IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Resolution for Comments CID 250 and CID 251 | | | | |
| Date:2013-03-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Lei Wang | InterDigital Communications | 781 Third Ave., King of Prussia, PA 19406 | 1 858 205 7286 | leiw@billeigean.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes a resolution to the Comments, CID 250 and CID 251, in the TGai/D0.2 review comments database, regarding the security field in FILS Discovery frame.

# Introduction

In TGai/D0.2 review comment database, 13/0036r9 [Ref-4], The Comments of CID 250 and CID 251 are as follows:

***CID 250 Comment: by Lei Wang (11-13-008r0)***

*Security field in FD frame needs to be defined.*

***Proposed change:***

*a separate contribution will be submitted by the commenter to define the security field in the FD frame.*

***CID 251 Comment: by David Goodall(11-13-0016r0)***

*The FD Security field is not yet defined.*

***Proposed change:***

*Provide a definition of the FD Security field.*

Note that both above comments identify that the FD Security field is missing and suggest that a definition of FD Security field should be provided. This contribution proposes a detailed definition of the FD Security field, as a proposed resolution to Comments, CID 250 and 251.

# Conventions

In this contribution, the proposed 802.11ai Specification Document text will be presented as modifications to the TGai draft specification 802.11ai/D0.4[Ref-3]. The following format conventions are used:

1. The new added text is marked as blue underline text;
2. The deleted text is marked as ~~red strikethrough text~~;
3. The unchanged baseline standard text stays in black text in the context of proposed TGai specification text;
4. The editorial instruction is marked as *italic text highlighted by Yellow*;
5. The quoted TGai SFD text is marked as *green italic text*; and
6. Any other text, e.g., discussions, proposed motions, etc., is in black text, but not in the context of proposed TGai specification text.

# Discussions

Contribution, 13/0010, was submitted before 2013 January meeting as a proposed resolution to the Comment of CID 250. However, it only contains the security considerations in the FILS Discovery (FD) frame design before 802.11ai TG reached basic agreements of the FILS Authentication schemes.

The FD Security field design should include the considerations of the TGai security related contents in the current TGai draft specification, 802.11ai/D0.4[Ref-3], which are mainly based on the contributions, 12/1045r6, 12/1385r1, 13/0046/r4, 13/0065r0, and 13/0127r2.

This contribution proposes a design of the FD Security indications, which is based on the considerations of supporting both legacy 802.11 security functionalities, e.g., full EAP authentication via IEEE 802.1X authentication, and TGai newly development security functionalities, i.e., FILS authentication schemes, including the FILS authentication using a TTP without PFS; FILS authentication using a TTP with PFS, and FILS authentication without a TTP and with PFS.

Since the security indications required in FILS Discovery frame to support the legacy 802.11 authentications (e.g., full EAP via 802.1X) and the indications required to support FILS authentications are fairly different from each other, we also propose to separately encode those two types of security indications in FD frame, such that an FD frame transmitter can include the two types of security indications separately based on its real needs, to achieve a better message efficiency.

In summary, this contribution proposes the following:

1. Keep the FD Security field in FD frame, but rename it as FD RSN Indications to reflect that it only contains the security indications for legacy 802.11 authentication schemes;
2. Add the FILS Indication element, as defined in subsectio8.4.2.186, to FD frame.

# Proposed 802.11ai Specification Text

The following proposed 802.11ai Specification Document text will be presented as modifications to the TGai draft specification 802.11ai/D0.4 [Ref-3].

*Instructions to Editor: make the following changes in Table 8-221f in line 20 to line 27 on page 40 in Section 8.5.8.34, in the TGai draft specification 802.11ai/D0.4 :*

**Table 8-221f — FILS Discovery frame format**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| ...... |  |  |
| 9 | FD RSN Indications ~~Security~~ | It is an optional field in the FD frame. Its presence is indicated by an 1-bit RSN Indications ~~Security~~ Presence Indicator in the FD Frame Control. |
| 10 | Reduced Neighbour Report | The Reduced Neighbor Report element ~~field~~, as specified in 8.4.2.175, is optionally present. |
| 11 | FILS Indication | The FILS Indication element, as specified in 8.4.2.186, is optionally present. |
| ...... |  |  |

*Instructions to Editor: make the following changes in the box of “Security presence indicator” in Figure 8-460o, in line 55 on page 40 in Section 8.5.8.34, in the TGai draft specification 802.11ai/D0.4 :*

~~Security~~ RSN Indications presence indicator

*Instructions to Editor: append the following text at the end of Section 8.5.8.34, i.e., line 65 on page 42 in the TGai draft specification 802.11ai/D0.4 :*

The FD RSN Indications field contains the security information for the STAs that are not able to use the FILS authentication schemes during initial link setup. It contains the information selected from the RSNE (Robust Security Network Element) as defined in Section 8.4.2.27 and the IP address support information. Its format is defined in Figure 8—460q.



**Figure 8-460q Format of the FD Security Field**

The FD RSN Indications field contains four 4-bit Cipher Suite Selectors, including, one 4-bit Group Data Cipher Suite selector, one 4-bit Group Management Cipher Suite selector, and two 4-bit Pairwise Cipher Suite Selectors. Each 4-bit Cipher Suite selector is a 4-bit code identifying a Cipher Suite Type as specified in Table 8-99. The definition of the 4-bit Cipher Suite Selectors is shown in Table 8-ai-3.

**Table 8-ai-3 Cipher Suite Selector Definitions**

|  |  |
| --- | --- |
| **Cipher Suite Selector (4 bits)** | **Cipher Suite Type** |
| 0b0000 – 0b0111 | Cipher Suite Type 0 to 7, in Table 8-99 |
| 0b1000 – 1101 | Reserved |
| 0b1110 | Vendor Specific |
| 0b1111 | no cipher suite selected |

The FD RSN Indications field contains two 4-bit AKM Suite Selectors. Each 4-bit Cipher Suite selector is a 4-bit code identifying a AKM Suite Type as specified in Table 8-101. The definition of the 4-bit AKM Suite Selectors is shown in Table 8-ai-4.

**Table 8-ai-4 AKM Suite Selector Definitions**

|  |  |
| --- | --- |
| **AKM Suite Selector (4 bits)** | **AKM Suite Type** |
| 0b0000 – 0b1001 | Cipher Suite Type 0 to 9, in Table 8-101. |
| 0b1010 – 1101 | Reserved |
| 0b1110 | Vendor Specific |
| 0b1111 | no AKM suite selected |

The FD RSN Indications field contains three 1-bit subfields, including Pre-Authentication (bit 24), Management Frame Protection required (bit 25), and Management Frame Protection Capable (bit 26), which have the same definitions as in the RSN capabilities field as specified in Section 8.4.2.27.4.

The FD RSN Indications field also contains two 1-bit subfields to indicate the supported IP address types, including IPv4 Supported (bit 27) and IPv6 supported (bit 28). If the IPv4 Supported subfield is set to 1, it indicates the IPv4 address type is supported, otherwise it indicates IPv4 is not supported. If the IPv6 Supported subfield is set to 1, it indicates the IPv6 address type is supported, otherwise it indicates IPv6 is not supported.

# Straw-Polls and Motions

The following lists the draft straw-polls and motions that are intended to present to the TGai Group in next Face-to-Face meeting.

**Motion-1:**Accept the text proposed in Section 4 of this contribution (13/0272) as the resolution to Comments, CID 250 and CID 251, in TGai review comment database (13/0036r9).

Yes: \_\_\_\_\_\_\_\_\_\_\_\_; No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; Abstain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Move:

Second:

# References:

1. 11-12-0151-15-00ai-Proposed-Specification-Framework-Document.docx
2. IEEE Std 802.11 – 2012
3. IEEE Std 802.11ai/D0.4
4. 11-13-0036-09-00ai-tgai-draft-review-combined-comments