IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P802.11ai Proposed State Machine Updates | | | | |
| Date: 2016-05-14 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Michael Montemurro | BlackBerry Ltd | 4701 Tahoe Blvd  Mississauga, ON, CANADA L4W 0B4 | +1-289-261-4183 | [mmontemurro@blackberry.com](mailto:mmontemurro@blackberry.com) |
| Mark Hamilton | Ruckus Wireless | 350 W. Java Dr  Sunnyvale, CA | +1.303.818.8472 | [mark.hamilton2152@gmail.com](mailto:mark.hamilton2152@gmail.com) |
| James Lepp | BlackBerry Ltd | 1001 Farrar Road, Ottawa, Canada |  | [jlepp@blackberry.com](mailto:jlepp@blackberry.com) |
| Mark Rison | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |

Abstract

This document proposes text changes to update the P802.11ai State Machine

* 1. **STA authentication and association**

# State variables

## Change as follows:

A STA (local) for which dot11OCBActivated is false keeps an enumerated state variable for each STA  (remote) with which direct communication via the WM is needed. In this context, direct communication  refers to the transmission of any class 2 or class 3 frame with an Address 1 field that matches the MAC  address of the remote STA.

A STA for which dot11MeshActivated is true (i.e., a mesh STA) does not use procedures described in 11.3.5  (Association, reassociation, and disassociation). Instead, a mesh STA uses a mesh peering management pro-  tocol (MPM) or an authenticated mesh peering exchange (AMPE) to manage states and state variables for  each peer STA. See 14.3 (Mesh peering management (MPM)) and 14.5 (Authenticated mesh peering  exchange (AMPE)) for details.

A STA for which dot11OCBActivated is true does not use MAC sublayer authentication or association and does not keep this state variable.

For nonmesh STAs, this state variable expresses the relationship between the local STA and the remote  STA. It takes on the following values:

* *State 1*: Initial start state for non-DMG STAs and for DMG STAs that perform IEEE Std 802.11  authentication. Unauthenticated and unassociated.
* *State 2*: Initial start state for DMG STAs that do not perform IEEE Std 802.11 authentication.  Authenticated (except DMG STAs that do not perform IEEE Std 802.11 authentication, which are  unauthenticated) but unassociated.
* *State 3*: Authenticated (except DMG STAs that did not perform IEEE Std 802.11 authentication, which are unauthenticated) and associated (Pending RSNA Authentication). The IEEE Std 802.1X Controlled Port is unblocked.
* *State 4*: Authenticated (except DMG STAs that did not perform IEEE Std 802.11 authentication, which are unauthenticated) and associated (RSN Established or Not Required).The IEEE Std 802.1X Controlled Port is unblocked, or not present.
* *~~State 5~~*~~: FILS authenticated and unassociated for FILS STA only.~~

The state variable is kept within the MLME (i.e., is written and read by the MLME). The SME may also read this variable.

Mesh STAs manage the state variable as described in 14.3.2 (State variable management).

# State transition diagram for nonmesh STAs

## Change Figure 10-12 as follows with the understanding that it is not possible to show revision marks in the drawing itself, thus this represents the end result of these changes

**State 1 Non-DMG STA only**

**Unauthenticated, Unassociated**

**Class 1 frames**

**State 4**

Deauthentication (Non-DMG STA)

**RSNA Established, or Not Required**

**Class 1, 2 & 3 frames IEEE802.1X Controlled Port UnBlocked**

**State 2**

**Authenticated (Non-DMG STA only), Unassociated**

**Class 1 & 2 frames**

Successful 1.Successful (Re)Association –

802.11 Authentication (Non-DMG STA) No RSNA Required

or FILS Authentication

Deauthentication

(Non-DMG STA)

2. Fast BSS Transition

3. PBSS 4-way Handshake

Successful

1. Unsuccessful (Re)Association

(Non-PCP/Non-AP STA)

Successful

(Re)Association – RSNA Required

2. Disassociation

1. Unsuccessful (Re)Association

(Non-PCP/Non-AP STA)

4-way Handshake Successful

2. Disassociation

4. FILS (Re)Association and Key Confirmation

|  |  |  |
| --- | --- | --- |
|  | **State 3** | |
| Deauthentication |
| **Authenticated(Non-DMG STA only),**  **Associated**  **(Pending RSN Authentication)**  **Class 1, 2 & 3 frames IEEE802.1X Controlled Port Blocked** | |
| (Non-DMG STA) |
|  | |  |

