IEEE P802.11
Wireless LANs

|  |
| --- |
| LB204 Comment Resolutions for CID 6024 and 6956  |
| Date: 2015-01-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Xiaofei WANG | InterDigital Communications, Inc. |  |  | xiaofei.wang@interdigital.com |
| Joseph LEVY | InterDigital Communications, Inc. | 2 Huntington QuadrangleMelville, NY 11747 | +1.516.835.9353 (m) | joseph.levy@interdigital.com |

Abstract

This document provides proposed text changes to the draft as a result for comment resolutions for CID 6024 and 6956. These comments address Clauses 8 and 11. The baseline for this comment resolution document is 802.11ai Draft 3.1. (**Please note, modifications required for the resolution of CID 6956 are on top of those made in 11-15/0021r3, approved by Motion #183)**

**Red Lined Text Changes for the Proposed Resolutions:**

**CID 6024**

**Instructions for Editor: please modify the text of 11.11.2.2.1, from Line 40, Page 113 to Line 14 Page 114 with the following changes:**

**Step-1: AP requirements** [13/1510r2]

Upon reception of the Authentication frame, the AP shall do the following: [13/1510r2]

1. If Authentication frame includes a Finite Cyclic Group field, then the AP shall first determine whether the indicated finite cyclic group in the received FILS authentication frame is supported.
2. If the indicated finite cyclic group in the received FILS authentication frame is not supported, the AP shall respond with an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] and the Status set to 77 (Authentication is rejected because the offered finite cyclic group is not supported) and shall terminate the exchange.
3. If the indicated finite cyclic group in the received FILS authentication frame is supported or if PFS is not being used in this exchange, the AP shall check whether PMKSA caching is being attempted by the presence of the PMKID list element.
	1. If the PMKID list element is present, the AP checks whether any PMKSA identifier offered in the PMKID list matches an identifier for a cached PMKSA. If so, the AP selects a PMKID that matches and continues the FILS shared key authentication protocol using the PMK from the identified PMKSA.
	2. If a PMKID list element is not present or if no PMKSA identifier offered in the PMKID list matches any identifier for a cached PMKSA, the AP checks whether an EAP-Initiate/Re-Auth packet is included. If not, the AP shall respond with an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Status set to 53 (invalid PMKID) and shall terminate the exchange.
	3. If an EAP-Initiate/Re-Auth packet is included, the AP shall [14/052r2]extract the EAP-Initiate/Re-auth data from the FILS [CID 2873]wrapped data field (see 8.4.2.184 (FILS Wrapped Data element)) and shall forward it to the Authentication Server. When applicable, the AP communicates with the Authentication Server using the same protocols [CID 2715]it uses when authenticating with EAP. Suitable protocols include, but are not limited to, remote authentication dial-in user service RADIUS (as specified in IETF RFC 2863-2000) and Diameter (as specified in IETF RFC 6942-2013).[13/1510r2][CID 2729][14/0823r2]

If PFS is being used, the AP shall also generate an ephemeral private key and perform the group’s scalar-op (see 11.3.4.1 (General)) to produce its own ephemeral public key. The AP may delay the generation of its ephemeral public/private key pair until after receiving a response from the Authentication Server, if applicable[14/052r2]. [13/1510r2][CID 4076]The Authentication Server processes the EAP-Initiate/Re-auth packet as specified in IETF RFC6696 and returns an EAP-Finish/Re-auth packet to the AP. In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet. [13/1510r2][14/052r2]If the Authentication Server responds with a failure indication, then the AP shall produce an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field)) and the Status set to 15 (Authentication rejected because of challenge failure). In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet and processing continues. [14/0823r2]

**CID 6596**

**Instructions for Editor: please modify the text of 8.6.8.38, with the following changes (Please note, these modifications are on top of those made in 11-15/0021r3, approved by Motion #183.):**

* FILS Discovery frame format

The FILS Discovery frame uses Public Action frame format. The format of its Action field is shown in Table 8-308a (FILS Discovery frame format).

|  |
| --- |
| * FILS Discovery frame format
 |
| Order | Information | Notes |
| 1 | Category [14/1107r3] |  |
| 2 | Public Action [14/1107r3] |  |
| 3 | FILS Discovery Information field  | [CID 4617] |
| 4 | Reduced Neighbor Report element [CID 5133]  | Reduced Neighbor Report element is optionally present. |
| 5 | FILS Indication element | The FILS Indication element is optionally present.  |
| 6 | Vendor Specific element | One or more Vendor Specific elements are optionally present. |

[14/1107r3] [CID 6333]

The Category field indicates the public category specified in Table 8-54 (Category values). [14/0412r3][CID 4887]

