  |
| --- | --- | --- |
|  | B0                          B3 | B4                                    B7 |
|  | Link ID  | Reserved |
| Bits: | 4 | 4 |
| Figure XX2 - MLO GTK subelement’s Link Info subfield format |
|  |

The LinkID field contains the link identifier for the link.

The definitions of the Key Info, Key Length, RSC, and Wrapped Key fields are the same as in the GTK subelement described above.

The MLO IGTK subelement contains the IGTK for a link, used for protecting robust Management frames. The MLO IGTK subelement format is shown in Figure XX3 (MLO IGTK subelement format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Key ID | IPN | Link Info | Key Length | Wrapped Key |
| Octets: | 1 | 1 | 2 | 6 | 1 | 1 | 24-40 |
|  | Figure XX3 – MLO IGTK subelement format |

The definitions of the Key ID, IPN, Key Length, and Wrapped Key fields are the same as in the IGTK subelement described above.

The definitions of Link Info fields is the same as the MLO GTK subelement described above.

The MLO BIGTK subelement contains the BIGTK for a link, used for protecting Beacon frames. The MLO BIGTK subelement format is shown in Figure XX4 (MLO BIGTK subelement format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Key ID | BIPN | Link Info | Key Length | Wrapped Key |
| Octets: | 1 | 1 | 2 | 6 | 1 | 1 | 24-40 |
|  | Figure XX4 – MLO BIGTK subelement format |

The definitions of the Key ID, BIPN, Key Length, and Wrapped Key fields are the same as in the BIGTK subelement described above.

The definitions of Link Info fields is the same as the MLO GTK subelement described above.

*TGbe editor: Change the title of clause 13* *as follows (track change on):*

* Fast BSS transition
* Overview

*TGbe editor: Change the first four paragraphs* *as follows (track change on):*

Fast BSS transition seeks to reduce the length of time that connectivity is lost between a STA and the DS or between an MLD and the DS during a BSS transition. The FT protocols are part of the reassociation service and only apply to STA transitions between APs, or a STA or non-AP MLD transition to an AP MLD or a non-AP MLD transition to an AP within the same mobility domain within the same ESS (see 4.5.3.2).

The FT protocols require information to be exchanged during the initial association (or a later reassociation) between a STA [known as the *FT Originator* (FTO)] and AP or between a non-AP MLD [known as the *FT Originator* (FTO)] and AP MLD. The initial exchange is referred to as the *FT initial mobility domain association*. Subsequent reassociations to APs within the same mobility domain may make use of the FT protocols.

Two FT protocols are defined:

* *FT protocol.* This protocol is executed when an FTO makes a transition to a target AP or target AP MLD and does not require a resource request prior to its transition.
* *FT resource request protocol.* This protocol is executed when an FTO requires a resource request prior to its transition.

For an FTO to move to a target AP or target AP MLD utilizing the FT protocols, the message exchanges are performed using one of two methods:

* *Over-the-Air.* The FTO communicates directly with the target AP or targe AP MLD using IEEE 802.11 authentication with the FT authentication algorithm.
* *Over-the-DS.* The FTO communicates with the target AP via the current AP. The communication between the FTO and the target AP is carried in FT Action frames between the FTO and the current AP. Between the current AP and target AP, communication is via an encapsulation method described in 13.10.3 (Remote Request/Response frame definition). The current AP converts between the two encapsulations.

APs advertise both capabilities and policies for supporting the FT protocols and methods.

* Key holders
* Introduction

*TGbe editor: Change the second paragraphs* *as follows (track change on):*

The R0KH and R1KH are part of AP’s or AP MLD’s SME RSNA key management. The computation of PMK-R0 and PMK-R1, and all of the intermediate results in the computations, shall be restricted to the R0KH. The computation of PTK, and all intermediate results in its computation, shall be restricted to the R1KH.

* Authenticator key holders

*TGbe editor: Change the first paragraphs* *as follows (track change on):*

The R0KH and R1KH are responsible for the derivation of keys in the FT key hierarchy. For fast BSS transition, the functions of the IEEE 802.1X Authenticator are distributed among the R0KH and R1KHs.

*TGbe editor: Change the 7th paragraphs* *as follows (track change on):*

The R1KH shall meet the following requirements:

* The R1KH-ID shall be set to a MAC address of the physical entity that stores the PMK-R1 and uses it to generate the PTK. That same MAC address shall be used to advertise the PMK-R1 identity to the STA or non-AP MLD and the R0KH.
* The R1KH shall derive and distribute the GTK andIGTK to all connected STAs. If the R1KH identifies an AP MLD, the R1KH shall distribute the GTKs and IGTKs for setup links to all connected non-AP MLDs.
* If beacon protection is enabled, the R1KH shall derive and distribute the BIGTK and BIPN to all connected STAs. If an R1KH identifies an AP MLD, the R1KH shall derive and distribute the BIGTKs and BIPNs for setup links to all connected non-AP MLDs.
* When the PMK-R1 lifetime expires, the R1KH shall delete the PMK-R1 PMKSA and shall revoke all PTKSAs derived from the PMK-R1 using the MLME-DELETEKEYS primitive.
* The R1KH shall not expose the PMK-R1 to other parties.Supplicant key holders

*TGbe editor: Change the 2nd paragraphs* *as follows (track change on):*

The S0KH interacts with the IEEE 802.1X functional block (see Figure 4-24 (Portion of the ISO/IEC basic reference model covered in this standard) in 4.9 (Reference model)) to receive the MSK resulting from an EAP authentication or the FILS-FT resulting from a FILS authentication. The S1KH interacts with the IEEE 802.1X entity to open the Controlled Port. Both the S0KH and S1KH interactions with the IEEE 802.1X entity occur within the SME of a STA or a non-AP MLD.

