IEEE P802.11
Wireless LANs

|  |
| --- |
| Defining OWE in 802.11 |
| Date: 2022-02-08 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes a resolution to CID 1084 from LB258.

**CID 1084**

*Comment*: if we're gonna start referring to OWE we should not treat it like a red-headed step child.

*Proposed Change*: Fully define OWE. Make a ref to RFC 8110 in 9.4.2.24.3, and in table 12-11 and every other place it needs definition. Yes this is a broad comment. There may be tendrils that need addressing so the scope of this CID must therefore be broad.

*Discussion*: At the time it was proposed, OWE was controversial enough and its utility was not well understood so it was decided to let the IETF define it and to give it a code point. Over time the perception of OWE has changed. It is widely implemented and is being proposed as a replacement for Open networks in 6GHz. It is possible to use RFC 8110 as the definition of the protocol in order to simply add support for it to the standard.

A straw poll in a TGme teleconference on January 24th, 2022 on whether OWE should be deemed an RSNA protocol passed 8-1-9-10, so adding it as an RSNA seems like the way to go. Arguably, this changes the definition of RSNE because there has been no unauthenticated method of connecting outside of Open (which is ***NOT*** an RSNE) and authentication in an RSNE has always been implied to be mutual. That said, the language on the subject is in an informative note that is obviously talking about 802.1x (it discusses assumptions around the AS, for instance) so restating that assumption and adding text regarding OWE won’t break anything.

*Proposed Resolution*: implement the editor instructions defined in {this document}.

*Instruct the editor to modify section 6.3.7 as indicated:*

**6.3.7.2 MLME-ASSOCIATE.request**

**6.3.7.2.1 Function**

This primitive requests association with a specified peer MAC entity that is within an AP.

**6.3.7.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-ASSOCIATE.request(

 PeerSTAAddress,

 BSSMaxIdlePeriod,

 ListenInterval,

 …

 WUR Mode,(11ba)

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for use in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.7.3 MLME-ASSOCIATE.confirm**

**6.3.7.3.1 Function**

This primitive reports the results of an association attempt with a specified peer MAC entity that is within an AP or PCP.

**6.3.7.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-ASSOCIATE.confirm(

 ResultCode,

 CapabilityInformation,

 AssociationID,

 …

 WUR Mode,(11ba)

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is present in the Association Response frame received from the AP; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for the AP from the Association Response frame that is used in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.7.4 MLME-ASSOCIATE.indication**

**6.3.7.4.1 Function**

This primitive indicates that a specific peer MAC entity is requesting association with the local MAC entity, which is in an AP or PCP..

**6.3.7.4.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-ASSOCIATE.indication(

 PeerSTAAddress,

 CapabilityInformation,

 BSSMAXIdlePeriod,

 …

 WUR Mode,(11ba)

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Association Request frame received from the STA; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key from the peer MAC entity for use in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.7.5 MLME-ASSOCIATE.response**

**6.3.7.5.1 Function**

This primitive is used to send a response to a specific peer MAC entity that requested an association with the STA that issued this primitive, which is in an AP or PCP.

**6.3.7.5.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-ASSOCIATE.response(

 PeerSTAAddress,

 ResultCode,

 AssociationID,

 …

 WUR Mode,(11ba)

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for the STA that issued this primitive, it is used in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

*Instruct the editor to modify section 6.3.8 as indicated:*

**6.3.8.2 MLME-REASSOCIATE.request**

**6.3.8.2.1 Function**

This primitive requests a change in association to a specified peer MAC entity that is in an AP or PCP.

**6.3.8.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-REASSOCIATE.request(

 NewPCPorAPAddress,

 BSSMaxIdlePeriod,

 ListenInterval,

 …

 WUR Mode,(11ba),

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for use in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.8.3 MLME-REASSOCIATE.confirm**

**6.3.8.3.1 Function**

This primitive reports the results of a reassociation attempt with a specified peer MAC entity that is within an AP or PCP.

**6.3.8.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-REASSOCIATE.confirm(

 ResultCode,

 CapabilityInformation,

 AssociationID,

 …

 WUR Mode,(11ba),

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Association Response frame received from the AP; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for the AP from the Reassociation Response frame that is used in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.8.4 MLME-REASSOCIATE.indication**

**6.3.8.4.1 Function**

This primitive indicates that a specific peer MAC entity is requesting reassociation with the local MAC entity, which is in an AP or PCP..

**6.3.8.4.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-REASSOCIATE.indication(

 PeerSTAAddress,

 CurrentAPAddress,

 CapabilityInformation,

 …

 WUR Mode,(11ba),

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is present if dot11WUROptionImplemented is true and the WUR Mode element is present in the Association Request frame received from the STA; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key from the peer MAC entity for use in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

**6.3.8.5 MLME-REASSOCIATE.response**

**6.3.8.5.1 Function**

This primitive is used to send a response to a specific peer MAC entity that requested a reassociation with the STA that issued this primitive, which is in an AP or PCP.