The Public Action field indicates the value of the FILS Discovery frame, as specified in Table 8-292 (Public Action field values) in  8.6.8.1 (Public Action frames).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| The FILS Discovery Information field is shown in Figure 8-662a (FILS Discovery Information field format). |  |  |  |  |  |  |
|  | FILS Discovery Frame Control | SSID/ Short SSID [Motion 122] | AP’s Next TBTT Offset [Motion 122] | Length | FD Capability | Operating Class |
| Octets: | 2 | 1-32 | 1 | 0 or 1 | 0 or 2 | 0 or 1 |
|  |  |  |  |  |  |  |
|  [CIDs 4031, 4055, 4616, 4250] | AP Configuration Sequence Number | Access Network Options | Primary Channel | FD RSN Information | Channel Center Frequency Segment 1 |
| Octets: | 0 or 1 | 0 or 1 | 0 or 1 | 0 or 5 | 0 or 1 |
|  | * FILS Discovery Information field format [14/0412r3][CIDs 4804, 4617
 |

 [14/0412r3]

 [14/0412r3]

The format of the 2-octet FILS Discovery Frame Control field is shown in  8-662b (FILS Discovery Frame Control field format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0 B4 | B5 | B6 | B7 |
|  | SSID Length | CapabilityPresenceIndicator | Short SSID Indicator | AP-CSNPresenceIndicator |
| Bits: | 5 |  | 1 | 1 | 1 |
|  |  |  |  |  |  |  |  |
| [CID 4585] | B8 | B9 | B10 | B11[13/1043r1] | B12 B15 |
|  | ANOPresenceIndicator | CCFS-1 Presence Indicator [13/1534r0] | Primary Channel Presence Indicator | RSN Info Presence Indicator | Length Presence Indicator | Reserved(3 bits) |  |
| Bits: | 1 | 1 | 1 | 1 | 1 | 3 |
| * FILS Discovery Frame Control field format
 |

The SSID Length subfield of the FILS Discovery Frame Control Field indicates the length, in octets, of the SSID/Short SSID field in the FILS Discovery frame. The value of this field is equal to the length of the SSID/Short SSID field in octets minus 1. [13/1339r1][CID 4162, 4163, 4164] When the Short SSID Indicator subfield is equal to 1, the value of the SSID Length subfield is equal to 3 (the length of the Short SSID in octets minus 1).

A value of 1 for the Capability Presence Indicator subfield indicates that the FD Capability field is present in the FILS Discovery frame. A value of 0 indicates that the FD capability field is not present in the FILS Discovery frame. [13/1339r1][14/0412r3][CIDs 4056, 4641, 4166, 4165, 4645, 4648, 4646, 4651, 4647, 4644, 4650, 4649] [14/1107r3]

A value of 1 for the Short SSID Indicator subfield indicates that a Short SSID is contained in the SSID/Short SSID field of the FILS Discovery frame. A value of 0 indicates that a SSID is contained in the SSID/Short SSID field of the FILS Discovery frame.

A value of 1 for the AP-CSN Presence Indicator subfield indicates that the AP-CSN field is present in the FILS Discovery frame. A value of 0 indicates that the AP-CSN field is not present in the FILS Discovery frame. [13/1339r1][14/0412r3][14/1107r3]

A value of 1 for the ANO Presence Indicator subfield indicates that the ANO field is present in the FILS Discovery frame. A value of 0 indicates that the ANO field is not present in the FILS Discovery frame. [13/1339r1][14/0412r3][14/1107r3]

A value of 1 for the CCFS-1 (channel center frequency segment 1) Presence Indicator subfield indicates that the 1-octet Channel Center Frequency Segment 1 field is present in the FILS Discovery frame. A value of 0 indicates that Channel Center Frequency Segment 1 is not present. [13/1534r0][14/0412r3][CID 4167][14/1107r3]

A value of 1 for the Primary Channel Presence Indicator subfield indicates that the Primary Channel field and the Operating Class field are present in the FILS Discovery frame. A value of 0 indicates that the Primary Channel field and the Operating Class field are not present in the FILS Discovery frame.[14/1107r3][13/1339r1][14/0412r3]

A value of 1 for the RSN Information Presence Indicator subfield indicates that the FD RSN information field is present in the FILS Discovery frame. A value of 0 indicates that the FD RSN information field is not present in the FILS Discovery frame.

