IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution to Comments : CID 2048,2956,3342,2051,2220,2368,3083,2939,2515,2054 | | | | |
| Date: 2013-09-30 | | | | |
| 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 |
|  |  |  |  |  |

Abstract

This document presents suggested proposal towards CID 2048,2956,3342,2051,2220,2368,3083,2939,2515,2054

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

* STA authentication and association

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number(C)** | **Page(C)** | **Line(C)** | **Comments** | **Proposed Change** |
| **2048** | **10.3.1** | **78** | **54** | **"A FILS STA for which dot11OCBActivated is false" -- this is in a "change" instruction. It is clearly new text, but it is not marked as such.** | **Add any missing markup to this subclause.** |
| **2956** | **10.3.1** | **78** | **54** | **Some of the changes here are not properly marked as changes from the baseline.** | **Fix the editing marks and instructions to the baseline editor so that the changes from the baseline can be identified.** |
| **3342** | **10.3.1** | **78** | **54** | **Some of the changes here are not properly marked as changes from the baseline.** | **Fix the editing marks and instructions to the baseline editor so that the changes from the baseline can be identified.** |
| **2051** |  | **82** | **65** | **"A STA shall not transmit Class 2 frames unless in State 2 or State 3 or State 4." - what about state 5?** | **Add "State 5" to the list** |
| **2220** | **10.3.3** | **82** | **65** | **A STA in state 5 can also transmit class 2 frames.** | **Change line 65 to "A STA shall not transmit Class 2 frames unless in State 2 or State 3 or State 4 or State 5."** |
| **2368** | **10.3.3** | **83** |  | **Informative notes that talk about uses of terms do not belong in an IEEE standard.** | **Delete lines 9 and 10: "The use of the word ... and Clause 9."** |
| **3083** |  | **83** |  | **10.3.4.2  Editorial  missing space in 'authenticationprocedure'** |  |
| **2939** | **10.3.3.** | **83** | **3** | **Conditional text on CIDs not conditional / still showing in draft** | **Make reference to CIDs conditional text** |
| **2515** | **64** | **83** | **10** | **Typo** | **Need space between authentication procedure** |
| **2054** | **10.3.4.1** | **83** | **42** | **"After successful FILS authentication a FILS STA will transition to State 5 from State 1." -- the "will" here is spurious (i.e. it's not a future action from the viewpoint of the protocol) . Also this statement says nothing about what happens if the STA was not in State 1.** | **"Sucessful FILS authentication sets the STA's state to State 5."** |

***Discussion:***

Clause 10.3 outlines the FILS authentication and association state variables and transition conditions, and also defines the filtering rules regarding the Class 1, 2 and 3 under different states.

After reviewing the CIDs, lots of which are related to editorial, and some CIDs can be addressed with clarifications and definitions.

***Proposed Resolution:***

**Revised**

### TGai Editor: Please apply the following changes to the subclauses of 10.3.1,

Notes to editor: the striked lines are removed, the highlight texts are the modifications.

**10.3.1 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 FILS STA 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 an enumerated state variable.( Notes: CID 2048，2956))

A STA for which dot11MeshActivated is true (i.e., a mesh STA) does not use procedures described in

10.3.5. 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 and 13.5 for

details.

A STA for which dot11OCBActivated is true does not use MAC sublayer authentication or association and

does not keep this state variable.

A STA for which dot11OCBActivated is true but intended to use FILS authentication will transition to State

5: FILS authenticated

For non-mesh 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. Unauthenticated, unassociated. State 1 is not used by

DMG STAs.

— State 2: Initial start state for DMG STAs. Authenticated (non-DMG STAs only), not associated.

— State 3: Authenticated (non-DMG STAs only) and associated (Pending RSN Authentication).

— State 4: For Infrastructure BSS and PBSS only, RSNA Established or Not Required. (Authenticated

and associated.)

— State 5: FILS authenticated and unassociated. State 5 is designed for the FILS authentication and

FILS association protocol

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

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.

**10.3.3 Frame filtering based on STA state**

The current state existing between the transmitter and receiver STAs determines the IEEE 802.11 frame

types that may be exchanged between that pair of STAs (see Clause 8). 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 State 5, only frame classes 1

and 2 are allowed.

In 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 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.”~~

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:

a) Class 1 frames

1) Control frames

i RTS

ii DMG Clear to send (DMG CTS)

iii CTS

iv Ack

v Grant

vi SSW

vii SSW-Feedback

viii SSW-Ack

ix Grant Ack

x CF-End+CF-Ack

xi CF-End

xii Within an IBSS and within a PBSS when dot11RSNAEnabled is false, Block Ack (Block-

Ack)

xiii Within an IBSS and within a PBSS when dot11RSNAEnabled is false, Block Ack Request

(BlockAckReq)

2) Management frames

i Probe Request/Response

ii Beacon

iii FILS Discovery Frame

iv Authentication

v Deauthentication

vi ATIM

vii Public Action

viii Self-protected Action

ix Within an IBSS, all Action frames and all Action No Ack frames

x Unprotected DMG Action frames

xi DMG: Link Measurement Request and Link Measurement Report frames

xii Within 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(Ed)

4) Data frames

i Data frames between STAs in an IBSS

ii Data frames between peers using DLS

iii Data frames within a PBSS

5) Extension frames

i DMG Beacon

b) Class 2 frames

1) Management frames

i Association Request/Response

ii Reassociation Request/Response

i Disassociation

c) Class 3 frames

1) Data frames

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

2) Management frames

i Within 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 (above)

3) Control frames

i PS-Poll

ii Poll

iii SPR

iv DMG DTS

v Block Ack (BlockAck), except those that are declared to be Class 1 (above)

vi 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 STA shall not transmit Class 3 frames unless in State 3 or State 4 or State 5[note：CID2220]

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 10.32.4).