* Capability and policy advertisement

*TGbe editor: Insert the following paragraph after the first paragraph* *as follows (track change on):*

The FT capability is advertised in the Beacon and Probe Response frames by including the MDE. The MDE is advertised in the Beacon and Probe Response frames to indicate the MDID, FT capability, and the FT policy.All APs affiliated with an AP MLD shall advertise the same MDE and at least one common AKM with Authentication type that indicates FT authentication.

* FT initial mobility domain association
* Overview

*TGbe editor: Change the first and second paragraphs* *as follows (track change on):*

The FT initial mobility domain association is the first (re)association in the mobility domain, where the SME of the STA or non-AP MLD enables its future use of the FT procedures.

FT initial mobility domain association is typically the first association within the ESS. In addition to Association Request and Response frames, Reassociation Request and Response frames are supported in the initial mobility domain association to enable both FT and non-FT APs or AP MLDs to be present in a single ESS.

NOTE– For MLO, the non-AP MLD and AP MLD include the Basic variant Multi-Link element in all Authentication and (Re)Association Request/Response frames. The Basic variant Multi-Link element includes the MLD address for the respective MLD and is used to establish the security association.

*TGbe editor: Change 13.4.2* *as follows (track change on):*

* FT initial mobility domain association in an RSN

A STA or a non-AP MLD indicates its support for the FT procedures by including the MDE in the (Re)Association Request frame and indicates its support of security by including the RSNE. The AP or AP MLD responds by including the FTE, MDE, and RSNE(s) in the (Re)Association Response frame. After a successful IEEE 802.1X authentication (if needed) or SAE authentication, the STA and AP or the non-AP MLD and the AP MLD perform an FT 4-way handshake. At the end of the sequence, the IEEE 802.1X Controlled Port is opened, and the FT key hierarchy has been established. The message flow between a STA and an AP is shown in Figure 13-2 (FT initial mobility domain association in an RSN).



A non-DMG STA or a non-AP MLD initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

STAAP: Authentication-Request (Open System authentication algorithm)

APSTA: Authentication-Response (Open System authentication algorithm, Status)

non-AP MLDAP MLD: Authentication-Request (Open System authentication algorithm, Basic variant Multi-Link element)

AP MLDnon-AP MLD: Authentication-Response (Open System authentication algorithm, Status, Basic variant Multi-Link element)

A DMG STA initiates the FT initial mobility domain association procedures by performing an IEEE 802.11
authentication using the SAE algorithm.

STA→AP: Authentication-Request (SAE algorithm)
AP→STA: Authentication-Response (SAE algorithm, Status)

The SME of the STA or non-AP MLD initiates the authentication exchange, through the use of the MLME‑AUTHENTICATE.request primitive, and the SME of the AP or AP MLD, respectively, responds with MLME‑AUTHENTICATE.response primitive. See 11.3.4 (Authentication and deauthentication).

Upon successful IEEE 802.11 Open System or SAE authentication, if using a suite type for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the STA shall send a (Re)Association Request frame to the AP that includes the MDE or a non-AP MLD shall send a (Re)Association Request frame that includes the MDE through an affiliated non-AP STA to the AP MLD through an affiliated AP. The contents of the MDE shall be the values advertised by the AP or any AP affiliated with the AP MLD in its Beacon or Probe Response frames. Additionally, the STA or non-AP MLD includes its security capabilities in the RSNE.

STAAP: (Re)Association Request (MDE, RSNE, RSNXE)

APSTA: (Re)Association Response (MDE, FTE[R1KH-ID, R0KH-ID], RSNXE)

non-AP MLDAP MLD: (Re)Association Request (MDE, RSNE, RSNXE, Basic variant Multi-Link element)

AP MLDnon-AP MLD: (Re)Association Response (MDE, FTE[R1KH-ID, R0KH-ID], RSNE, RSNXE, Basic variant Multi-Link element)

The SME of the STA or non-AP MLD initiates the (re)association through the use of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive. The SME of the AP or AP MLD responds to the indication with MLME-ASSOCIATE.response or MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_MDE. If an MDE is present in the (Re)Association Request frame and the contents of the RSNE do not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_AKMP.

For MLO, if the contents of the MDE received by the AP MLD do not match the contents advertised in the Beacon and Probe Response frames of APs affiliated with the AP MLD, the AP MLD shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_MDE. If an MDE is present in the (Re)Association Request frame and the contents of the RSNE do not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the AP MLD shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_AKMP.

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The (Re)Association Response frame from the AP MLD shall contain an MDE, with contents as presented in Beacon and Probe Response frames of APs affiliated with the AP MLD. The FTE shall include the key holder identities of the AP or the AP MLD, 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.

On successful (re)association, the S0KH on the STA or the non-AP MLD and the R0KH on the AP or the AP MLD, respectively, then proceed with an IEEE 802.1X authentication using EAPOL PDUs carried in IEEE 802.11 Data frames if SAE authentication was not performed (i.e., if the suite type is not 00-0F-AC:9). The S0KH shall use the value of R0KH-ID as the endpoint identifier of the NAS Client (NAS-Identifier if RADIUS is used) in the exchange as defined in IETF RFC 3748.

If IEEE 802.1X authentication was performed, then upon successful completion of authentication, the R0KH receives the MSK and authorization attributes. If SAE authentication was performed, the R0KH receives the PMK, resulting in the successful completion of SAE. If a key hierarchy already exists for this STA or non-AP MLD belonging to the same mobility domain (i.e., having the same MDID), the R0KH shall delete the existing PMK-R0 security association and PMK-R1 security associations. It then calculates the PMK-R0, PMKR0Name, and PMK‑R1 and makes the PMK-R1 available to the R1KH of the AP with which the STA is associated or the AP MLD with which the non-AP MLD is associated.