#### Figure 11-13— Relationship between state and services between a given pair of nonmesh STAs

* + 1. **Frame filtering based on STA state**

## Change as follows:

The current state existing between the transmitter and receiver STAs determines the IEEE Std 802.11 frame types that may be exchanged between that pair of STAs (see Clause [9 (Frame formats)](#bookmark0)). A unique state exists for each pair of transmitter and receiver STAs. The allowed frame types are grouped into classes and the classes correspond to the STA state. In State 1, only Class 1 frames are allowed. In State 2, ~~either~~ only Class 1 ~~or~~ and Class 2 frames are allowed. In State 3 and State 4, all frames are allowed (Classes 1, 2, and 3). ~~I~~n the definition of frame classes, the following terms are used:

* + - * Within an infrastructure BSS: both the transmitting STA and the recipient STA participate in the same infrastructure BSS.
      * Within a PBSS: both the transmitting STA and the recipient STA participate in the same PBSS.
      * Within an IBSS: both the transmitting STA and the recipient STA participate in the same IBSS.
      * dot11RSNAEnabled: reference to the setting of dot11RSNAEnabled at the STA that needs to deter- mine whether a transmission or reception is permitted.

NOTE—The phrase “within a BSS” comprises “within a PBSS,” “within an IBSS,” “within a MBSS,” or “within an infrastructure BSS.”

STA A participates in the same infrastructure BSS as STA B if at least one of the following conditions is met:

* + - * STA A is associated with STA B, and either STA A or STA B is an AP.
      * STA A receives a frame with the value of its TA field equal to the MAC address of STA B and with the value of its BSSID field equal to the BSSID of the BSS with which STA A is associated.
      * STA A receives an Information Response frame from the AP with which it is associated containing an explicit indication that STA B is a member of the BSS with which STA A is associated.

STA A participates in the same PBSS as STA B if at least one of the following conditions is met:

* + - * STA A is associated with STA B, and either STA A or STA B is a PCP.
      * STA A receives a frame with the value of its TA field equal to the MAC address of STA B and with the value of its BSSID field equal to the BSSID of the PBSS that STA A has joined or started.
      * STA A receives a frame, i.e. an Information Response frame, from its PCP containing an explicit indication that STA B is a member of the PBSS that STA A has joined.

STA A participates in the same IBSS as STA B if STA A receives a frame with the value of its TA field equal to the MAC address of STA B and with the value of its BSSID field equal to the BSSID of the IBSS that STA A has joined or started.

The frame classes are defined as follows:

1. Class 1 frames
   1. Control frames i RTS
2. CTS
3. DMG Clear to send (DMG CTS) iv Ack
4. Grant
5. SSW
6. SSW-Feedback viii SSW-Ack
7. Grant Ack
8. CF-End+CF-Ack xi CF-End
9. In an IBSS and in a PBSS when dot11RSNAEnabled is false, block ack (BlockAck)
10. In an IBSS and in a PBSS when dot11RSNAEnabled is false, Block Ack Request (Block- AckReq)
    1. Management frames

i Probe Request/Response ii Beacon

1. Authentication
2. Deauthentication v ATIM
3. Public Action
4. Self-protected Action
5. Within an IBSS, all Action frames and all Action No Ack frames ix Unprotected DMG Action frames
6. In a DMG BSS, Link Measurement Request and Link Measurement Report frames
7. In a PBSS when dot11RSNAEnabled is false, all Action and Action No Ack frames except the following frames:
   1. ADDTS Request
   2. ADDTS Response
   3. DELTS
   4. Data frames
      1. Data frames between IBSS STAs
      2. Data frames between peers using DLS iii Data frames within a PBSS
   5. Extension frames

i DMG Beacon

1. Class 2 frames
   1. Management frames
      1. Association Request/Response
      2. Reassociation Request/Response i Disassociation
2. Class 3 frames
   1. Data frames

i Data frames between STAs in an infrastructure BSS or in an MBSS

* 1. Management frames

1. In an infrastructure BSS, an MBSS, or a PBSS, all Action and Action No Ack frames except those that are declared to be Class 1 or Class 2 frames
   1. Control frames i PS-Poll
2. Poll
3. SPR
4. DMG DTS
5. block ack (BlockAck), except those that are declared to be Class 1
6. Block Ack Request (BlockAckReq), except those that are declared to be Class 1 (above)

Class 2 and Class 3 frames are not allowed in an IBSS. If a STA in an IBSS receives a Class 2 or Class 3 frame, it shall ignore the frame.

