IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Comment Resolution from the 3rd Recirculation | | | | |
| Date: 2011-04-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CIDs: 3003, 3004, 3005, 3006, 3007, 3008, 3010, 3011, 3012, 3013, 3014, 3129, 3130, 3134, 3135, 3136, 3137, 3140, 3141, 3142, 3143, 3144, 3145, 3146, 3147, 3148, 3204, 3213, 3220, 3226, 3227, 3228, and 3229. In addition, it removes the term PMKName from the draft and replaces it with the more correct PMKID and it removes the PMKID, peerLinkID and peerNonce from the set of data that are used to locate a mesh peering (i.e. the mesh peering identifier).

***Modify section 7.3.2.102 as indicated:***

* Mesh Peering Management element

The Mesh Peering Management element is used to manage a mesh peering with a peer mesh STA. The format of the Mesh Peering Management element is shown in Figure 7-95o137 (Mesh Peering Management element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | Local Link ID | Peer Link ID (conditional) | Reason Code (conditional) | Chosen PMK (optional) |
| Octets: 1 | 1 | 2 | 2 | 2 | 16 |
| * Mesh Peering Management element format | | | | | |

The Chosen PMK field is present when dot11MeshSecurityEnabled is true and contains the PMKID used to identify the PMK used to protect the Mesh Peering Management frame.

***Modify section 7.4.14.2.2 as indicated:***

* Mesh Peering Open frame details

The Mesh Peering Open frame is used to open a mesh peering using the procedures defined in 11C.3 (Mesh peering management (MPM)). The Mesh Peering Open frame is also, together with Mesh Peering Confirm and Mesh Peering Close Action frames, referred to as a Mesh Peering Management frame. The format of the Mesh Peering Open frame Action field is shown in Table 7-57v25 (Mesh Peering Open frame Action field format).

|  |  |  |
| --- | --- | --- |
| * Mesh Peering Open frame Action field format | | |
| Order | Information | Notes |
|  | MIC element | MIC element is present when dot11MeshSecurityActivated is true and a PMK exists between the sender and recipient of this frame. |
| Last | Authenticated Mesh Peering Exchange | The Authenticated Mesh Peering Exchange element is present when dot11MeshSecurityActivated is true and a PMK exists between the sender and receipient of this frame. |

***Modify section 7.4.14.3.2 as indicated:***

* Mesh Peering Confirm frame details

The Mesh Peering Confirm frame is used to confirm a mesh peering using the procedures defined in 11C.3 (Mesh peering management (MPM)). The Mesh Peering Confirm frame is also, together with Mesh Peering Open and Mesh Peering Close Action frames, referred to as a Mesh Peering Management frame. The format of the Mesh Peering Confirm frame Action field is shown in Table 7-57v26 (Mesh Peering Confirm frame Action field format).

|  |  |  |
| --- | --- | --- |
| * Mesh Peering Confirm frame Action field format | | |
| Order | Information | Notes |
|  | MIC element | MIC element is present when dot11MeshSecurityActivated is true and a PMK exists between the sender and recipient of this frame. |
| Last | Authenticated Mesh Peering Exchange | The Authenticated Mesh Peering Exchange element is present when dot11MeshSecurityActivated is true and a PMK exists betwee n the sender and recipient of this frame.. |

***Modify section 7.4.14.4.2 as indicated:***

* Mesh Peering Close frame details

The Mesh Peering Close frame is used to close a mesh peering using the procedures defined in 11C.3 (Mesh peering management (MPM)). The Mesh Peering Close frame is also, together with Mesh Peering Open and Mesh Peering Confirm Action frames, referred to as a Mesh Peering Management frame. The format of the Mesh Peering Close frame Action field is shown in Table 7-57v27 (Mesh Peering Close frame Action field format).

|  |  |  |
| --- | --- | --- |
| * Mesh Peering Close frame Action field format | | |
| Order | Information | Notes |
|  | MIC element | MIC element is present when dot11MeshSecurityActivated is true and a PMK exists between the sender and the recipient of this frame. |
| Last | Authenticated Mesh Peering Exchange | The Authenticated Mesh Peering Exchange element is present when dot11MeshSecurityActivated is true and a PMK exists between the sender and the recipient of this frame. |

***Modify section 8.2a.5.1 as indicated:***

* Message exchanges

The protocol consists of two message exchanges, a commitment exchange and a confirmation exchange. The commitment exchange is used to force each party to the exchange to commit to a single guess of the password. The confirmation exchange is used to prove that the password guess was correct.The rules for performing these exchanges are specified by the finite state machine in 8.2a.8 (SAE finite state machine).

