IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Authentication Protocol for 11ai | | | | |
| Date: 2011-12-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rob Sun  Li Yunbo  Edward Au  Phil Barber | Huawei Technology | Suite 400, 303 Terry Fox drive,  Kanata, On | +1 613 2781948 | Rob.sun@huawei.com |
|  | ZTE |  |  |  |

Abstract

This document presents suggested text to the FILS authentication protocol for TGai

***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.

***Modify section 10.3.4.1 as indicated***

**10.3.4.1 General**

This subclause describes the procedures used for IEEE 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. The STA shall not transmit Class 2 frames unless in State 2 or State 3 or

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

If both the STAs agree to parameters of FILS authentication through the Authentication Algorithm Number filed carried in either the Beacon or Probe Request/Response, the STA will switch to the State 5 upon successful authentication. The unsuccessful authentication will leave the STA’s state unchanged. In State 5, the STA shall only transmit Class 1 , 2 and some selected Class 3 frames with some management and data frames to complete the FILS authentication.

Deauthentication notification sets the STA's state to State 1. The STA shall become authenticated again

prior to sending Class 2 frames. 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.

Deauthentication notification set the STA’s state which is now State 5 in the FILS authentication to State 1. The STA may retry FILS authentication or become authenticated to State 2 through open authentication.

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.

Authentication is optional in an IBSS. In an infrastructure BSS, authentication is required. APs do not initiate authentication.

***Modify section 4.5.4.2 as indicated***

* Authentication

IEEE 802.11 authentication operates at the link level between IEEE 802.11 STAs. IEEE Std 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication.

IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is an SS. This service may be used by all STAs to establish their identity to STAs with which they communicate, in both ESS and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, an association is not(#1421) established.

IEEE Std 802.11 defines five802.11(#12858) authentication methods: Open System authentication, Shared Key authentication, FT authentication(11r), simultaneous authentication of equals (SAE), and FILS authentication.(11s) Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. FT authentication relies on keys derived during the initial mobility domain association to authenticate the (#1112)stations as defined in Clause 12 (Fast BSS transition).(11r) SAE authentication uses finite field cryptography to prove knowledge of a shared password.(11s) FILS authentication enables the fast authentication mechanisms without compromising the RSNA security architecture. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA might support SAE authentication and FILS authentication.(11s) An RSNA also supports authentication based on IEEE Std 802.1X-2004, or preshared keys (PSKs) after Open System authentication(11s). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This standard does not specify an EAP method that is mandatory to implement. See 11.5.5 (RSNA policy selection in an IBSS and for DLS) for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port. In a FILS authentication, in order to enable the parallel processing of the authentication and authorization, some selected data frames will be allowed to transmitted over the IEEE 802.1X uncontrolled port before the authentication is complete.

***Create section 4.10.3.2a***

**4.10.3.4a AKM operations with AS at FILS authentication**

The following AKM operations are carried out when authentication is accomplished using the FILS authentication.

* A STA discovers the AP’s security policy through passively monitoring the Beacon frames or through active probling. After discovery the STA performs FILS authentication using 802.11 Authentication frames with the AP.
* STA should start the authentication with EAPOL-start message containing the FILS authentication parameters to AP.
* AP should receive the EAPOL data frame via the 802.1X uncontrolled port and reconstruct the EAP frame and send it over to Authentication Server for authentication
* Upon successful EAP authentication handshake, whereby the specific EAP authentication is out of the scope, the Authenticator should store the PMK and also generate ANounce and derive PTK for later optimized key agreement, also, the AP will send the 802.1X EAPOL success message along with the keying materials and MIC for message integrity protection to STA. and AP also transmits the encrypted GTK and IGTK with key wrapping function to STA.
* At STA, upon receiving the EAPOL success message from AP, the STA should derive the PMK and the PTK with SNounce based on the KDF function specified in section 11.6. STA also verifies the received MIC.
* STA should send the association request with piggybacked EAPOL-key message containing SNounce and MIC for message integrity protection).
* Upon receiving the 802,11 association request message along with EAPOL key message, the AP shall verify that the SNonce in this message matches the value provided by the STA in the above 802.1X EAPOL success message. AP also verifies the received MIC.
* AP will unlock the 802.1x controlled port for other class 3 data frames to traverse through
* The detailed message flow is depicted as figure xx: FILS authentication protocol

Figure xx: AKM operation with AS at FILS authentication

***Modify section 8.4.1.1 as indicated:***

* Authentication Algorithm Number field

The Authentication Algorithm Number field indicates a single authentication algorithm. The length of the Authentication Algorithm Number field is 2 octets. The Authentication Algorithm Number field is illustrated in Figure 8-35 (Authentication Algorithm Number field). The following values are defined for authentication algorithm number:

Authentication algorithm number = 0: Open System

Authentication algorithm number = 1: Shared Key

Authentication algorithm number = 2: Fast BSS Transition(11r)

Authentication algorithm number = 3: simultaneous authentication of equals (SAE)

Authentication algorithm number = 4: FILS authentication (11s)

Authentication algorithm number = 65 535: Vendor specific use

NOTE—The use of this value implies that a Vendor Specific element(Ed) is included with more information.(#10081)

All other values of authentication algorithm number are reserved.