IEEE P802.11
Wireless LANs

|  |
| --- |
| CID 1276 Protected AID Switch |
| Date: 2022-02-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| David Halasz | Morse Micro |  |  | dave.halasz@morsemicro.com |
| Dave Goodall | Morse Micro |  |  | dave@morsemicro.com |

Abstract

This document proposes comment resolutions for LB258 CID 1276.

*Discussion :*

CID 1276 is shown on the next page.

Submission 11-19-0114-05-000m-text-proposal-for-protecting-twt-action-frames.doc has changes for adding integrity protected versions of some S1G action frames. This submission builds on 802.11-19/114r5 to add integrity protection for S1G action frames including AID Switch Request and Response.

Proposed Resolution:

* CID 1276 : Revised. The comment is regarding AID switching. But there are other S1G Action frames. Resolution includes the remaining S1G Action frames. Incorporate the changes shown as “Proposed change” in this document.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 1276 | 10.2 | 2196 | 4 | S1G use of SID in PV1 is problematic in combination with the AID switching mechanism since SID is based on AID and the AID switching/assignment operations use unprotected AID Switch Request/Response frames (these are defined in Table 9-582 -- Unprotected S1G Action field values). While the CCMP AAD design protects the actual MAC address and as such, the integrity of the frames from that view point, it cannot prevent potential denial of service attacks where unprotected frames could be used to replace the SID(s) used to target the frames. As an example, an attacker could replace this mapping on the STA for another STA and whenever PV1 is used, the real recipient would not be receiving them. Such an easy to use mechanism for selectively dropping frames could be quite helpful for helping other attacks that would normally depend on a more complex man-in-the-middle style design intercepting and selectively forwarding frames. Unprotected AID changes could also result in denial of service against power saving mechanism in a similar manner since the TIM element bits would not be in sync between the AP and non-AP STAs if an attacker has changed them on one end using the unprotected mechanism. | Since AID switching is defined as an optional mechanism, the easiest solution here could be to disallow its use completely. If this mechanism is seen useful, a better approach would be to define a protected variants of the AID Switch Request/Response frames and allow only those protected variants to be used. |

*Proposed change : for clause 9.4.2.241*

|  |
| --- |
| * **Extended RSN Capabilities field**
 |
| **Bit** | **Information** | **Notes** |
| 0–3 | Field length | The length of the Extended RSN Capabilities field, in octets, minus 1, i.e., *n* – 1. |
| 4 | Protected TWT Operations Support | The STA sets the Protected TWT Operations Support field to 1 when dot11ProtectedTWTOperationsImplemented is true, and sets it to 0 otherwise. See 10.47.1 (TWT overview). |
| 5 | SAE hash-to-element | The STA supports directly hashing to obtain the PWE instead of looping. See 12.4.4.2.3 (Hash-to-element(#331) generation of the password element with ECC groups) and 12.4.4.3.3 (Direct generation of the password element with FFC groups). |
| 6(M34) | Reserved | Used by the Wi-Fi Alliance® [[1]](#footnote-1). |
| 7(11ba) | Protected WUR Frame Support | The STA sets the Protected WUR Frame Support field to 1 when dot11RSNAWURFrameProtectionActivated is true, and sets it to 0 otherwise.  |
| 11(11ay)(M34) | Protected Announce Support | The non-EDMG STA sets the Protected Announce Support field to 1 when dot11ProtectedAnnounceImplemented is true, and sets it to 0 otherwise. See 12.6.20 (Robust management frame selection procedure). |
| <ANA> | Extended S1G Action Protection | The STA sets the Extended S1G Action Protection field to 1 when dot11ExtendedS1GActionProtectionOperationsImplemented is true and sets it to 0 otherwise.  |
| (M34)8, 9, 10, 12, <ANA>– (8´*n* – 1) | Reserved |  |

*Proposed change : for clause 9.6.25.1*

|  |
| --- |
| * S1G Action field values
 |
| S1G Action field value | Description |
| 0 | Reachable Address Update |
| 1 | Relay Activation Request |
| 2 | Relay Activation Response |
| 3 | Header Compression Update |
| 4 | Protected TWT Setup |
| 5 | Protected TWT Teardown |
| 6 | Protected TWT Information |
| 7 | Protected AID Switch Request |
| 8 | Protected AID Switch Response |
| 9 | Protected Sync Control |
| 10 | Protected STA Information Announcement |
| 11 | Protected EDCA Parameter Set |
| 12 | Protected EL Operation |
| 13 | Protected Sectorized Group ID List |
| 14 | Protected Sector ID Feedback |
| 15–255 | Reserved |

*Proposed change : insert after clause 9.6.25.8*

9.6.25.9 Protected AID Switch Request frame format

The Protected AID Switch Request frame allows robust STA-STA communication of the same information that is conveyed in the AID Switch Request frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected AID Switch Request frame has the same format as the Action field of the unprotected AID Switch Request frame (see 9.6.24.2 (AID Switch Request frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.10 Protected AID Switch Response frame format