A value of 1 for the Length Presence Indicator subfield indicates that the Length field is present in the FILS Discovery frame. A value of 0 indicates that the Length field is not present in the FILS Discovery frame. [13/1043r1][14/0412r3][14/1107r3] [13/1043r1][14/0412r3][14/1107r3]

The SSID/Short SSID field is variable length between 1 and 32 octets. When the value of the Short SSID Indicator subfield is equal to 1, the SSID/Short SSID field contains the 4-byte Short SSID (see 8.4.2.169 (Reduced Neighbor Report)). Otherwise, the SSID/Short SSID field contains the SSID, of which the length is specified by the 5-bit SSID Length field in the FILS Discovery frame Control of the FILS Discovery frame (see 8.4.2.2 (SSID element)).

The AP’s Next TBTT Offset (ANTO) field indicates the time offset in number of TUs, rounded down to the closest TU, between the transmission of the FILS Discovery frame and the next TBTT of a targeted AP. [14/0412r3][CID 4621]

The Length field is 1 octet in length and indicates the length of the remaining fields in the FILS Discovery Information field in octets. Its value is variable. [14/0412r3]

The FD Capability field contains the information that advertises the capabilities of the STA transmitting the FILS Discovery frame. Its length is 2 octets. Its presence is indicated by the 1-bit Capability Presence Indicator subfield in the FILS Discovery frame Control being equal to 1. The format of the FD Capability field is shown in Figure 8-662c (FD Capability field format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0 | B1 | B2 B4 | B5 B7 |
| [14/1270r0] | ESS | Privacy | BSS Operating Channel Width [14/0834r3]  | Maximum Number of Spatial Streams [CID 4889] |
| Bits: | 1 | 1 |  | 3 | 3 |
|  |  |  |  |  |  |  |  |  |
|  | B8 | B9 | B10 B12 | B13 B15 |
|  | Reserved | Multiple BSSIDs Presence Indicator | Maximum PHY Type[14/0834r3]  | FILS Minimum Rate  |
| Bits: | 1 | 1 | 3 | 3 |
| * FD Capability field format [CID 4618]
 |

 [14/0412r3]

The subfields ESS and Privacy are interpreted as specified in 8.4.1.4 (Capability Information field). [13/1339r1]

[14/1270r0][Motion #136]The 3-bit BSS Operating Channel Width subfield indicates the BSS operating channel width of the transmitting AP, as defined in Table 8-308b (BSS Operating Channel Width).

|  |
| --- |
| * BSS Operating Channel Width [14/0834r3]
 |
| BSS Operating Channel Width Subfield (3 bits) | HR/DSSS, OFDM, ERP, HT or VHT BSS operating channel width | TVHT BSS operating channel width |
| 0 | 20 MHz or 22 MHz | TVHT\_W |
| 1 | 40 MHz | TVHT\_W+W |
| 2 | 80 MHz | TVHT\_2W |
| 3 | 160 MHz or 80+80 MHz | TVHT\_4W or TVHT\_2W+2W |
| 4 - 7 | Reserved | Reserved |

 [14/0834r3][14/1270r0]

NOTE—FILS is only supported in non-DMG infrastructure BSS. FILS is not supported in IBSS, PBSS, or MBSS. [CIDs 4881, 4006][CID 6294]

The 3-bit Maximum Number of Spatial Streams subfield is coded per Table 8-308c (Maximum Number of Spatial Streams).

|  |
| --- |
| * Maximum Number of Spatial Streams [14/0834r3]
 |
| Nss Subfield (3 bits) | Maximum Number of Spatial Streams |
| 0 | 1 |
| 1 | 2 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 to 8 |
| 5 - 7  | Reserved |

 [CID 4889] [14/0834r3]

The Multiple BSSIDs Presence Indicator subfield is 1 bit in length and is set to 1 to indicate that the Multiple BSSID element is present in the Beacon frame. It is set to 0 to indicate that the Multiple BSSID element is not present in the Beacon frames.

The 3-bit Maximum PHY Type subfield is defined as in Table 8-308d (Maximum PHY Type subfield).

|  |
| --- |
| * Maximum PHY Type subfield [14/0834r3]
 |
| Maximum PHY Type subfield (3 bits) | Maximum PHY Type [14/0834r3]  |
| 0 | HR/DSSS (See Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)) |
| 1 | ERP-OFDM (See Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification) and 19 (Extended Rate PHY (ERP) specification))  |
| 2 | HT (See Clause 20 (High Throughput (HT) PHY specification)) |
| 3 | VHT (See Clause 22 (Very High Throughput (VHT) PHY specification)) OrTVHT (See Clause 23 (Television Very High Throughput (TVHT) PHY specification ))[CID 4027] |
| 4 - 7 | Reserved |

 [14/0834r3]

