IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SAE anti-clogging token | | | | |
| Date: 2019-12-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses the SAE anti-clogging token field design and complexities in P802.11-REVmd/D3.0 and proposes a cleaner design that does not require as complex parsing rules. The proposed design is backwards compatible with the current standard IEEE Std 802.11-2016.

**Discussion**

REVmd has added new fields and elements to SAE Authentication frames: Password Identifier element and Rejected Groups element. These are conditionally included at the end of the frame. Since these are preceded by conditionally included variable length (non-IE) field (Anti-Clogging Token field), parsing of the frame has become significantly more complex. This undesired complexity has resulted in need for 12.4.7.4 describing rules for how to parse the frame. This complexity could be avoided by replacing Anti-Clogging Token field with a new information element, say Anti-Clogging Token Container element, that would encapsulate the Anti-Clogging Token field and by mandating this new element to be used instead of the field whenever using SAE with Password Identifiers or H2E (i.e., the cases that use the new Password Identifier and Rejected Groups elements). This would result in all the non-IE fields being present and all the information elements being at the end of the frame which would simplify parsing significantly.

In addition to simplifying the Anti-Clogging Token field parsing, the proposed changes are addressing couple of errors in the description of when this field is present. The introduction of hash-to-element method for deriving PWE introduced these in Table 9-43.

**Proposed changes**

**9.3.3.11 Authentication frame format**

*Add new row to Table 9-42 and modify Table 9-43 as shown below.*

The frame body of an Authentication frame contains the information shown in Table 9-42 (Authentication frame body). FT authentication is used when FT support is advertised by the AP and dot11FastBSSTransitionActivated is true in the STA. SAE authentication is used when dot11MeshActiveAuthenticationProtocol is sae (1). FILS authentication is used if support for FILS authentication is advertised by the AP and dot11FILSActivated is true in the STA.(11ai)

**Table 9-42—Authentication frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 1 | Authentication algorithm number |  |
| 2 | Authentication transaction sequence number |  |
| 3 | Status code | The status code information is reserved in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). |
| 4(11ai) | Finite Cyclic Group | An unsigned integer indicating a finite cyclic group as described in 9.4.1.42 (Finite Cyclic Group field)(#2437). This is present only in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). |
| 5(11ai) | Anti-Clogging Token | A random bit string used for anti-clogging purposes as described in 12.4.6 (Anti-clogging tokens). This is present only in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). |
| … | | |
| 22(M41) | Password Identifier(M41) | The Password Identifier element is optional present in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames)(M41). |
| 23(M137) | Rejected Groups(M137) | The Rejected Groups element is present only in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). (M137) |
| 24 | Anti-Clogging Token Container | The Anti-Clogging Token Container element is present only in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). |
| Last | Vendor Specific | One or more vendor-specific elements are optionally present. These elements follow all other elements. |

**Table 9-43—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication algorithm** | **Authentication transaction sequence number** | **Status code** | (#2528)**Presence of fields and elements from order 4 onwards** |
| … | | | |
| SAE | 1 | Any | (Ed)The Scalar field(#2531) is present if the Status Code field is zero or 126(M137).  (#2471)(Ed)The FFE field(#2531) is present if the Status Code field is zero or 126(M137).  (#2530)(Ed)When Password Identifier is not used and hunting-and-pecking is used to derive PWE, the Anti-Clogging Token field(#2534) is present if the Status Code field is 76 (M137) or if the Authentication frame is in response to a previous rejection with the Status Code field equal to 76 (M137).  (Ed)The Finite Cyclic Group field(#2531) is present if the Status Code field is zero, 76, 77 or 126(M137).(M104)  (#2530)(M41)(Ed)The Password Identifier element is optionally present if the Status Code field is zero, 123 or 126(M137)(Ed). The Rejected Groups element is conditionally present if the Status Code is 126.(M137)  When either Password Identifier is used or hash-to-element is used to derive PWE, the Anti-Clogging Token Container element is present if the Status Code is 76 or 126 or if the Authentication frame is in response to a previous rejection with the Status Code field equal to 76 or 126. |
| … | | | |