If the SME of the STA or the non-AP MLD cannot authenticate the AS, then it shall disassociate with an MLME-DISASSOCIATE.request primitive. If the AS signals the Authenticator that the STA or the non-AP MLD cannot be authenticated, then the SME of the AP or the AP MLD, respectively, shall disassociate with an MLME-DISASSOCIATE.request primitive.

If the MSK lifetime attribute is provided by the AS, the lifetime of the PMK-R0 shall not be more than the lifetime of the MSK. If the MSK lifetime attribute is not provided, the PMK-R0 lifetime shall be dot11FTR0KeyLifetime. For PSK, the PMK-R0 lifetime shall be dot11FTR0KeyLifetime. The lifetime of the PMK-R1s and PTK shall be the same as the lifetime of PMK-R0. When the key lifetime expires, each key holder shall delete its respective PMK-R0, PMK-R1, and PTK SAs.

The R1KH and S1KH then perform an FT 4-way handshake. The EAPOL-Key frame notation is defined in 12.7.4 (EAPOL-Key frame notation).

R1KHS1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {} or {MAC Address})

S1KHR1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE[PMKR1Name], MDE, FTE, RSNXE} or { RSNE[PMKR1Name], MDE, FTE, RSNXE, MAC Address, MLO Linkn})

R1KHS1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE[PMKR1Name], MDE, GTK[N], IGTK[M], BIGTK[Q], FTE, TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE} or {MLO Linkn with RSNE[PMKR1Name], MDE, MLO GTKn, MLO IGTKn, MLO BIGTKn, FTE, TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE, MAC\_Address})

S1KHR1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {} or {MAC Address})

, where MLO GTKn is MLO GTK KDE for link n, MLO IGTKn is MLO IGTK KDE for link n, and MLO BIGTKn is MLO BIGTK KDE for link n.

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

It is assumed by this standard that the reassociation deadline is administered consistently across the mobility domain. The mechanism for such consistent administration is outside the scope of this standard.

The PTK shall be calculated by the R1KH and S1KH according to the procedures given in 12.7.1.6.5 (PTK).

Upon completion of a successful FT 4-way handshake, the IEEE 802.1X Controlled Port shall be opened on both the non-AP STA and the AP or the non-AP MLD and the AP MLD. Subsequent EAPOL-Key frames shall use the key replay counter to detect replayed messages.

Upon completion of a successful FT 4-way handshake, the PTK lifetime timer is initiated. The operation of this timer prevents the PTKSA being used for longer than the value provided in the TIE[KeyLifetime] sent in message 3.

Once the PTKSA key lifetime expires, as indicated by the TIE[KeyLifetime], to continue its association in the mobility domain the STA or the non-AP MLD shall perform the FT initial mobility domain association procedures. If the AP or the AP MLD sends a Deauthentication or Disassociation frame to the STA or the non-AP MLD, respectively, with reason code INVALID\_AUTHENTICATION, then to continue its association in the mobility domain, the STA or the non-AP MLD shall perform the FT initial mobility domain association procedures with any AP or any AP MLD, respectively, in the mobility domain. If the Supplicant EAPOL state machines are triggered to send an EAPOL-Start frame after a successful initial mobility domain association, the STA or the non-AP MLD shall perform the FT initial mobility domain association procedures.

*TGbe editor: Change 13.4.3* *as follows (track change on):*

* FT initial mobility domain association in a non-RSN

In this sequence, the STA or non-AP MLD utilizes the FT procedures by including the MDE in the (Re)Association Request frame. The AP or AP MLD responds by including the MDE in the (Re)Association Response frame. The message flow between a STA and an AP is shown in Figure 13-3 (FT initial mobility domain association in a non-RSN).



The STA or non-AP MLD initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

STAAP: Authentication-Request (Open System authentication algorithm)

APSTA: Authentication-Response (Open System authentication algorithm, Status)

non-AP MLDAP MLD: Authentication-Request (Open System authentication algorithm, Basic variant Multi-Link element)

AP MLDnon-AP MLD: Authentication-Response (Open System authentication algorithm, Status, Basic variant Multi-Link element)

The SME of the STA or the non-AP MLD initiates the authentication exchange through the use of the primitive MLME‑AUTHENTICATE.request primitive, and the SME of the AP or the AP MLD responds with MLME-AUTHENTICATE.response primitive. See 11.3.4 (Authentication and deauthentication).

Upon successful IEEE 802.11 Open System authentication, the STA shall send a (Re)Association Request frame to the AP and shall include the MDE or a STA affiliated with the non-AP MLD shall send a (Re)Association Request frame to an AP affiliated with the AP MLD that includes the MDE. The contents of the MDE shall be the values advertised by the AP or any AP affiliated with the AP MLD in its Beacon or Probe Response frames.

STAAP: (Re)Association Request (MDE)

APSTA: (Re)Association Response (MDE)

non-AP MLDAP MLD: (Re)Association Request (MDE, Basic variant Multi-Link element)

AP MLDnon-AP MLD: (Re)Association Response (MDE, Basic variant Multi-Link element)

The SME of the STA or the non-AP MLD initiates the (re)association through the use of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive. The SME of the AP or the AP MLD responds to the indication with MLME-ASSOCIATE.response or MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_MDE.

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames.