The 3-bit FILS Minimum Rate subfield indicates the minimum rate to be used by the AP transmitting the FILS Discovery frame and by FILS STAs in subsequent transmissions between the AP and FILS STAs. [14/1107r3]Depending on the PHY Type of the received FILS Discovery frame sub, the FILS minimum rate is represented as a bit rate value or as an MCS value as shown in Table 8-308e (FILS Minimum Rate subfield). If an MCS value is provided, then the FILS Minimum Rate can be derived from the MCS value and the PHY Type in the FD Capability field.

|  |
| --- |
| * FILS Minimum Rate subfield
 |
| FILS Minimum Rate subfield (3 bits) | FILS Minimum Rate / MCS |
| If received FILS Discovery frame type is 0 (HR/DSSS)[14/0834r3] | If received FILS Discovery frame type is 1 (ERP-OFDM) | If received FILS Discovery frame type is 2 (HT) | If received FILS Discovery frame type is 3 (VHT or TVHT) |
| 0 | 1 Mbps | 6 Mbps | MCS 0 [CID 4888]  | MCS 0 |
| 1 | 2 Mbps | 9 Mbps | MCS 1 | MCS 1 |
| 2 | 5.5 Mbps | 12 Mbps | MCS 2 | MCS 2 |
| 3 | 11 Mbps | 18 Mbps | MCS 3 | MCS 3 |
| 4 | Reserved | 24 Mbps | MCS 4 | MCS 4 |
| 5 - 7 | Reserved | Reserved | Reserved | Reserved |

 [14/0834r3]

The Operating Class field is 1 octet in length. It specifies the operating class of the Primary Channel of the transmitting AP (see 8.4.1.36 (Operating Class)). [14/0412r3]

AP Configuration Sequence Number (AP-CSN) field format is defined in  8.4.2.178 (AP Configuration Sequence Number element). [14/0412r3][CIDs 4622, 4623, 4624 multiple places, , 4628, 4627, 4626, 4625]

Access Network Options (ANO) field format is specified in Figure 8-399 (Access Network Options field format) in 8.4.2.91 (Interworking element). [14/0412r3][CIDs 4026, 4624, , 4628, 4627, 4626, 4625]

Primary Channel field is present and set to the channel number of the primary channel (See 10.16.2 (Basic 20/40 MHz BSS functionality)) if the FILS Discovery frame is transmitted as a non-HT duplicate PPDU, otherwise the field is not present. [14/0412r3]

Channel Center Frequency Segment 1 field is present and set to the index of the channel center frequency of the frequency segment 1 for an 80+80 MHz VHT BSS, if the FILS Discovery frame is transmitted as a non-HT duplicate PPDUs at an 80+80 MHz channel bandwidth; otherwise the field is not present. [14/0412r3]

[14/0412r3][CIDs 4629, 4628, 4627, 4626, 4625]The FD RSN Information field contains the RSN information, including: RSN capability, an authentication suite selector, a pairwise cipher suite selector, a group data cipher suite selector, and a group management cipher suite selector. Its length is 5 bytes. Its format is defined in Figure 8-662d (Format of the FD RSN Information Field).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| [CID 4426] | B0 B15 | B16 B21 | B22 B27 | B28 B33 | B34 B39 |
|  | RSN Capability | Group Data Cipher Suite Selector | Group Mgmt Cipher Suite Selector | Pairwise Cipher Suite Selector | AKM Suite Selector |
| Bits: | 16 | 6 | 6 | 6 | 6 |
| * Format of the FD RSN Information Field [13/1043r1]
 |

 [13/1043r1]

The FD RSN information field contains a 2-octet RSN Capability subfield, as specified in Figure 8-217 (RSN Capabilities field format) in 8.4.2.24.4. (RSN capabilities).[13/1043r1]

The FD RSN information field also contains three 6-bit Cipher Suite Selectors, including one 6-bit Group Data Cipher Suite selector, one 6-bit Group Management Cipher Suite selector, and one 4-bit Pairwise Cipher Suite Selector. Each 6-bit Cipher Suite selector is a 6-bit code identifying a Cipher Suite Type as specified in Table 8-128 (Cipher suite selectors). The definition of the 6-bit Cipher Suite Selectors is shown in Table 8-308f (Cipher Suite Selector Definitions). [13/1043r1]

|  |
| --- |
| * Cipher Suite Selector Definitions [13/1043r1]
 |
| Cipher Suite Selector  | Cipher Suite Type |
| 0 - 13[CID 4885]  | Cipher Suite Type 0 to 13, in Table 8-138 (Cipher suite selectors) |
| 14-61 | Reserved |
| 62 | Vendor Specific |
| 63 | No cipher suite selected [CID 4884]  |

**References:**

1. **IEEE 802.11-14/1351r15, TGai LB204 comments on D3.0, Marc Emmelmann, November 2014**
2. **IEEE P802.11ai™/D3.1, November 2014**