**6.3.8.5.2 Semantics of the service primitive**

The primitive parameters are as follows:

 MLME-REASSOCIATE.response(

 PeerSTAAddress,

 ResultCode,

 AssociationID,

 …

 WUR Mode,(11ba),

 Diffie-Hellman Parameter,

 VendorSpecificInfo

 )

|  |  |  |  |
| --- | --- | --- | --- |
|  **Name** |  **Type** |  **Valid range** |  **Description** |
|  WUR Mode | WUR Mode element | As defined in 9.4.2.293 (WUR Mode element)) | Specifies the proposed service parameters for the WUR Mode Setup request. The parameter is optionally present if dot11WUROptionImplemented is true; otherwise, this parameter is not present. |
| Diffie-Hellman Parameter | Diffie-Hellman Parameter element | As defined in RFC 8110 | Provides a public key for the STA that issued this primitive, it is used in the OWE exchange. Present if OWE is being performed; otherwise it is not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.25 (Vendor Specific element) | Zero or more elements |

*Instruct the editor to modify table 9-188 as indicated:*

 **Table 9-188—AKM suite selectors**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  OUI | Suite Type | Authentication type | Key management type | Key derivation type | Authentication algorithm numbers (see 9.4.1.1 (Authentication Algorithm Number field)) | Cipher suite selection restriction |
| 00-0F-AC | 18 | None | RSNA key management as defined in 12.7 (Keys and key distribution) | RFC 5869 using hash algorithm as defined in RFC 8110 | Open |  None |

*Instruct the editor to modify section 12.2.2 as indicated:*

**12.2.2 Security methods**

RSNA security comprises the following algorithms and procedures:

* TKIP, described in 12.5.2 (Temporal key integrity protocol (TKIP))
* CCMP, described in 12.5.3 (CTR with CBC-MAC protocol (CCMP))
* GCMP, described in 12.5.5 (GCM protocol (GCMP))
* BIP, described in 12.5.4 (Broadcast/multicast integrity protocol (BIP))
* RSNA establishment and termination procedures, including use of IEEE 802.1X authentication, described in 12.6 (RSNA security association management), SAE authentication described in 12.4 (Authentication using a password), and OWE described in RFC 8110

*Instruct the editor to modify section 12.2.4 and 12.2.5 as indicated:*

**12.2.4 RSNA establishment**

An SME establishes an RSNA in one of seven ways:

1. When an RSNA STA chooses not to associate with a peer in a PBSS, its SME establishes an RSNA with the peer following the RSNA establishment steps in an IBSS in accordance with method c) or d) above, as appropriate, with the caveat that the RSNA authentication and key management algorithm is executed only once between the peers
2. If an RSNA allows for confidentiality-only (no authentication) in an infrastructure BSS, the SME establishes an RSNA as follows:
	1. It identifies the AP as an RSNA AP from the AP’s Beacon, DMG Beacon, Announce, Information Response, or Probe Response frames.
	2. It shall invoke Open System authentication if the STA is a non-DMG STA.
	3. It negotiates cipher suites and performs a Diffie-Hellman exchange duringthe association process as described in 12.6.2 (RSNA selection), 12.6.3 (RSNA policy selection in an infrastructure BSS), and RFC 8110 (Opportunistic Wireless Encryption).
	4. It establishes one or more temporal keys by executing a key management algorithm using the protocol defined in 12.7 (Keys and key distribution)
	5. It protects the data link by programming the negotiated cipher suites, and the established temporal key into the MAC and then invoking protection.
	6. If the STAs negotiate management frame protection, the SME programs the TK and pairwise cipher suite into the MAC for protection of individually addressed robust Management frames. It also installs the IGTK and IPN for protection of group addressed robust Management frames.
	7. If beacon protection is enabled, the SME programs the BIGTK and BIPN into the MAC for protection of Beacon frames.

**12.2.5 RSNA assumptions and constraints**

An RSNA assumes the following:

1. Mutual authentication, when employed, needs to be strong, meaning impersonation attacks are computationally infeasible when based on the information exposed by the authentication.

*Instruct the editor to modify table 12-11 as indicated:*

 **Table 12-11—Integrity and key wrap algorithms**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  AKM | Integrity algorithm | KCK\_bits | Size of MIC | Key wrap algorithm | KEK\_bits | KCK2\_bits | KEK2\_bits |
| 00-0F-AC:17 | AES-SIV-512/HMAC-SHA-384 | 0 | 0/24 | AES-SIV-512/NIST AES Key Wrap | 512 | 192 | 256 |
| 00-0F-AC:18 | HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 | 128/192/256 | 16/24/32 | NIST AES Key Wrap | 128/256/256 | 0 | 0 |
| 00-0F-AC:19 | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |

*Instruct the editor to modify sections 12.6.1.1.1, 12.6.1.1.2, and 12.6.1.3.2 as indicated:*

**12.6.1.1 Security association definitions**

**12.6.1.1.1 General**

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 be consistent among all parties,

and needs to 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 RSNA STA:

* PMKSA: A result of a successful IEEE 802.1X exchange, OWE exchange, SAE authentication, FILS authentication, or preshared PMK information. A PMKSA can be cached.

**12.6.1.1.2 PMKSA**

The PMKSA is created by the Authenticator’s SME and Supplicant’s SME when EAP authentication, SAE authentication, FILS authentication, or an OWE exchange completes successfully, or when the PSK is configured.

**12.6.1.3.2 Security association in an ESS**

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

1. The STA selects an authorized ESS by selecting among APs that advertise an appropriate SSID.
2. The STA then performs IEEE 802.11 authentication followed by association to the chosen AP. Confirmation of security parameters takes place during association. A STA performing IEEE 802.1X authentication uses Open System authentication. A STA performing password-based authentication can use SAE authentication. A STA performing FILS uses FILS authentication. A STA executing the OWE exchange uses Open System authentication.

NOTE 5—A secure IEEE 802.1X network cannot support promiscuous association, e.g., an unauthenticated operation of IEEE Std 802.11. A trust relationship is needed between the STA and the AS of the targeted SSID prior to association and secure operation, in order for the association to be trustworthy.Without some sort of prior relationship between the ESS and the STA an attacker could deploy a rogue AP that would not be detected by the STA.

NOTE 6—OWE networks are promiscuous and do not require any prior relationship between the ESS and STA. There is a guarantee of confidentiality of the communication between the STA and AP but there is no authentication. OWE networks are therefore not suited to situations where detection of a rogue access point is necessary or where networks require definitive identification of associated STAs.

1. The last step is key management. The authentication process, whether SAE authentication or FILS authentication utilizing Authentication frames or IEEE 802.1X authentication utilizing Data frames post association, or the OWE exchange utilizing Association frames creates cryptographic keys shared between the cryptographic endpoints—the AP and STA, or the IEEE 802.1X AS and the STA, when using SAE/FILS/OWE or IEEE Std 802.1X, respectively. When using IEEE Std 802.1X, 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, to complete security association establishment. When using SAE authentication or OWE there is no AS and therefore no key transfer; the 4-way handshake is performed directly between the AP and STA. The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected robust Management frames. When FILS authentication is performed, the key confirmation is performed using association frames. Hence, no additional handshake is necessary.

When FT is not enabled, a STA roaming within an ESS establishes a new PMKSA by one of the five schemes:

* In the case of (re)association followed by IEEE 802.1X authentication, PSK authentication, or the OWE exchange 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 Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all BSSIDs in the ESS.
* A STA (AP) can cache PMKSAs for APs (STAs) in the ESS to which it has previously performed a full IEEE 802.1X authentication, SAE authentication, or OWE exchange. If a STA wishes to roam to an AP for which it has cached one or more PMKSAs, it can include one or more PMKIDs in the RSNE of it (Re)Association Request frame. An AP that has retained the PMK for one or more of the PMKIDs can proceed with the 4-way handshake (see 12.6.10.3 (Cached PMKSAs and RSNA key management)). If the STA fails to send a PMKID when the negotiated AKM uses IEEE 802.1X authentication, the STA and AP need to perform a full IEEE 802.1X authentication.

*Instruct the editor to modify section 12.6.10 as indicated:*

**12.6.10 RSNA establishment in an infrastructure BSS**

**12.6.10.1 General**

When establishing an RSNA in a non-FT environment or during an FT initial mobility domain association, a STA shall use IEEE 802.11 SAE authentication, FILS authentication, or Open System authentication prior to (re)association.

SAE authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for SAE in its RSNE.

FILS authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds an AP that advertises support for FILS authentication in its RSNE.

OWE is initiated when a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for OWE in its RSNE.

*Instruct the editor to modify section 12.12.2 as indicated:*

**12.12.2 Security constraints in the 6 GHz band**

The following apply to a STA operating in the 6 GHz band:

* The STA shall not use the following pre-RSNA security methods:
* WEP
* Open System authentication without encryption
* Shared Key authentication
* The STA shall not use the following cipher suite selectors:
* 00-0F-AC:0 (Use group cipher suite)
* 00-0F-AC:1 (WEP-40)
* 00-0F-AC:2 (TKIP)
* 00-0F-AC:5 (WEP-104)
* The STA shalluse Opportunistic Wireless Encryption (12.2.4 (RSNA establishment) using IETF RFC 8110) when connecting in an infrastructure BSS without authentication (as a replacement for Open System authentication without encryption).

**References:**