If the contents of the MDE received by the AP MLD do not match the contents advertised in the Beacon and Probe Response frames of APs affiliated with the AP MLD, the AP MLD shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_MDE.

The (Re)Association Response frame from the AP MLD shall contain an MDE, with contents as presented in Beacon and Probe Response frames of APs affiliated with the AP MLD.

On successful (re)association, the AP and the non-AP STA or the AP MLD and the non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)) to enable Data frame transmission.

*TGbe editor: Change 13.5* *as follows (track change on):*

* FT protocol
* Overview

STAs and MLDs with dot11FastBSSTransitionActivated equal to true shall support the FT protocol.

The FT protocol supports resource requests as part of the reassociation. The optional FT resource request protocol (see 13.6 (FT resource request protocol)) supports resource requests prior to reassociation.

A STA or a non-AP MLD shall not use any authentication algorithm except the FT authentication algorithm when using the FT protocol.

To prevent key reinstallation attacks, the non-AP STA shall maintain a copy of the most recent GTK, IGTK, and BIGTK when present installed as part of the FT protocol as if they were installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations)) and shall refuse to update a GTK, IGTK, or a BIGTK when the key to be set matches any one of these three keys (see 6.3.19 (SetKeys)).

To prevent key reinstallation attacks, the non-AP MLD shall maintain a copy of the most recent GTK, IGTK, and BIGTK in each setup link when present installed as part of the FT protocol as if they were installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations)) and shall refuse to update a GTK, IGTK, or a BIGTK of each setup link when the key to be set matches any one of these three keys (see 6.3.19 (SetKeys)).

* Over-the-air FT protocol authentication in an RSN

The over-the-air FT protocol in an RSN to transition from current AP to target AP is shown in Figure 13-5 (Over-the-air FT protocol in an RSN).

The FTO and AP or AP MLD use the FT authentication sequence to specify the PMK-R1 security association and to provide values of SNonce and ANonce that enable a liveness proof, replay protection, and PTK separation. This exchange enables a fresh PTK to be computed in advance of reassociation. The PTKSA is used to protect the subsequent reassociation transaction, including the optional RIC-Request.

To perform an over-the-air fast BSS transition to a target AP, the FTO and target AP shall perform the following exchange:

FTOTarget AP: Authentication-Request (FTAA, 0, RSNE[PMKR0Name], MDE, FTE[SNonce, R0KH-ID])

Target APFTO: Authentication-Response (FTAA, Status, RSNE[PMKR0Name], MDE, FTE[ANonce, SNonce, R1KH-ID, R0KH-ID])

To perform an over-the-air fast BSS transition to a target AP MLD, the FTO and target AP MLD shall perform the following exchange:

FTOTarget AP MLD: Authentication-Request (FTAA, 0, RSNE[PMKR0Name], MDE, FTE[SNonce, R0KH-ID], Basic variant Multi-Link element)

Target AP MLDFTO: Authentication-Response (FTAA, Status, RSNE[PMKR0Name], MDE, FTE[ANonce, SNonce, R1KH-ID, R0KH-ID], Basic variant Multi-Link element)

The SME of the FTO initiates the authentication exchange, through the use of the MLME‑AUTHENTICATE.request primitive, and the SME of the AP or AP MLD responds with an MLME-AUTHENTICATE.response primitive. See 11.3.4 (Authentication and deauthentication). The MLME primitives for Authentication when the FT authentication algorithm is selected use only authentication transaction sequence number values 1 and 2.

In the Authentication-Request frame, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Request frame is sent by non-AP STA affiliated with the non-AP MLD. The elements in the frame, and their required contents, shall be as given in 13.8.2 (FT authentication sequence: contents of first message).

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the authentication request with status code STATUS\_INVALID\_MDE. If the contents of the MDE received by the AP MLD do not match the contents advertised in the Beacon and Probe Response frames of any AP affiliated with he AP MLD, the AP MLD shall reject the authentication request with status code STATUS\_INVALID\_MDE. If the Authentication-Request frame contains an authentication algorithm equal to FT authentication and the contents of the RSNE do not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the AP or AP MLD shall reject the authentication request with status code STATUS\_INVALID\_AKMP. If the FTE in the FT Request frame contains an invalid R0KH-ID, the AP or AP MLD shall reject the FT Request frame with status code STATUS\_INVALID\_FTE. If the RSNE in the Authentication-Request frame contains an invalid PMKR0Name and the AP or the PA MLD has determined that it is an invalid PMKR0Name, the AP or the AP MLD shall reject the authentication request with status code STATUS\_INVALID\_PMKID. If the requested R0KH is not reachable, the AP or AP MLD shall respond to the authentication request with status code R0KH\_UNREACHABLE. If the FTO selects a pairwise cipher suite in the RSNE that is different from the ones used in the Initial mobility domain association, then the AP or AP MLD shall reject the authentication request with status code STATUS\_INVALID\_PAIRWISE\_CIPHER. Subsequent to a rejection of an authentication request, the FTO may retry the authentication request.

In the Authentication-Response frame, the SA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Response frame is sent by an AP affiliated with the AP MLD, and the DA field of the message header shall be set to the MAC address of the FTO. The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, and their required contents, shall be as given in 13.8.3 (FT authentication sequence: contents of second message).

The R1KH of the target AP or target AP MLD uses the value of PMKR0Name and other information in the frame to calculate PMKR1Name. If the target AP or target AP MLD does not have the key identified by PMKR1Name, it may retrieve that key from the R0KH identified by the FTO. See 13.2 (Key holders). Upon receiving a new PMK-R1 for a STA or non-AP MLD, the target AP or target AP MLD, respectively, shall delete the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

The FTO and the target AP or target AP MLD compute the PTK and PTKName using the PMK-R1, PMKR1Name, ANonce, and SNonce, as specified in 12.7.1.6.5 (PTK). The PTKSA shall be deleted by the target AP or target AP MLD if it does not receive a Reassociation Request frame from the FTO within the reassociation deadline timeout value.