A STA shall not transmit Class 2 frames unless in State 2 or State 3 or State 4.

A ~~non-FILS~~ STA shall not transmit Class 3 frames unless in State 3 or State 4.

~~A FILS STA shall not transmit Class 3 frames unless in State 4.~~

A multiband capable device that uses OCT to move from State 2 to either State 3 or State 4 shall not transmit frames before the transmitting STA becomes on-the-air enabled (see 11.33.4 (On-channel Tunneling (OCT) operation)).

# Authentication and deauthentication

* + - 1. **General**

## Change as follows:

This subclause describes the procedures used for IEEE Std 802.11 authentication and deauthentication. The states used in this description are defined in [11.3.1 (State variables)](#bookmark3).

Successful authentication sets the ~~non-FILS~~ STA’s state to State 2, if it was in State 1. Unsuccessful authen- tication leaves the STA's state unchanged.

Deauthentication notification sets the STA’s state to State 1. Deauthentication notification when in State 3 or 4 implies disassociation as well. A STA may deauthenticate a peer STA at any time, for any reason.

If STA A in an infrastructure BSS receives a Class 2 or Class 3 frame from STA B that is not authenticated with STA A (i.e., the state for STA B is State 1), STA A shall discard the frame. If the frame has an individ- ual address in the Address 1 field, the MLME of STA A shall send a Deauthentication frame to STA B.

~~Successful FILS authentication sets the STA’s state to State 5 4 if the STA’s state was State 1.~~

Authentication is optional in an IBSS. In a non-DMG infrastructure BSS, authentication is required. In a DMG infrastructure BSS and PBSS, the Open System authentication algorithm is not used (see 12.3.3.1 (Overview)). APs do not initiate authentication.

# Authentication - originating STA

## Change as follows:

Upon receipt of an MLME-AUTHENTICATE.request primitive that is part of an on-channel tunneling (see

* + 1. (On-channel Tunneling (OCT) operation)), the originating STA shall follow the rules in 11.33.4 (On-channel Tunneling (OCT) operation) in addition to the authentication procedure described below.

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA shall authenticate with the indicated STA using the following procedure:

* + - 1. If the STA is in an IBSS the SME shall delete any PTKSA,GTKSA, IGTKSA and temporal keys held for communication with the indicated STA by using the MLME-DELETEKEYS.request prim- itive (see 12.6.18 (RSNA security association termination)).
      2. The STA shall execute one of the following:
         1. For the Open System or Shared Key authentication algorithm, the authentication mechanism described in 12.3.3.2 (Open System authentication) or 12.3.3.3 (Shared Key authentication), respectively.
         2. For the fast BSS transition (FT) authentication algorithm in an ESS, the authentication mecha- nism described in 13.5 (FT Protocol), or, if resource requests are included, 13.6 (FT Resource Request Protocol).
         3. For SAE authentication in an infrastructure BSS, IBSS, or MBSS, the authentication mecha- nism described in 12.4 (Authentication using a password).
         4. For FILS authentication in an ESS, the authentication mechanism described in [12.11 (Authen-](#bookmark1) [tication for FILS)](#bookmark1).
      3. If the authentication was successful within the AuthenticateFailureTimeout, the state for the indi- cated STA shall be set to State 2 if it was State 1; the state shall remain unchanged if it was other than State 1.
      4. The MLME shall issue an MLME-AUTHENTICATE.confirm primitive to inform the SME of the result of the authentication.