When a party has sent its message in the commit exchange it is said to have *committed* and when it has sent its message in the confirmation exchange it has *confirmed*. The following rules are ascribed to the protocol:

* A party may *commit* at any time
* A party *confirm*s after it has *committed* and its peer has *committed*
* A party *accept*s authentication after a peer has *confirmed*
* The protocol successfully *terminates* after each peer has *accepted*

***Modify section 8.4.1.1.1c as indicated:***

* Mesh PMKSA

The mesh PMKSA is the result of successful completion of the active authentication protocol. This security association is bidirectional. The two authenticated parties use the information in the security association for both sending and receiving. The mesh PMKSA is created by the Mesh STA’s SME when the active authentication protocol completes successfully with the peer mesh STA. The mesh PMKSA is used to create the mesh TKSA. Mesh PMKSAs are cached for up to their lifetimes. Mesh PMKSAs contain the following elements, and are identified by their PMKID.

* PMKID, as defined in 8.2a.5.4 (Processing of a peer’s Commit Message).
* Mesh STA’s MAC address
* Peer mesh STA’s MAC address
* PMK
* AEK, as defined in 8.8.1 (Keys and key derivation algorithm)
* Lifetime, as defined in 8.5.1.2
* Selected AKM suite (see 7.3.2.25.2 (AKM Suites))

***Modify section 8.4.1.1.2a as indicated:***

* Mesh TKSA

The mesh TKSA is a result of the AMPE. This security association is also bidirectional. The mesh TKSA shall be deleted when the lifetime expires. The mesh TKSA contains the following elements:

* MTK, as defined in 8.8.1 (Keys and key derivation algorithm)
* PMKID
* local mesh STA MAC address
* peer mesh STA MAC address
* local Link ID
* peer Link ID
* local nonce
* peer nonce
* Lifetime
* Pairwise cipher suite selector

***Modify section 11C.3.2 as indicated:***

* Mesh authentication

In order to create a secure peering, mesh STAs first authenticate each other and create a mesh PMKSA. This can be done using either SAE or IEEE 802.1X. Mesh STAs shall support SAE authentication (see 8.2a (Authentication using a password)) using a pre-shared secret with the candidate peer mesh STA. Optionally, mesh STAs may support IEEE 802.1X authentication (see 5.8 (IEEE Std 802.11 and IEEE Std 802.1X-2004))..

When dot11MeshActiveAuthenticationProtocol is 1 (SAE) the scanning mesh STA shall initiate SAE to the candidate mesh STA. If SAE terminates unsuccessfully, the scanning mesh STA shall terminate the peering establishment procedure. Otherwise, the PMK that results from successful SAE authentication shall be used to create a mesh PMKSA.

When dot11MeshActiveAuthenticationProtocol is 2 (802.1X), then the scanning mesh STA shall initiate the MPM protocol to establish a peering. If the MPM protocol fails then the scanning mesh STA shall terminate the peering establishment procedure. Otherwise, IEEE 802.1X authentication shall be performed between the two peers according to the following:

* If only one mesh STA has the Connected to AS field set to 1, that STA shall act as the IEEE 802.1X authenticator and the other STA shall act as the IEEE 802.1X supplicant;
* If both mesh STAs have the Connected to AS field set to 1, then the mesh STA with the higher MAC address shall act as the IEEE 802.1X authenticator and the other mesh STA will act as the 802.1X IEEE supplicant (see 8.5.1 (Key hierarchy) for MAC comparison).

If IEEE 802.1X authentication fails, the peering establishment procedure shall be terminated and the peering established between the two mesh STAs shall be closed. Otherwise, the peering established between the two mesh STAs shall be closed and a mesh PMKSA shall be created using the PMK that resulted from the successful IEEE 802.1X authentication.

***Modify section 11C.3.3.1 as indicated:***

* Overview

A mesh STA uses a mesh peering instance controller to manage all mesh peering instances.

The mesh peering instance controller performs the following functions:

* Create and destroy MPM finite state machines and AMPE finite state machines
* Manage instance identifiers for each mesh peering instance
* Manage mesh TKSAs for each mesh peering instance when dot11MeshSecurityActivated is true
* Pre-process the incoming Mesh Peering Management frames and pass the frames to the finite state machine with matching instance identifier
* Pass internal commands to the finite state machine with matching instance identifier

A mesh peering instance is identified by a mesh peering instance identifier. The mesh peering instance identifier consists of the localLinkID, , localMAC, and peerMAC.