If the FTO does not receive a response to the Authentication-Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3 (STA authentication and association). If the Status Code field value returned by the target AP or target AP MLD is SUCCESS, the FTO and target AP transition to State 2 (as defined in 11.3 (STA authentication and association)); the FTO may continue with reassociation (13.7.1 (FT reassociation in an RSN)). Handling of errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

* Over-the-air FT protocol in a non-RSN

The over-the-air FT protocol in a non-RSN to transition from current AP to target AP is shown in Figure 13-8 (Over-the-air FT protocol in a non-RSN).

To perform an over-the-air fast BSS transition to a target AP in a non-RSN, the FTO and target AP shall perform the following exchange:

FTOTarget AP: Authentication-Request (FTAA, 0, MDE)

Target APFTO: Authentication-Response (FTAA, Status, MDE)

To perform an over-the-air fast BSS transition to a target AP MLD in a non-RSN, the FTO and target AP MLD shall perform the following exchange:

FTOTarget AP MLD: Authentication-Request (FTAA, 0, MDE, Basic variant Multi-Link element)

Target AP MLDFTO: Authentication-Response (FTAA, Status, MDE, Basic variant Multi-Link element)

In the Authentication-Request frame, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Request frame is sent by a non-AP STA affiliated with the non-AP MLD. The elements in the frame, and their required contents, shall be as given in 13.8.2 (FT authentication sequence: contents of first message).

If the contents of the MDE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the authentication request with status code STATUS\_INVALID\_MDE. If the contents of the MDE received by the target AP MLD do not match the contents advertised in the Beacon and Probe Response frames of any AP affiliated with the AP MLD, the target AP MLD shall reject the authentication request with status code STATUS\_INVALID\_MDE.

In the Authentication-Response frame, the SA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Response frame is sent by an AP affiliated with the AP MLD, and the DA field of the message header shall be set to the MAC address of the FTO. The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, and their required contents, shall be as given in 13.8.3 (FT authentication sequence: contents of second message).

If the FTO does not receive a response to the Authentication-Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3 (STA authentication and association). If the Status Code field value returned by the target AP or AP MLD is SUCCESS, the FTO and target AP or target AP MLD transition to State 2 (as defined in 11.3 (STA authentication and association)); the FTO may continue with reassociation (13.7.2 (FT reassociation in a non-RSN)). Handling of errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

*TGbe editor: Change 13.7* *as follows (track change on):*

* FT reassociation
* FT reassociation in an RSN

If the FTO does not send a Reassociation Request frame to the target AP or target AP MLD within the reassociation deadline interval received during the FT initial mobility domain association, the target AP or target AP MLD may delete the PTKSA, and the FTO shall abandon this transition attempt.

The FTO shall perform a reassociation directly with the target AP via the following exchange:

FTOTarget AP: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request, RSNXE)

Target APFTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N], IGTK[M], BIGTK[Q]], RIC‑Response, RSNXE)

The FTO shall perform a reassociation directly with the target AP MLD via the following exchange:

FTOTarget AP MLD: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RSNXE, Basic variant Multi-Link element)

Target AP MLDFTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, MLO GTKn, MLO IGTKn, MLO BIGTKn], RSNXE, Basic variant Multi-Link element)

, where MLO GTKn is MLO GTK subelement for link n, MLO IGTKn is MLO IGTK subelement for link n, and MLO BIGTKn is MLO BIGTK subelement for link n.

The SME of the FTO initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the AP or AP MLD responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

In the Reassociation Request frame, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Request frame is sent by a non-AP STA affiliated with the non-AP MLD. The elements in the frame, the element contents, and the MIC calculation shall be as given in 13.8.4 (FT authentication sequence: contents of third message).

The R1KH of the target AP or target AP MLD verifies the MIC in the FTE in the Reassociation Request frame and shall discard the request if the MIC is incorrect.

If the target AP includes an RSNXE in its Beacon and Probe Response frames and the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, but the Reassociation Request frame does not include an RSNXE, the R1KH of the target AP shall discard the request.

If any AP affiliated with the target AP MLD includes an RSNXE in its Beacon and Probe Response frames and the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, but the Reassociation Request frame does not include an RSNXE, the R1KH of the target AP MLD shall discard the request.

If dot11RSNAOperatingChannelValidationActivated is true and the FTO indicates OCVC capability, the target AP shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true:

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation))

Otherwise, the AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE.

If the contents of the MDE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE. If the contents of the MDE received by the target AP MLD do not match the contents advertised in the Beacon and Probe Response frames of any AP affiliated with the AP MLD, the target AP MLD shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE. If the FTE in the Reassociation Request frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce, the AP or AP MLD shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE. If the RSNE in the Reassociation Request frame contains an invalid PMKR1Name, the AP or AP MLD shall reject the Reassociation Request frame with status code STATUS\_INVALID\_PMKID.

In the Reassociation Response frame, the SA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Response frame is sent by an AP affiliated with the AP MLD, and the DA field of the message header shall be set to the MAC address of the FTO. The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, the element contents, and the MIC calculation shall be as given in 13.8.5 (FT authentication sequence: contents of fourth message).

The S1KH of the FTO verifies the MIC in the FTE in the Reassociation Response frame and shall discard the response if the MIC is incorrect.