# Authentication - destination STA

## Change as follows:

Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA shall authenticate with the originating STA using the following procedure:

* + - * 1. If Open System or Shared Key authentication algorithm is being used, the STA shall execute the procedure described in 12.3.3.2 (Open System authentication) or 12.3.3.3 (Shared Key authentica- tion), respectively. These result in the generation of an MLME-AUTHENTICATE.indication primi- tive to inform the SME of the authentication request.
        2. If FT authentication is being used, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, including the FT Authentication Ele- ments, and the SME shall execute the procedure as described in 13.5 (FT Protocol) or 13.6 (FT Resource Request Protocol).
        3. If SAE authentication is being used in an infrastructure BSS, IBSS, or MBSS, the MLME shall issue an MLMEAUTHENTICATE. indication primitive to inform the SME of the authentication request, including the SAE Authentication Elements, and the SME shall execute the procedure as described in 12.4 (Authentication using a password).
        4. If FILS authentication is being used in an ESS, the MLME shall issue an MLME-AUTHENTI- CATE.indication primitive to inform the SME of the authentication request, and the SME shall exe- cute the procedure described in 1 12.11 (Authentication for FILS).
        5. If the STA is in an IBSS and management frame protection was not negotiated when the PTKSA(s) were created, the SME shall delete any PTKSA,GTKSA, IGTKSA and temporal keys held for com- munication with the originating STA by using the MLME-DELETEKEYS.request primitive (see

12.6.18 (RSNA security association termination)).

* + - * 1. Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is not SUC- CESS, the MLME shall transmit an Authentication frame with the corresponding status code, as defined in [9.4.1.9 (Status Code field),](#bookmark4) and the state for the originating STA shall be left unchanged. The Authentication frame is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5 (FT Protocol) or 13.6 (FT Resource Request Protocol). If dot11FILSFDFrameBeaconMaximumInteval is not equal to 0, and if a Beacon frame or FD frame has not been transmitted by an AP for a period that is equal to dot11FILSFD- FrameBeaconMaximumInterval, that AP shall queue for transmission a FD frame or a Beacon frame unless the next TBTT is within a duration indicated by the value of dot11FILSFDFrameBeaconMin- imumInterval.
        2. Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is SUCCESS, the MLME shall transmit an Authentication frame that is constructed using the appropriate proce- dure in 12.3.3.2 (Open System authentication), 12.3.3.3 (Shared Key authentication), 13.5(FT Proto- col) or 13.6 (FT Resource Request Protocol), with a status code of Successful, and the state for the originating STA shall be set to State 2 if it was in State 1.

If the STA is in an IBSS, if the SME decides to initiate an RSNA, and if the SME does not know the security policy of the peer, it may issue an individually addressed Probe Request frame to the peer by invoking an MLME-SCAN.request primitive to discover the peer’s security policy.

An AP may provide neighbor report information to a STA that requests authentication or association by responding with an Authentication or (Re)Association Response frame that includes the Reason Code field set to REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION and that includes one or more Neighbor Report elements.

An AP may provide estimated association response latency to the non-AP STA as AssociationDelayInfo parameter ( 9.4.2.175 (Association Delay Info element)). The AssociationDelayInfo parameter shall be larger than dot11HLPWaitTime. The AssociationDelayInfo is provided in the Association Delay Info ele- ment ( 9.4.2.175 (Association Delay Info element)). When a non-AP STA receives the Authentication frame including Association Delay Info element, the non-AP STA sets the dot11AssociationResponseTimeOut equal to or larger than the content of the element.

# Association, reassociation, and disassociation

* + - 1. **General**

## Change as follows:

Subclause [11.3.5 (Association, reassociation, and disassociation)](#bookmark7) describes the procedures used for IEEE Std 802.11 association, reassociation and disassociation.

The states used in this description are defined in [11.3.1 (State variables).](#bookmark3)

Successful association enables a STA to exchange Class 3 frames. Successful association sets the non-FILS STA’s state to State 3 or State 4. Successful association sets the state for ~~and for~~ FILS STAs to State 4.

Successful reassociation enables a STA to exchange Class 3 frames. Unsuccessful reassociation when not in State 1 leaves the STA’s state unchanged (with respect to the AP or PCP that was sent the Reassociation Request (which may be the current STA)). Successful reassociation sets the non-FILS STA’s state to State 3 or State 4 (with respect to the AP or PCP that was sent the Reassociation Request frame). Successful reassociation when not in State 1 sets the STA’s state to State 2 (with respect to the current AP or PCP, if this is not the AP or PCP that was sent the Reassociation Request frame). Successful reassociation sets a FILS STA’s state to State 4 and enables it to exchange Class 3 frames. Reassociation shall be performed only if the originating STA is already associated in the same ESS.