A mesh peering instance consists of its identifier (the localLinkID, localMAC, peerMAC), a peerLinkID (an integer generated by the peer mesh STA or candidate peer mesh STA), and the configuration and capability negotiated and agreed upon by exchanging Mesh Peering Open frames (see 7.4.14.2) and Mesh Peering Confirm frames (see 7.4.14.3). If dot11MeshSecurityActivated is true, the mesh peering instance also contains a PMKID identifying the shared PMKSA, a localNonce chosen by the mesh STA and a peerNonce chosen by the peer mesh STA or candidate peer mesh STA.

The localMAC is the MAC address of the mesh STA that is managing this mesh peering instance. The peerMAC is the MAC address of the peer mesh STA or the candidate peer mesh STA. The localLinkID is an integer generated by the mesh STA. The localLinkID shall be unique among all existing link identifiers used by the mesh STA for its MPM finite state machines. The mesh STA selects the localLinkID to provide high assurance that the same number has not been used to identify a recent MPM finite state machine. The peerLinkID is the localLinkID of the peer mesh STA or candidate peer mesh STA and is supplied in the Mesh Peering Management element (see 7.3.2.102 (Mesh Peering Management element)) of the Mesh Peering Open and Mesh Peering Confirm frames.

***Modify section 11C.3.3.2 as indicated:***

* Creating a new mesh peering instance

The mesh peering instance controller creates a new mesh peering instance after either of the following two events:

* The receipt of a Mesh Peering Open frame from a candidate peer mesh STA according to the rules of 11C.3.4 (Mesh peering instance selection)
* The receipt of an MLME-MESHPEERINGMANAGEMENT.request primitive with a Mesh Peering Open frame

A unique localLinkID shall be generated for the mesh peering instance. If the mesh peering instance is established by AMPE, a random local nonce shall also be generated.

***Delete section 11C.3.3.3 and adjust the section numbering for subsequent sub-sections:***

***Modify section 11C.3.4 as indicated:***

* Mesh peering instance selection

The content of a Mesh Peering Management frame received from a candidate peer mesh STA, and the set of mesh peering instances in the mesh peering instance controller determine whether

* A new mesh peering instance is created (see 11C.3.3.2 (Creating a new mesh peering instance)); or,
* An existing mesh peering instance is updated .

If the Mesh Peering Protocol Identifier field in the Mesh Configuration element indicates “mesh peering management protocol,” the Authenticated Mesh Peering element and MIC element, if present in the frame, shall be ignored.

If the Mesh Peering Protocol Identifier field in the Mesh Peering Management element indicates “authenticated mesh peering exchange” and the Authenticated Mesh Peering Exchange element or MIC element is not included in the frame, the frame shall be silently discarded.

If the frame contains a group address in TA or RA, it shall be silently discarded.

If the incoming Mesh Peering Management frame is for AMPE and the Chosen PMK from the received frame contains a PMKID that does not identify a valid mesh PMKSA, the frame shall be silently discarded.

If the Mesh Peering Management frame has not been silently discarded, the mesh peering instance controller attempts to locate a matching mesh peering instance identifier. A match is determined by checking the contents of the Mesh Peering Management frame with each peering instance. A match is found if all the following conditions are true:

* The transmitter’s MAC address (address 2) is the same as the peerMAC of the mesh peering instance
* The receiver’s MAC address(address 1) is the same as the localMAC of the mesh peering instance
* The value of the Peer Link ID field is the same as the localLinkID of the mesh peering instance

If the incoming frame is a Mesh Peering Open frame and no matching peering instance was found, a new mesh peering instance is created (and a new Mesh TSKA if dot11MeshSecurityActivated is true). See 11C.3.3.2 (Creating a new mesh peering instance).

If the incoming frame is a Mesh Peering Confirm or Mesh Peering Close frame and no matching mesh peering instance is found, it shall be silently discarded.

If the incoming Mesh Peering Management frame is for AMPE and has not been discarded it shall be further processed as follows:

* If the Peer Nonce field is present in the received frame, and the localNonce in the mesh peering instance is different than the Peer Nonce field of the received frame, the frame shall be dropped.
* If the peerNonce in the mesh peering instance exists and is different than the Local Nonce field of the received frame, the frame shall be dropped.