If in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field are not identical to the corresponding RSNE fields in the Beacon and Probe Response frames received from the target AP, the S1KH of the FTO shall discard the response. If in the Reassociation Response frame each RSNE field other than the PMKID Count field and the PMKID List field of a link are not identical to the corresponding RSNE field of the link received from an AP of the target AP MLD, the S1KH of the FTO shall discard the response. If the PMKID List field does not include the correct PMKR1Name value, the S1KH of the FTO shall discard the response.

If the Beacon and Probe Response frames received from the target AP did not include an RSNXE, but the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, the S1KH of the FTO shall discard the response.

If the Beacon and Probe Response frames received from an AP affiliated with the target AP MLD did not include an RSNXE, but the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, the S1KH of the FTO shall discard the response.

If the Reassociation Response frame includes the RSNXE, the S1KH of the FTO shall verify that this element matches information included in the Beacon and Probe Response frames received from the target AP. If the Reassociation Response frame includes the RSNXE of a link, the S1KH of the FTO shall verify that this element matches information corresponding to the link received from an AP affiliated with the target AP MLD. If those frames did not include the RSNXE or if the contents of the RSNXE are not identical, the S1KH of the FTO shall discard the response.

If dot11RSNAOperatingChannelValidationActivated is true and the target AP indicates OCVC capability, FTO shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation))

Otherwise, the FTO reject the Reassociation Response frame by discarding the frame.

If an FTO is performing a reassociation exchange as part of the FT resource request protocol, then the FTO shall not include the RIC-Request in the Reassociation Request frame, and the AP shall not include the RIC-Response in the Reassociation Response frame. If the reassociation exchange is part of the FT resource request protocol and the AP is unable to honor the resources that have been placed in the accepted state for that FTO, then the AP shall reject the Reassociation Request frame and may use status code DENIED\_INSUFFICIENT\_BANDWIDTH.

If the FTO did not utilize the FT resource request protocol, the FTO may make a request for resources by including a RIC-Request (see 13.11 (Resource request procedures)) in the Reassociation Request frame. The RIC-Request is generated by the procedures of 13.11.3.1 (FTO procedures), and the RIC-Response is generated by the procedures of 13.11.3.2 (AP procedures).

If the Status Code field value returned by the target AP or target AP MLD in the response is REFUSED\_REASON\_UNSPECIFIED, TRANSACTION\_SEQUENCE\_ERROR, or REJECTED\_SEQUENCE\_TIMEOUT, then the FTO shall abandon this transition attempt. Handling of other errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

Upon a successful reassociation, the PTKSA has been established and proven live. The SME of the AP or AP MLD shall open the IEEE 802.1X Controlled Port. The FTO shall transition to State 4 (as defined in 11.3 (STA authentication and association)). If the target AP or AP MLD is distinct from the previous AP or AP MLD, the FTO shall enter State 1 with respect to the previous AP or AP MLD.

Upon a successful reassociation, the FTO shall delete any corresponding PTKSA with its previous AP or AP MLD. The SME of the FTO shall issue an MLME-DELETEKEYS.request primitive to delete the pairwise keys with the previous AP or AP MLD, and the FTO and the AP or AP MLD shall issue an MLME-SETKEYS.request primitive and MLME-SETPROTECTION.request primitive to install the pairwise keys. The PTK lifetime timer shall be initialized with the value calculated as the difference between the TIE[KeyLifetime] sent in message 3 of the FT initial mobility domain association and the time since the completion of the FT 4-way handshake during the FT initial mobility domain association.

When the IEEE 802.1X Controlled Port is opened, the EAPOL-Key frame replay counter shall be initialized to 0. The R1KH shall increment the key replay counter on each successive EAPOL-Key frame that it transmits.

* FT reassociation in a non-RSN

The FTO shall perform a reassociation with the target AP via the following exchange:

FTOTarget AP: Reassociation Request(MDE, RIC-Request)

Target APFTO: Reassociation Response(MDE, RIC-Response)

The FTO shall perform a reassociation with the target AP MLD via the following exchange:

FTOTarget AP MLD: Reassociation Request(MDE, Basic variant Multi-Link element)

Target AP MLDFTO: Reassociation Response(MDE, Basic variant Multi-Link element)

The SME of the FTO initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the AP or AP MLD responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

In the Reassociation Request frame, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Request frame is sent by a non-AP STA affiliated with the non-AP MLD. The elements in Reassociation Request frame, and their required contents, shall be as given in 13.8.4 (FT authentication sequence: contents of third message).

If the contents of the MDE received by the target AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE.

If the contents of the MDE received by the target AP MLD do not match the contents advertised in the Beacon and Probe Response frames of any AP affiliated with the AP MLD, the target AP MLD shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE.

In the Reassociation Response frame, the SA field of the message header shall be set to the BSSID of the target AP’s BSS or the MLD MAC address of the target AP MLD if the Authentication-Response frame is sent by an AP affiliated with the AP MLD, and the DA field of the message header shall be set to the MAC address of the FTO. The elements in Reassociation Response frame, and their required contents, shall be as given in 13.8.5 (FT authentication sequence: contents of fourth message). The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field).

If the FTO is performing a reassociation exchange as part of the FT resource request protocol, then the FTO shall not include the RIC-Request in the Reassociation Request frame, and the AP shall not include the RIC‑Response in the Reassociation Response frame.

If the FTO did not utilize the FT resource request protocol, the FTO may make a request for resources by including a RIC-Request (see 13.11 (Resource request procedures)) in the Reassociation Request frame. The RIC-Request is generated by the procedures of 13.11.3.1 (FTO procedures), and the RIC-Response is generated by the procedures of 13.11.3.2 (AP procedures).

