IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed 802.11ai specification text for FILS authentication state machine | | | | |
| Date: 2012-11-05 | | | | |
| 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 |
|  |  |  |  |  |

Abstract

This submission proposes the 802.11ai specification text for the FILS authentication State machine as a part of Security Framework , based on the accepted features and functionalities in the 802.11ai Specification Framework Document (SFD), i.e., Section 4.1 and 4.3, in 12/0151r13[Ref-1], and also based on the relevant discussions in previous TGai meetings [Ref-9][Ref-10] .

The numbering of the clauses is taken from 2012 revision of IEEE802.11 standard [Ref-2].

# Introduction

To facilitate a fast initial link setup, high-level descriptions about FILS authentication and state machine related features/functionalities have been accepted in 802.11ai Specification Framework Document (SFD), 12/0151r13 .

The 802.11Task Group (TGai) has issued a new call for contributions for Specification Tex for the TGai detailed Draft Text, 12/0992r1 [Ref-6].

As a response to the TGai Call-for-Contributions, this document proposes further detailed text for TGai Specification Document, to provide additional descriptions / specifications for the FILS authentication state machine related features / functionalities.

# Proposed 802.11ai Specification Text

## Modify the following definition into 10.3.1 as indicated:

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

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, unauthenticated, unassociated.

— *State 2:* Authenticated, not associated.

— *State 3:* Authenticated and associated (Pending RSN Authentication).

— *State 4:* Authenticated and associated.

--- *State 5: FILS authenticated*

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.

## *Modify section 10.3.2 as indicated*

Figure 10-6 shows the state transition diagram for non-mesh STA states. Note that only events causing state

changes are shown. The state of the sending STA given by Figure 10-6 is with respect to the intended

receiving STA

**Figure 10-6—Relationship between state and services**

## *Modify section 10.3.3 as indicated*

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 class 1, 2 and selected Class 3 frames including some management and data frames are all allowed. The frame classes are defined follows:

a) Class 1 frames

1) Control frames

i) RTS

ii) CTS

iii) ACK

iv) CF-End+ACK

v) CF-End

vi) Within an IBSS, Block Ack (BlockAck)

vii) Within an IBSS, Block Ack Request (BlockAckReq)

2) Management frames

i) Probe Request/Response

ii) Beacon

iii) Authentication

iv) Deauthentication

v) ATIM

vi) Public Action

vii) Self-protected Action

viii) Within an IBSS, all Action frames and all Action No Ack frames

3) Data frames

i) Data frames between STAs in an IBSS

ii) Data frames between peers using DLS

b) Class 2 frames

1) Management frames

i) Association Request/Response

ii) Reassociation Request/Response

iii) 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 or an MBSS, 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) Within an infrastructure BSS or an MBSS, Block Ack (BlockAck)

iii) Within an infrastructure BSS or an MBSS, Block Ack Request (BlockAckReq)

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.

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.

# Straw-Polls and Motions

**Motion:** Include the text proposed in section 2 and its subsections this contribution (12/1282), into the TGai Draft Specification Document (D0.1).

Yes: \_\_\_\_\_\_\_\_\_\_\_\_; No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; Abstain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Move:

Second: