IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Motherhood and Apple Pie | | | | |
| Date: 2011-11-4 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at aruba networks (one word) dot com |
|  |  |  |  |  |

Abstract

This document suggests some general text that should be non-controversial.

***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 allows two STAs to authenticate each other with the help of a trusted third party. 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.

Either SAE authentication, FILS authentication or(11s) the Open System 802.11 authentication algorithm is used in RSNs based on infrastructure BSS and IBSS, although Open System 802.11 authentication is optional in an RSN based on an IBSS. SAE authentication is used in an MBSS.(11s) RSNA disallows the use of Shared Key 802.11 authentication.(#12858)

***Modify section 4.5.4.3 as indicated:***(11s)

* Deauthentication

The deauthentication service is invoked when an existing Open System, Shared Key, SAE(11s) or FILS authentication is to be terminated. Deauthentication is an SS.

When the deauthentication service is terminating SAE authentication any PTKSA, GTKSA, mesh TKSA, or mesh GTKSA related to this SAE authentication is destroyed. If PMK caching is not enabled, deauthentication also destroys any PMKSA created as a result of this successful SAE authentication.(11s)

In an ESS, because authentication is a prerequisite for association, the act of deauthentication causes(#1421) the STA to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. The association at the transmitting STA is terminated when the STA sends a deauthentication notice to an associated STA. Deauthentication, and if associated, disassociation can not be refused by the receiving STA except when management frame protection(#12241) is negotiated and the message integrity check fails.(11w)

In an RSN ESS, Open System 802.11(#12858) authentication is required. In an RSN ESS, deauthentication results in termination of any association for the deauthenticated STA. It also results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the pairwise transient key security association (PTKSA). The deauthentication notification is provided to IEEE Std 802.1X-2004 via the MAC layer.

In an RSNA, deauthentication also destroys any related pairwise transient key security association(PTKSA)(11w), group temporal key security association (GTKSA), station-to-station link (STSL) master key security association (SMKSA), STSL transient key security association (STKSA), and integrity group temporal key security association (IGTKSA)(11w) that exist in the STA and, if applicable, closes the associated IEEE 802.1X Controlled Port. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

In an RSN IBSS, Open System authentication is optional, but a STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

***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 = <ANA-5>: Fast Initial Link Setup 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.

***Modify section 8.4.2.27.3 as indicated:***

* AKM suites

The AKM Suite Count field indicates the number of AKM suite selectors that are contained in the AKM Suite List field.

The AKM Suite List field contains a series of AKM suite selectors contained in the RSN (#1684)element. In an IBSS(#13085) only a single AKM suite selector may be specified because STAs in an IBSS (#10287)use the same AKM suite and because there is no mechanism to negotiate the AKMP in an IBSS (see 11.5.5).

Each AKM suite selector specifies an AKMP. Table 8-101 gives the AKM suite selectors defined by this -standard. An AKM suite selector has the format shown in Figure 8-187.(#11242)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * Table 8-101-- AKM suite selectors | | | | |
| OUI | Suite type | Meaning | | |
| Authentication type | Key management type | Key derivation type (11w) |
| 00-0F-AC | <ANA-6> | FILS | FILS key management as defined in 11.9a | Defined in 11.9.a |
| 00-0F-AC | <ANA-6>+1 –255 | Reserved | Reserved | Reserved |
| Vendor OUI | Any | Vendor-specific | Vendor-specific | Vendor-specific |
| Other | Any | Reserved | Reserved | Reserved |

***Modify section 10.3.2.2 as indicated:***

* Authentication—originating STA

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA(#3097) shall authenticate with the indicated STA using the following procedure:(11r)

* If the STA is in an IBSS the SME shall delete any PTKSA and temporal keys held for communication with the indicated(#11069) STA by using the MLME-DELETEKEYS.request primitive (see 11.5.12 (RSNA security association termination)).(#10600)
* (#1342)The STA(#10600) shall execute one of the following:(11r)
* 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.(11r)
* 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).(#10600)(11r)
* For SAE authentication in an ESS, IBSS, or MBSS, the authentication mechanism described in 11.3 (Authentication using a password).(11s)

4) For FILS authentication in an ESS or IBSS, the authentication mechanism described in 11.9a (FILS Authentication).

* If the authentication was successful within the AuthenticateFailureTimeout(#1342), the state(#1342) for the indicated STA shall be set to State 2 if it was State 1; the state shall remain unchanged if it(Ed) was other than State 1.(#10600)
* The MLME(#1342) shall issue an MLME-AUTHENTICATE.confirm primitive to inform the SME of the result of the authentication.

***Modify section 10.3.2.3 as indicated:***

* Authentication—destination STA

Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA(#3097) shall authenticate with the originating(#1342) STA using the following procedure:

1. If FILS authentication is being used in an ESS or IBSS, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, including the FILS authentication element, and the SME shall execute the procedure described in 11.9a (Authentication for fast link setup)

***Modify section 11.5.1.1.1 and 11.5.1.1.2 as indicated:***

* Security association definitions
* General(#2119)

IEEE Std 802.11 uses the notion of a security association to describe secure operation. Secure communications are possible only within the context of a security association, as this is the context providing the state—cryptographic keys, counters, sequence spaces, etc.—needed for correct operation of the IEEE 802.11 cipher suites.