**9.4.1.38 Anti-Clogging Token field**

*No changes in 9.4.1.38 – only included for context.*

The Anti-Clogging Token field is used with SAE authentication for denial-of-service protection as specified in 12.4 (Authentication using a password). See Figure 9-126 (Anti-Clogging Token field format(#2607)).

|  |
| --- |
| Anti-Clogging Token |

Octets: variable

**Figure 9-126—Anti-Clogging Token field format**(#2607)

**9.4.2 Elements**

**9.4.2.1 General**

*Add a new row in Table 9-94 as shown below.*

**Table 9-94—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| … | | | | |
| (M137)Rejected Groups (see 9.4.2.246 (Rejected Groups element(M137))) | 255 | 92 | No | No |
| Anti-Clogging Token Container | 255 | *<ANA>* | No | No |
| Reserved(#1100) | 255 | 93–255(#2693)(#2215)(#1283)(M40) |  |  |
| NOTE— See 10.28.6 (Element parsing) on the parsing of elements.(#283) | | | | |

**9.4.2.x Anti-Clogging Token Container element**

*Add a new subclause at the end of 9.4.2 (after all the existing 9.4.2.x subclauses).*

The Anti-Clogging Token Container element is used to carry Anti-Clogging Token field in contexts where an information element is needed. The format of the Anti-Clogging Token Container element is shown in Figure 9-y (Anti-Clogging Token Container element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Anti-Clogging Token |
| Octets: | 1 | 1 | 1 | variable |

**Figure 9-y—Anti-Clogging Token Container element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Anti-Clogging Token field contents is defined in 9.4.1.38 (Anti-Clogging Token field).

**12.4.7.4 Encoding and decoding of SAE Commit messages**

*Modify 12.4.7.4 as shown below.*

An SAE Commit message shall be encoded as an Authentication frame with an Authentication Algorithm Number field set to 3, a Transaction Sequence Number of 1 and a Status Code of SUCCESS or SAE\_HASH\_TO\_ELEMENT. Status codes not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT indicate a rejection of a peer’s SAE Commit message and are described in 12.4.7.6 (Status codes).(M137)

An SAE Commit message shall consist of a Finite Cyclic Group field (9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (9.4.1.40 (FFE field(#2302))). If the SAE Commit message is in response to an Anti-Clogging Token field(#2534) request (see 12.4.7.6 (Status codes)), the Anti-Clogging Token field(#2534) is present (see 9.4.1.38 (Anti-Clogging Token field)). When a password identifier is used or PWE is derived using hash-to-element, the Anti-Clogging Token field is encapsulated in an Anti-Clogging Token Container element; otherwise, the Anti-Clogging Token field is included in the frame as a separate field as described in Table 9-43 (Presence of fields and elements in Authentication frames). If a password identifier is used in generation of the password element (PWE) the Password identifier element shall be present and the identifier shall be encoded as a UTF-8 string in the Identifier portion of the element (see 9.4.2.216 (Password Identifier element(M41)(M101))).(M41)(M137) If an SAE Commit message with status code equal to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if applicable, to the Rejected Groups field of the Rejected Groups element. Each rejected group shall be represented as an unsigned 16-bit integer using the bit ordering conventions of 9.2.2 (Conventions).

When transmitting an SAE Commit message, the scalar and element shall be converted to octet strings and placed in the Scalar field and FFE field, respectively. The scalar shall be treated as an integer and converted into an octet string of length m such that 28m > r , where r is the order of the group, according to 12.4.7.2.2 (Integer to octet string conversion), and the element shall be converted into (an) octet string(s) according to 12.4.7.2.4 (Element to octet string conversion). When receiving an SAE Commit message the component octet strings in the Scalar field and FFE field(#2530) shall be converted into a scalar and element, respectively, according to 12.4.7.2.3 (Octet string to integer conversion) and 12.4.7.2.5 (Octet string to element conversion), respectively.