***Modify section 11C.3.5.2 as indicated:***

* Mesh Peering Open frame processing

The mesh STA checks that the Mesh ID element and Mesh Configuration element of the Mesh Peering Open frame is identical to its own mesh STA configuration as specified in 11C.2.3 (Mesh profile) and 11C.2.4 (Mesh STA configuration). If a mismatch is found the frame shall be rejected with a reason code of MESH-CONFIGURATION-POLICY-VIOLATION and the mesh peering establishment attempt shall be terminated.

When the mesh STA has established a mesh PMKSA with the candidate peer mesh STA, the mesh peering instance controller shall silently discard the Mesh Peering Open frame in the following two conditions:

* The Mesh Peering Open frame supports MPM protocol and the negotiated active authentication is SAE, or
* The Mesh Peering Open frame supports AMPE but the PMKID in the Chosen PMK field in the Authenticated Mesh Peering Exchange element does not identify a mesh PMKSA.

If the Mesh Peering Open frame is not discarded, the mesh peering instance controller actively rejects or accepts the mesh peering open request (see 11C.4 (Mesh peering management finite state machine (MPM FSM))). If dot11MeshAcceptingAdditionalPeerings is set to zero the Mesh Peering Open request shall be rejected with reason code MESH-MAX-PEERS.

If the peerLinkID in the mesh peering instance has not been set, the Local Link ID field of the Mesh Peering Open request shall be copied into the peerLinkID in the mesh peering instance. If the incoming Mesh Peering Open frame is for AMPE and the peerNonce in the mesh peering instance has not been set, the Local Nonce field in the incoming Mesh Peering Open frame shall be copied into the peerNonce in the mesh peering instance.

The mesh peering open request may be rejected due to an internal reason with a reason code of MESH-PEERING-CANCELED.

If the Mesh Peering Open request is rejected, the REQ\_RJCT event shall be passed with the specified reason code to the protocol finite state machine to actively reject the mesh peering open request.

NOTE—Example internal reasons to reject new mesh peering request could be the mesh STA has reached its capacity to set up more mesh peering, the mesh STA is configured to reject mesh peering request from another specific peer mesh STA.

***Modify section 11C.3.6.2 as indicated:***

* Mesh Peering Confirm frame processing

The mesh STA shall check that the Mesh ID element and Mesh Configuration element of the Mesh Peering Confirm frame match its own mesh STA configuration as specified in 11C.2.3 (Mesh profile) and 11C.2.4 (Mesh STA configuration). If a mismatch is found, the frame shall be rejected with the reason code of MESH-INCONSISTENT-PARAMETERS.

Otherwise, the mesh STA accepts the Mesh Peering Confirm frame and performs the actions described in 11C.4 (Mesh peering management finite state machine (MPM FSM)).

If the peerLinkID in the mesh peering instance has not been set, the Local Link ID field of the Mesh Peering Confirm request shall be copied into the peerLinkID in the mesh peering instance. If the incoming Mesh Peering Confirm frame is for AMPE and the peerNonce in the mesh peering instance has not been set, the Local Nonce field in the incoming Mesh Peering Confirm frame shall be copied into the peerNonce in the mesh peering instance.

***Modify section 11C.5.5.2.1 as indicated:***

* Generating Mesh Peering Open frames for AMPE

In addition to contents for establishing a mesh peering as specified in 11C.3.5.1 (Generating Mesh Peering Open frames), the Mesh Peering Open frame, when used for the AMPE, shall contain the following:

* In the Mesh Configuration element, the Mesh Peering Protocol Identifier shall be set to 1 “authenticated mesh peering exchange protocol.”
* In the Mesh Peering Management element, the Chosen PMK field shall be set to PMKIDthat identifies the mesh PMKSA the mesh STA established with the candidate peer mesh STA.

***Modify section 11C.6.5 as indicated:***

* Mesh group key implementation considerations

If the MGTK source does not receive a Mesh Group Key Acknowledge frame to its Mesh Group Key Inform frames, it shall attempt dot11MeshConfigGroupUpdateCount additional transmits of the Mesh Group Key Inform frame. The retransmit timeout value shall be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If there is no listen interval, then 100 ms shall be used for all timeout values. If it still has not received a response after this, then the MGTK source shall tear down the mesh peering and mesh TKSA with this MGTK recipient, by generating a CNCL event for the peering instance and pass the event to the mesh peering instance controller.

**References:**

**document 11-11/0539r0**