A security association is a set of policy(ies) and key(s) used to protect information. The information in the security association is stored by each party of the security association, needs to(#10380) be consistent among all parties, and needs to(#10380) have an identity. The identity is a compact name of the key and other bits of security association information to fit into a table index or an MPDU. The following types of security associations are supported by an RSN STA(11w):

* PMKSA: A result of a successful IEEE 802.lX exchange, SAE authentication, FILS authenticaiton,(11s) preshared PMK information, or PMK cached via some other mechanism.
* PMKSA

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. When the PMKSA is the result of a successful SAE authentication, it is generated as a result of the successful completion of the SAE exchange.(11s) When the PMKSA is the result of a successful FILS authentication, it is generated as a result of the successful completion of the FILS authentication protocol. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is created by the Supplicant’s SME when the EAP authentication, or FILS authenticaiton completes successfully or the PSK is configured. The PMKSA is created by the Authenticator’s SME when the PMK is created from the keying information transferred from the AS, when IEEE 802.1X authentication is utilized, or when the SAE exchange or FILS authentication exchange successfully completes(11s) or the PSK is configured. The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes. The PMKSA consists of the following elements:

***Modify section 11.5.1.3.2 as indicated:***

* Security association in an ESS

In an ESS there are two cases:

* Initial contact between the STA and the ESS
* Roaming by the STA within the ESS

A STA and AP establish an initial security association via the following steps:

* The STA selects an authorized ESS by selecting among APs that advertise an appropriate SSID and capabilities.
* The STA then performs(11s) IEEE 802.11(11s) authentication followed by association to the chosen AP. Confirmation(11s) of security parameters takes place during association. A STA performing IEEE 802.1X authentication uses Open System authentication. A STA performing secure password-based, or PSK, authentication uses SAE authentication.(11s) A STA performing authentication for fast initial link set-up performs FILS authentication.

NOTE 1—It is possible for more than one PMKSA to exist. As an example, a second PMKSA might(#10381) come into existence through PMKSA caching. A STA might leave the ESS and flush its cache. Before its PMKSA expires in the AP’s cache, the STA returns to the ESS and establishes a second PMKSA from the AP’s perspective.

NOTE 2—An attack altering the security parameters is(#10369) detected by the key derivation procedure.

NOTE 3—IEEE 802.11 Open System authentication provides no security, but is included to maintain backward compatibility with the IEEE 802.11 state machine (see 10.3 (STA authentication and association)).

* SAE authentication and FILS authentication provide mutual authentication and derivation of a PMK. If Open System authentication is chosen instead,(11s) the (#3098)Authenticator or the (#3098)Supplicant initiates IEEE 802.1X authentication. The EAP method used by IEEE Std 802.1X-2004(#10369) needs to support mutual authentication, as the STA needs assurance that the AP is a legitimate AP.

NOTE 1—Prior to the completion of IEEE 802.1X authentication and the installation of keys, the IEEE 802.1X Controlled Port in the AP blocks(#10369) all data frames. The IEEE 802.1X Controlled Port returns to the unauthorized state and blocks all data frames before invocation of an MLME-DELETEKEYS.request primitive. The IEEE 802.1X Uncontrolled Port allows IEEE 802.1X frames to pass between the Supplicant and Authenticator. Although IEEE Std 802.1X-2004 does not require a Supplicant Controlled Port, this standard assumes that the Supplicant has a Controlled Port in order to provide the needed level of security. Supplicants without a Controlled Port compromise RSN security and are not(#10382) used.

NOTE 2—Any secure network cannot support promiscuous association, e.g., an unsecured operation of IEEE Std 802.11. A trust relationship is needed(#10383) between the STA and the AS of the targeted SSID prior to association and secure operation, in order for the association to be trustworthy. The reason is that an attacker can deploy a rogue AP just as easily as a legitimate network provider can deploy a legitimate AP, so some sort of prior relationship is necessary to establish credentials between the ESS and the STA.

* The last step is key management. The authentication process, whether SAE authentication or FILS authentication utilizing IEEE 802.11 authentication frames or IEEE 802.1X authentication utilizing data frames post association, creates cryptographic keys shared between the cryptographic endpoints—the AP and STA,(11s) or the IEEE 802.1X AS and the STA, when using SAE/FILS or IEEE 802.1X, respectively. When using IEEE 802.1X(11s) the AS transfers these keys to the AP, and the AP and STA uses one of the key confirmation handshakes, e.g., the 4-Way Handshake or FT 4-Way Handshake,(#1038) to complete security association establishment. When using SAE authentication there is no AS and therefore no key transfer; the 4-way Handshake is performed directly between the AP and STA.(11s) The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected (#13074)robust management frames(11w).FILS authentication performs key confirmation as part of the exchange and no additional handshake is necessary.

When FT is not enabled, a STA roaming within an ESS establishes a new PMKSA by one of the four(11s) schemes:(#1039)

* In the case of (re)association followed by IEEE 802.1X or PSK authentication, the STA repeats the same actions as for an initial contact association, but its Supplicant also deletes the PTKSA when it roams from the old AP. The (#3098)Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all BSSIDs in the ESS.
* In the case of SAE authentication followed by (re)association, the STA repeats the same actions as for initial contact association, but the non-AP STA also deletes the PTKSA when it roams from the old AP. Note that a STA can take advantage of the fact that it can perform SAE authentication to multiple APs while maintaining a single association with one AP, and then use any of the PMKSAs created during authentication to effect a fast BSS transition.(11s)
* In the case of FILS authentication, the STA repeats the same actions as for initial contact and authentication. Note that a STA can take advantage of the fact that it can initiate FILS authentication to multiple APs while maintaining a single association with one AP, and finalize the FILS authentication with one AP.