Disassociation notification when not in State 1 sets ~~the~~ a non-FILS STA’s state to State 2. Disassociation notification when not in State 1 sets a FILS STA’s state to State 1. The STA shall become associated again prior to sending Class 3 frames. A STA may disassociate a peer STA at any time, for any reason.

If non-DMG STA A in an infrastructure BSS receives a Class 3 frame from STA B that is authenticated but not associated with STA A (i.e., the state for STA B is State 2), STA A shall discard the frame. If the frame has an individual address in the Address 1 field, the MLME of STA A shall send a Disassociation frame to STA B.

If DMG STA A in an infrastructure BSS receives a Class 3 frame from STA B that is not associated with STA A (i.e., the state for STA B is State 2), STA A shall discard the frame. If the frame has an individual address in the Address 1 field, the MLME of STA A shall send a Disassociation frame to STA B.

If an MM-SME coordinated STA receives an Association Response frame with a result code equal to SUC- CESS and with the Single AID field within MMS element equal to 1, then

* For each of its MAC entities advertised within the MMS element and for which dot11RSNAEnabled is true, the state is set to State 3. Progress from State 3 to State 4 occurs independently in each such MAC entity.
* For each of its MAC entities advertised within the MMS element and for which dot11RSNAEnabled is false, the state is set to State 4.

If the MM-SME coordinated STA in State 3 is assigned an AID for only the MAC entity identified by the RA field of the Association Response frame with result code equal to SUCCESS, the MM-SME may repeat the association procedure for any other MAC entity coordinated by the MM-SME.

Association is not applicable in an IBSS. In an infrastructure BSS, association is required. In a PBSS, asso- ciation is optional. APs do not initiate association.

# Non-AP and non-PCP STA association initiation procedures

## Change as follows:

g) If an MLME-ASSOCIATE.confirm primitive is received with a ResultCode of SUCCESS, and RSNA is required, and FILS authentication was not used, then the SME shall perform a 4-way handshake to establish an RSNA. As a part of a successful 4-way handshake, the SME shall enable protection by generating an MLME-SETPROTECTION.request(Rx\_Tx) primitive. If an MLME- ASSOCIATE.confirm primitive is received with a ResultCode of SUCCESS, and FILS authentication was used, then the SME shall enable protection by generating an MLME- SETPROTECTION.request(Rx\_Tx) primitive.

# AP or PCP association receipt procedures

## Change as follows:

n) If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS and RSNA establishment is required, and FILS authentication was not used, the SME shall attempt a 4-way handshake. Upon a successful completion of ~~a~~the 4-way handshake, the SME shall enable protection by issuing an MLME-SETPROTECTION.request(Rx\_Tx) primitive. ~~and the state for the STA shall~~ ~~be set to State 4..~~ If FILS authentication was used, the SME shall enable protection by generating an MLME-SETPROTECTION.request(Rx\_Tx) primitive. In either case, upon receipt of the MLME- SETPROTECTION.request(Rx\_Tx), the MLME shall set the state for the STA to State 4.

# Non-AP and non-PCP STA reassociation initiation procedures

## Change as follows:

g) If an MLME-REASSOCIATE.confirm primitive is received with a ResultCode of SUCCESS, and RSNA is required, and FILS authentication was not used, and the STA is in State 3, then the SME shall perform a 4-way handshake to establish an RSNA. As a part of a successful 4-way handshake, the SME shall enable protection by generating an MLME-SETPROTECTION.request(Rx\_Tx) primitive. If an MLME-REASSOCIATE.confirm primitive is received with a ResultCode of SUC- CESS, and FILS authentication was used, and the STA is in State 3, then the SME shall enable pro- tection by generating an MLME-SETPROTECTION.request(Rx\_Tx) primitive.

# AP or PCP reassociation receipt procedures

## Change as follows:

r) If the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS, RSNA estab- lishment is required, the reassociation is not part of the BSS transition, and FT and FILS are ~~is~~not in use, the SME shall attempt a 4-way handshake. Upon a successful completion of ~~a~~the 4-way hand- shake, the SME shall enable protection by issuing an MLME-SETPROTECTION.request(Rx\_Tx) primitive ~~and the state for the STA shall be set to State 4~~. If FILS authentication was used, the SME shall enable protection by generating an MLME-SETPROTECTION.request(Rx\_Tx) primitive. In either case, upon receipt of the MLME-SETPROTECTION.request(Rx\_Tx), the MLME shall set the state for the STA to State 4.