IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Authentication State Machine for FILS | | | | |
| Date: 2013-06-05 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rob Sun | Huawei Technology | Suite 400, 303 Terry Fox drive,  Kanata, On | +1 613 2781948 | Rob.sun@huawei.com |
| Lei Wang | InterDigital Communications | 781 Third Ave., King of Prussia, PA 19406 | 1 858 205 7286 | leiw@billeigean.com |

Abstract

This document presents suggested proposal towards CID 1238 and CID 1010 for TGai. The proposal also included updated state machine (CID 1239 which was concluded during May, 2013 meeting) as per the most recent update from P802.11REVmb\_D1.4

***Modify the following definition into 10.3.1 as highlighted in red texts:***

* STA authentication and association
* State variables

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 (11ai) for which dot11OCBActivated is false and dot11FILSActivated is true uses the state transition as described in section 10.3.2, in which the STA keeps the neumerated state variable.

A STA for which dot11MeshActivated is true (i.e., a mesh STA) does not use procedures described in 10.3.5 (Association, reassociation, and disassociation). Instead, a mesh STA uses a mesh peering management protocol (MPM) or a authenticated mesh peering exchange (AMPE) to manage states and state variables for each peer STA. See 13.3 (Mesh peering management (MPM)) and 13.5 (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.(11ad) Unauthenticated, unassociated. State 1 is not used by DMG STAs.(11ad)
* *State 2:* Initial start state for DMG STAs.(11ad) Authenticated (non-DMG STAs only)(11ad), not associated.
* *State 3:* Authenticated (non-DMG STAs only)(11ad) and associated (Pending RSN Authentication).
* *State 4:* For Infrastructure BSS and PBSS only, RSNA Established or Not Required.(11ad)
* *State 5:* FILS authenticated and un-associated. State 5 is designed for FILS authentication and association protocol (11ai)

State 1 is not used by DMG STAs, and the state machine starts in State 2.(11ad)

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 13.3.2 (State variable management).

* State transition diagram for nonmesh STAs

Figure 10-12 (Relationship between state and services between a given pair of non-mesh STAs(#80)) shows the state transition diagram for nonmesh STA states. Note that only events causing state changes are shown. The state of the sending STA given by Figure 10-12 (Relationship between state and services between a given pair of non-mesh STAs(#80)) is with respect to the intended receiving STA.

* Modify the figure as per figure 10-12

Figure 10-12- Relationship between State and Services between a given pair of non-mesh STAs

* Frame filtering based on STA state

The current state existing between the transmitter and receiver STAs determines the IEEE Std(#130) 802.11 frame types that may be exchanged between that pair of STAs (see Clause 8 (Frame formats)). 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 Class 1 or Class 2 frames are allowed. In State 3 and State 4, all frames are allowed (Classes 1, 2, and 3). In the definition of frame classes, the following terms are used:(11ad)

* *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 determine 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.” (11ad)

STA A participates in the same infrastructure BSS as STA B if at least one of the following conditions is met:(11ad)

* 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:(11ad)

* 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.,(#1559) 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.(11ad)

The frame classes are defined as follows:

* Class 1 frames
* Control frames
* RTS
* CTS
* DMG Clear to send (DMG CTS)(11ad)(Ed)
* (#1198)Ack
* Grant(11ad)
* SSW(11ad)
* SSW-Feedback(11ad)
* SSW-(#1198)Ack(11ad)
* Grant (#1198)Ack(11ad)
* CF-End+CF-Ack(Ed)
* CF-End
* Within an IBSS and within a PBSS when dot11RSNAEnabled is false(11ad), Block Ack (BlockAck)
* Within an IBSS and within a PBSS when dot11RSNAEnabled is false(11ad), Block Ack Request (BlockAckReq)
* Management frames
* Probe Request/Response
* Beacon
* FILS Discovery Frame
* Authentication Deauthentication
* ATIM
* Public Action
* Self-protected Action
* Within an IBSS, all Action frames and all Action No Ack frames
* Unprotected DMG Action frames(11ad)
* DMG: Link Measurement Request and Link Measurement Report frames(11ad)
* Within a PBSS when dot11RSNAEnabled is false, all Action and Action No Ack frames except the following frames:(11ad)
* ADDTS Request
* ADDTS Response
* DELTS(Ed)
* Data frames
* Data frames between STAs in an IBSS
* Data frames between peers using DLS
* Data frames within a PBSS(11ad)
* Extension frames(11ad)
* DMG Beacon(11ad)
* Class 2 frames
* Management frames
* Association Request/Response Reassociation Request/Response
* Disassociation
* Class 3 frames
* Data frames
* Data frames between STAs in an infrastructure BSS or in an MBSS
* Management frames
* Within an infrastructure BSS, an MBSS, or a PBSS(11ad), all Action and Action No Ack frames except those that are declared to be Class 1 or Class 2 frames(Ed)
* Control frames
* PS-Poll
* Poll(11ad)
* SPR(11ad)
* DMG DTS(11ad)
* Block Ack (BlockAck), except those that are declared to be Class 1(11ad)(Ed)
* Block Ack Request (BlockAckReq), except those that are declared to be Class 1 (above)(11ad)

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.(11ad)

A STA shall not transmit Class 3 frames unless in State 3 or State 4.(11ad)

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

A multi-band 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 10.33.4 (On-channel Tunneling (OCT) operation

(11ad))). (11ad)

The use of the word “receive” in 10.3 (STA authentication and association) refers to a frame that meets all of the filtering criteria specified in Clause 11 (Security) and Clause 9 (MAC sublayer functional description).

* Authentication and deauthentication
* General

This subclause describes the procedures used for IEEE Std(#130) 802.11 authentication and deauthentication. The states used in this description are defined in 10.3.1 (State variables).

Successful authentication sets the STA’(#1485)s state to State 2, if it was in State 1. Unsuccessful authentication leaves the STA’(#1485)s state unchanged.(11ad)

Deauthentication notification sets the STA’(#1485)s state to State 1. (11ad)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 individual address in the Address 1 field, the MLME of STA A shall send a Deauthentication frame to STA B.

Sucessful FILS authentication in 11ai FILS STA will be transitioned to state 5 if it’s started in State 1. Unsuccessful FILS 11ai authentication will leave the STA’s state unchanged.

Deauthentication notification in 11ai sets the STA’s state to state 1 from state 5 for any reasons.

Authentication is optional in a non-DMG(11ad) IBSS. In a non-DMG(11ad) infrastructure BSS, authentication is required. APs do not initiate authentication. Authentication and deauthentication are not supported by DMG STAs.(11ad)

* FAssociation, reassociation, and disassociation
* General

Subclause 10.3.5 (Association, reassociation, and disassociation) describes the procedures used for IEEE Std(#130) 802.11 association, reassociation and disassociation.

The states used in this description are defined in 10.3.1 (State variables).

Successful association enables a STA to exchange Class 3 frames. Successful association sets the STA’(#1485)s state to State 3 or State 4.

Successful FILS association (11ai) enables a STA to sets the STA’s sate from State 5 to 4, and exchange the Class 3 frames defined in section 10.3.1

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 PCP/AP(11ad) that was sent the Reassociation Request (which may be the current STA)). Successful reassociation sets the STA’s state to State 3 or State 4 (with respect to the PCP/AP(11ad) that was sent the Reassociation Request). Successful reassociation when not in State 1 sets the STA’s state to State 2 (with respect to the current PCP/AP(11ad) , if this is not the PCP/AP(11ad) that was sent the Reassociation Request). Successful reassociation (with respect to 11ai) sets the STA’s state to State 4 to enable a STA 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 STA’s state to State 2. 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(11ad) 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.(11ad)

If an MM-SME coordinated STA receives an Association Response frame with a result code equal to SUCCESS and with the value of the Single AID field within MMS element equal to 1, then (11ad)

* 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 with result code equal to SUCCESS, the MM-SME may repeat the association procedure for any other MAC entity coordinated by the MM-SME. (11ad)

Association is not applicable in an IBSS. In an infrastructure BSS, association is required. In a PBSS, association is optional.(11ad) APs do not initiate association.