If the Status Code field value returned by the target AP or target AP MLD in the response is REFUSED\_REASON\_UNSPECIFIED, TRANSACTION\_SEQUENCE\_ERROR, or REJECTED\_SEQUENCE\_TIMEOUT, then the FTO shall abandon this transition attempt. Handling of other errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

If the AP or AP MLD has dot11RSNAActivated equal to true, upon a successful reassociation, the SME shall open the IEEE 802.1X Controlled Port.

Upon a successful reassociation, the target AP or target AP MLD and the FTO shall transition to State 4 (as defined in 11.3 (STA authentication and association)). If  the target AP or target AP MLD is distinct from the previous AP or previous AP MLD, then the FTO shall enter State 1 with respect to the previous AP or previous AP MLD.

*TGbe editor: Change 13.8* *as follows (track change on):*

* FT authentication sequence
* Overview

The FT authentication sequence comprises four sets of FT elements. Each set of FT elements is referred to in 13.8 (FT authentication sequence) as a *message*. These messages are included in the FT Protocol frames or FT Resource Request Protocol frames to initiate a fast BSS transition. The FT authentication sequence is always initiated by the FTO and responded to by the target AP or target AP MLD.

In an RSN, the first two messages in the sequence allow the FTO and target AP or target AP MLD to provide association instance identifiers, SNonce and ANonce, respectively. SNonce and ANonce are chosen randomly or pseudorandomly and are used to generate a fresh PTK. The first two messages also enable the target AP or target AP MLD to provision the PMK-R1 and the FTO and target AP or target AP MLD to compute the PTK. The third and fourth messages demonstrate liveness of the peer, authenticate the elements, and enable an authenticated resource request.

When an FTO invokes the FT protocol, then the first two messages of the sequence are both carried in Authentication frames or both carried in Action frames, and these messages are described in 13.8.2 (FT authentication sequence: contents of first message) and 13.8.3 (FT authentication sequence: contents of second message). The third and fourth messages in the sequence are carried in the Reassociation Request and Reassociation Response frames and are described in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message).

When the FTO invokes the FT resource request protocol, then the first four messages of the sequence are all carried in Authentication frames or all carried in Action frames, and these messages are described in 13.8.2 (FT authentication sequence: contents of first message) to 13.8.5 (FT authentication sequence: contents of fourth message). The fifth and sixth frames of the FT resource request protocol are carried in the Reassociation Request frame and Reassociation Response frame and are described in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message).

Regardless of the transport mechanism, the information contained in the FT authentication sequence consists of the set of elements shown in Table 13-1 (FT authentication elements).

|  |
| --- |
| * FT authentication elements
 |
| Information | Presence in Authentication Sequence messages | Description |
| RSN | The RSNE is present if dot11RSNAActivated is true. | 9.4.2.24 (RSNE) |
| Mobility Domain | The Mobility Domain element is present. | 9.4.2.46 (Mobility Domain element (MDE)) |
| Fast BSS Transition | The Fast BSS Transition element is present if dot11RSNAActivated is true. | 9.4.2.47 (Fast BSS Transition element (FTE)) |
| Timeout Interval (reassociation deadline) | The Timeout Interval element is optionally present in the fourth message of the sequence if dot11RSNAActivated is not true. | 9.4.2.48 (Timeout Interval element (TIE)) |
| RIC | The RIC Data element is optionally present in the third and fourth messages.  | 9.4.2.49 (RIC Data element (RDE)) |
| RSNXE | The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP or an AP affiliated with the target AP MLD and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element, and is present in the fourth message if an RSNXE was present in the third message and the target AP or an AP affiliated with the target AP MLD set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element. | 9.4.2.241 (RSN Extension element (RSNXE)) |

The first message is used by the FTO to initiate a fast BSS transition. When RSNA is enabled, the FTO shall include the R0KH-ID and the SNonce in the FTE and the PMKR0Name in the RSNE. The target AP or the target AP MLD can use the PMKR0Name to derive the PMKR1Name, and if the target AP or target AP MLD does not have the PMK-R1 identified by PMKR1Name, it may attempt to retrieve that key from the R0KH identified by R0KH-ID. See 13.2 (Key holders). The FTO includes a fresh SNonce as its contribution to the association instance identifier and to provide key separation of the derived PTK; it is selected randomly to serve as a challenge that demonstrates the liveness of the peer in the fourth message.

The second message is used by the target AP or target AP MLD to respond to the requesting FTO. The target AP or target AP MLD provides the key holder identifiers and key names used to generate the PTK. The target AP or target AP MLD also includes a fresh ANonce as its contribution to the association instance identifier and to provide key separation of the derived PTK. The response includes a status code.

In an RSN, the third message is used by the FTO to assert to the target AP or target AP MLD that it has a valid PTK. If no resources are required, then the FTO omits inclusion of the RIC.

The fourth message is used by the target AP or target AP MLD to respond to the requesting FTO. This message serves as final confirmation of the transition, establishes that the AP or AP LD possesses the PMK-R1 and is participating in this association instance, and protects against downgrade attacks. Note, however, that the RIC is absent if no resources were requested in the third message. This also includes a status code and may include a reassociation deadline.

* FT authentication sequence: contents of first message

If present, the RSNE shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR0Name.
* All other fields shall be as specified in 9.4.2.24 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).

The MDE shall contain the MDID field and the FT Capability and Policy field settings obtained from the target AP or any AP affiliated with the target AP MLD, as advertised by the target AP or any AP affiliated with the target AP MLD in Beacon and Probe Response frames. The MDID shall be identical to that obtained during the FT initial mobility domain association exchange.