The use of the word “receive” in 10.3 refers to a frame that meets all of the filtering criteria specified in

Clause 11 and Clause 9.

**10.3.4 Authentication and deauthentication**

***Change as follows:***

**10.3.4.1 General**

This subclause describes the procedures used for IEEE Std 802.11 authentication and deauthentication. The

states used in this description are defined in 10.3.1.

Successful authentication sets the STA's state to State 2, if it was in State 1. Unsuccessful authentication

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 non-DMG 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.

~~After S~~uccessful FILS authentication ~~will transition to~~ sets the STA to State 5 from State 1. Unsuccessful FILS

authentication ~~will~~ leave a FILS STA's state unchanged.

Deauthentication notification sets a FILS STA's state to State 1.[note：CID2054]

Authentication is optional in a non-DMG 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.

***Change as follows:***

**10.3.4.2 Authentication - originating STA**

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

10.32.4), the originating STA shall follow the rules in 10.32.4 in addition to the authentication procedure [note：CID3083，2515]

described below.

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA shall authenticate

with the indicated STA using the following procedure: previously

a) If the STA is in an IBSS the SME shall delete any PTKSA and temporal keys held for communication

with the indicated STA by using the MLME-DELETEKEYS.request primitive (see 11.5.12

(RSNA security association termination)).

b) The STA shall execute one of the following:

1) For the Open System or Shared Key authentication algorithm, the authentication mechanism

described in 11.2.3.2 (Open System authentication) or 11.2.3.3 (Shared Key authentication),

respectively.

2) For the FT authentication algorithm in an ESS, the authentication mechanism described in 12.5

(FT Protocol), or, if resource requests are included, 12.6 (FT Resource Request Protocol).

3) For SAE authentication in an ESS, IBSS, or MBSS, the authentication mechanism described in

11.3 (Authentication using a password).

4) For FILS authentication in an ESS, the authentication mechanism described in 11.11 (Authentication

for Fast Initial Link setup).

c) If the authentication was successful within the AuthenticateFailureTimeout, the state for the indicated

STA shall be set to State 2 if it was State 1; the state shall remain unchanged if it was other

than State 1

d) The MLME shall issue an MLME-AUTHENTICATE.confirm primitive to inform the SME of the

result of the authentication.

**10.3.5 Association, reassociation, and disassociation**

*Change as follows:*

**10.3.5.1 General**

Subclause 10.3.5 describes the procedures used for IEEE Std 802.11 association, reassociation and disassociation.

The states used in this description are defined in 10.3.1.

Successful association enables a STA to exchange Class 3 frames. Successful association sets the STA's

state to State 3 or State 4.

Successful FILS association enables a STA to exchange Class 3 frames. Successful association sets the FILS

STA's state 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 PCP/AP 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 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, if this is not the PCP/AP that was

sent the Reassociation Request). 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 STA's state to State 2. Disassociation notification

when not in State 1 sets a FILS STA's state to State 5. 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 SUCCESS

and with the value of 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 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, association

is optional. APs do not initiate association.

***Change subclause 10.3.4.3 as follows:***

**10.3.4.3 Authentication - destination STA**

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:

a) If Open System or Shared Key authentication algorithm is being used, the STA shall execute the

procedure described in 11.2.3.2 or 11.2.3.3, respectively. These result in the generation of an

MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request.

b) 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 Elements,

and the SME shall execute the procedure as described in 12.5 or 12.6.

c) If SAE authentication is being used in an ESS, 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 11.3

d) If FILS authentication is being used in an ESS, the MLME shall issue an MLME-AUTHENTICATE.

indication primitive to inform the SME of the authentication request, including the FILS

authentication elements, and the SME shall execute the procedure described in 11.11 (Authentication

for Fast Initial Link setup)

e) 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 and temporal keys held for communication with the

originating STA by using the MLME-DELETEKEYS.request primitive (see 11.5.15).

e)f) Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is not SUCCESS,

the MLME shall transmit an Authentication frame with the corresponding status code, as

defined in 8.4.1.9, and the state for the originating STA shall be left unchanged. The Authentication

frame is constructed using the appropriate procedure in 11.2.3.2, 11.2.3.3, 11.11.2.2, 12.5 or12.6.

f)g) 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 procedure

in 11.2.3.2, 11.2.3.3, 11.11.2.2, 12.5 or 12.6, 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.