IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB232 comment resolution for authentication frame | | | | |
| Date: 2018-04-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Robert Stacey | Intel |  | +1-503-724-0893 | robert.stacey@intel.com |
|  |  |  |  |  |

Abstract

Resolution to CID 1443

## Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 1443 | Mark RISON | 818.01 | 9.3.3.12 | For backward-compatibility, new elements cannot be inserted ahead of elements defined in prior revisions of the standard | In Table 9-39 Authentication frame body move the Multi-band and Neighbor Report rows to be immediately after the Status code row |

## Discussion

802.11ai has moved the yellow fields ahead of the green elements. The yellow fields are relavant for SAE and, at least pre-11ai, do not appear together with any green elements in the same frame. The green elements are relavant for Shared Key (WEP) and FT and, pre-11ai, do not appear together with yellow fields in the same frame. So, as far as legacy compatibility is concerned, a problem has not been created with the reordering.

The FILS Shared Key authentication with PFS algorithm includes the Finite Cyclic Group field and Finite field element (which is actually a field) together with the RSN element in the Authentication frame. This appears to be the motivation for the reordering – to have the fields appear ahead of the element. I don’t see a technical reason for doing this -- the motivation appears to be asthetics. Reverting to the pre-11ai order would create a compatibility issue for STAs that support the FILS Shared Key authentication with PFS algorithm.

|  |  |  |
| --- | --- | --- |
| * 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 9-40 (Presence of fields and elements in Authentication frames). |
| 4(11ai) | Finite Cyclic Group | An unsigned integer indicating a finite cyclic group as described in 12.4.4 (Finite cyclic groups). This is present only in certain Authentication frames as defined in Table 9-40 (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 9-40 (Presence of fields and elements in Authentication frames). |
| 6(11ai) | Send-Confirm | A binary encoding of an integer used for anti-replay purposes as described in 12.4.7.5 (Encoding and decoding of SAE Confirm messages). This is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 7(11ai) | Scalar | An unsigned integer encoded as described in 12.4.7.4 (Encoding and decoding of SAE Commit messages). This is present only in cer-tain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 8(11ai) | Finite field element | A Finite field element field from a finite field encoded as described in 12.4.7.4 (Encoding and decoding of SAE Commit messages). This is present only(Ed) in cer-tain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 9(11ai) | Confirm | An unsigned integer encoded as described in 12.4.7.5 (Encoding and decoding of SAE Confirm messages). This is present only in cer-tain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 10(11ai) | Challenge text | A Challenge Text element is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 11(11ai) | RSN | An RSNE is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 12(11ai) | Mobility Domain | An MDE is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 13(11ai) | Fast BSS Transition | An FTE is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 14(11ai) | Timeout Interval (reassociation deadline) | A TIE containing the reassociation deadline interval is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 15(11ai) | RIC | A resource information container, containing a variable number of elements, is present only in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 16 | Multi-band | The Multi-band element is optionally present if dot11MultibandImplemented is true. |
| 17 | Neighbor Report | One or more Neighbor Report elements are present only in cer-tain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames). |
| 18(11ai) | FILS Nonce(11ai) | The FILS Nonce element is present in FILS Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames).(11ai) |
| 19(11ai) | FILS Session(11ai) | The FILS Session element is present in FILS Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames).(11ai) |
| 20(11ai) | FILS Wrapped Data(11ai) | The FILS Wrapped Data element is present in FILS Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames).(11ai) |
| 21(11ai) | Association Delay Info(11ai) | The Association Delay Info element is present in FILS Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames).(11ai) |
| 22(M41) | Password Identifier(M41) | The Password Identifier element is optional present in certain Authentication frames as defined in Table 9-40 (Presence of fields and elements in Authentication frames)(M41). |
| Last | Vendor Specific | One or more vendor-specific elements are optionally present. These elements follow all other elements. |

## Proposed resolution to 1443:

REJECTED –Authentication frames other than those used with the FILS Shared Key authentication with PFS algorithm do not include included fields with order 4-9 together with elements with order 10-15. The reordering has not created a backward compatibility issue. Reverting to the original order would create a backward compatibility issue for STAs that support the FILS Shared Key authentication with PFS algorithm.