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.
* All other fields shall be set to 0.
* FT authentication sequence: contents of second message

If the status code is SUCCESS, then the following rules apply.

If present, the RSNE(s) shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall be set to the value contained in the first message of this sequence.
* All other fields shall be identical to the contents of the RSNE advertised by the AP or the AP affiliated with the AP MLD in Beacon and Probe Response frames.

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be the same as the MDE advertised by the target AP or any AP affiliated with the AP MLD in Beacon and Probe Response frames.

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 or target AP MLD, from dot11FTR1KeyHolderID.
* ANonce shall be set to a value chosen randomly by the target AP or target AP MLD, 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.
* All other fields shall be set to 0.
* FT authentication sequence: contents of third message

If present, the RSNE shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR1Name.
* All other fields shall be as specified in 9.4.2.24 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be identical to the MDE contained in the first message of this sequence.

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: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.
* When the negotiated AKM is 00-0F-AC:13, the MIC shall be calculated using the KCK and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:16, the MIC shall be calculated using the KCK2 and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:17, the MIC shall be calculated using the KCK2 and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* If dot11RSNAOperatingChannelValidationActivated is true and Authenticator indicates OCVC capability, the supplicant shall include FT OCI subelement in FTE.
* The MIC shall be calculated on the concatenation of the following data, in the order given here:
* FTO’s MAC address (6 octets)
* Target AP’s or target AP MLD’s MAC address (6 octets)
* Transaction sequence number (1 octet), which shall be set to the value 5 if this is a Reassociation Request frame and, otherwise, set to the value 3
* RSNE
* MDE
* FTE, with the MIC field of the FTE set to 0
* Contents of the RIC-Request (if present)
* RSNXE (if present)
* Non-AP STA MAC address corresponding to all the requested links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Request frame
* All other fields shall be set to 0.

If resources are being requested by the FTO, then a sequence of elements forming the RIC‑Request shall be included.

The RSNXE shall be present if an RSNXE was present in a Beacon or Probe Response frame that the FTO has received from the target AP or an AP affiliated with the target AP MLD and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

* FT authentication sequence: contents of fourth message

If the status code is SUCCESS, then the following rules apply.

If present, the RSNE(s) shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR1Name
* All other fields shall be identical to the contents of the RSNE advertised by the target AP or the AP affiliated with the target AP MLD in Beacon and Probe Response frames.

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be identical to the MDE contained in the second message of this sequence.

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 or an AP affiliated with the target AP MLD includes an RSNXE in its Beacon and Probe Response frames; otherwise this subfield shall be set to 0.
* If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC capability, the Authenticator shall include FT OCI subelement in FTE.
* When this message of the authentication sequence appears in a Reassociation Response frame, the Optional Parameter(s) field in the FTE may include the GTK, IGTK and BIGTK subelements or MLO GTK, MLO IGTK, and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK, an MLO GTK, an MLO IGTK, or an MLO BIGTK are included, the Key field of the subelement shall be wrapped using KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-10 (Integrity and key wrap algorithms) and 12.7.2 (EAPOL-Key frames). The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received message, the receiver shall ignore this trailing padding. Addition of padding does not change the value of the Key Length field. Note that the length of the encrypted Key field can be determined from the length of the GTK, IGTK, BIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.
* 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 algorithm shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:13, the MIC shall be calculated using the KCK and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:16, the MIC shall be calculated using the KCK2 and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:17, the MIC shall be calculated using the KCK2 and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* The MIC shall be calculated on the concatenation of the following data, in the order given here:
* FTO’s MAC address (6 octets)
* Target AP’s or target AP MLD’s MAC address (6 octets)
* Transaction sequence number (1 octet), which shall be set to the value 6 if this is a Reassociation Response frame or, otherwise, set to the value 4
* RSNE if Basic variant Multi-Link element is not included in the Reassocaition Response frame
* RSNEs corresponding to all accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassociation Response frameMDEFTE, with the MIC field of the FTE set to 0
* Contents of the RIC-Response (if present)
* RSNXE (if present) if Basic variant Multi-Link element is not included in the Reassocaition Response frame
* RSNXEs (if present) corresponding to all accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Response frame
* AP MAC address corresponding to all the accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Response frame
* All other fields shall be set to 0.

If this message is other than a Reassociation Response frame and dot11RSNAActivated is false, a TIE may appear. If this message is other than a Reassociation Response frame, includes a RIC-Response, and dot11RSNAActivated is false, then a timeout interval shall appear. If it appears, it shall be set as follows:

* Timeout Interval Type field shall be set to 1 (reassociation deadline).
* Timeout Interval Value field shall be set to the reassociation deadline time.

If resources were requested by the FTO, then a RIC-Response shall be included.

The RSNXE shall be present if an RSNXE was present in the third message and the target AP or an AP affiliated with the target AP MLD set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

* FT security architecture state machines
* Introduction

*TGbe editor: Change the fifth paragraph as follows (track change on):*

The interactions between the R0KH and IEEE Std 802.1X, between the R1KH and IEEE Std 802.1X, and between the S1KH and IEEE Std 802.1X occur within the SME. At both the target AP or target AP MLD and at the FTO, the R1KH and S1KH initialize the IEEE 802.1X EAPOL state machines in the respective SMEs. The Controlled Port is opened without an EAP exchange when the reassociation completes.

* S1KH state machine
* S1KH state machine variables

*TGbe editor: Change the third bullet of the first paragraph as follows (track change on):*

The following list summarizes the variables used by the S1KH state machine:

* *Init.* This variable is set to true to initialize the S1KH state machine. In addition, this variable is used to restart the state machine when transitioning to a new AP or AP MLD.