The Protected AID Switch Response frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the AID Switch Response frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected AID Switch Response frame has the same format as the Action field of the unprotected AID Switch Response frame (see 9.6.24.3 (AID Switch Response frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.11 Protected Sync Control frame format

The Protected Sync Control frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the Sync Control frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected Sync Control frame has the same format as the Action field of the unprotected Sync Control frame (see 9.6.24.4 (Sync Control frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.12 Protected STA Information Announcement frame format

The Protected STA Information Announcement frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the STA Information Announcement frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected STA Information Announcement frame has the same format as the Action field of the unprotected STA Information Announcement frame (see 9.6.24.5 (STA Information Announcement frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.13 Protected EDCA Parameter Set frame format

The Protected EDCA Parameter Set frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the EDCA Parameter Set frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected EDCA Parameter Set frame has the same format as the Action field of the unprotected EDCA Parameter Set frame (see 9.6.24.6 (EDCA Parameter Set frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.14 Protected EL Operation frame format

The Protected EL Operation frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the EL Operation frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected EL Operation frame has the same format as the Action field of the unprotected EL Operation frame (see 9.6.24.7 (EL Operation frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.15 Protected Sectorized Group ID List frame format

The Protected Sectorized Group ID List frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the Sectorized Group ID List frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected Sectorized Group ID List frame has the same format as the Action field of the unprotected Sectorized Group ID List frame (see 9.6.24.10 (Sectorized Group ID List frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

9.6.25.16 Protected Sector ID Feedback frame format

The Protected Sector ID Feedback frame is an Action frame of category S1G and is defined to allow robust STA-STA communication of the same information that is conveyed in the Sector ID Feedback frame that is not robust (see 9.6.24.1 (Unprotected S1G Action field)).

The Action field of the Protected Sector ID Feedback frame has the same format as the Action field of the unprotected Sector ID Feedback frame (see 9.6.24.11 (Sector ID Feedback frame format)), except that the Order 2 item is the S1G Action field, which is defined in 9.6.25.1 (S1G Action field), instead of the Unprotected S1G Action field.

*Proposed change : insert after the first paragraph of clause 10.20*

When performing the S1G dynamic AID operations described in 10.20 (S1G dynamic AID assignment), if management frame protection is negotiated and both STAs set the Extended S1G Action Protection field in the RSNXE that they transmit to 1, the STAs shall

— use individually addressed Protected AID Switch Request, Protected AID Switch Response and Protected Information Announcement frames instead of AID Switch Request, AID Switch Response and STA Information Announcement frames, respectively and

— discard any individually addressed AID Switch Request, AID Switch Response or STA Information Announcement frame received from the peer STA, with which management frame protection is negotiated.

STAs that exchange individually addressed Protected AID Switch Request, Protected AID Switch Response or Protected STA Information Announcement frames shall follow the rules defined in 12.6.19 (Protection of robust Management frames).

When management frame protection is not negotiated or the Extended S1G Action Protection field in the RSNXE transmitted by either STA is set to 0, the STAs shall not use the Protected AID Switch Request, Protected AID Switch Response nor the Protected STA Information Announcement frame.

*Proposed change : insert after the first paragraph of clause 10.49*

When performing the Sync frame operation described in 10.49 (Sync frame operation), if management frame protection is negotiated and both STAs set the Extended S1G Action Protection field in the RSNXE that they transmit to 1, the STAs shall

— use individually addressed Protected Sync Control frames instead of Sync Control frames and

— discard any individually addressed Sync Control frames received from the peer STA, with which management frame protection is negotiated.

STAs that exchange individually addressed Protected Sync Control frames shall follow the rules defined in 12.6.19 (Protection of robust Management frames).

When management frame protection is not negotiated or the Extended S1G Action Protection field in the RSNXE transmitted by either STA is set to 0, the STAs shall not use the Protected Sync Control frame.

*Proposed change : for clause 11.46*

An EL STA receiving MLME-ELOPERATION.request primitive shall include an EL Operation element in Probe Request, TDLS Setup Request, TDLS Setup Response, and (Re)Association Request frames and may send EL Operation or Protected EL Operation frames.

When supporting energy limited STA operation described in 11.46 (Support for energy limited STAs), if management frame protection is negotiated and both STAs set the Extended S1G Action Protection field in the RSNXE that they transmit to 1, the STAs shall

— use individually addressed Protected EL Operation frames instead of EL Operation frames and

— discard any individually addressed EL Operation frames received from the peer STA, with which management frame protection is negotiated.

STAs that exchange individually addressed Protected EL Operation frames shall follow the rules defined in 12.6.19 (Protection of robust Management frames).

When management frame protection is not negotiated or the Extended S1G Action Protection field in the RSNXE transmitted by either STA is set to 0, the STAs shall not use the Protected EL Operation frame.

*Proposed change : insert at the end of clause 10.53.2*

When performing the Sectorized beam operation described in 10.53 (Sectorized beam operation), if management frame protection is negotiated and both STAs set the Extended S1G Action Protection field in the RSNXE that they transmit to 1, the STAs shall

— use individually addressed Protected Sectorized Group ID List and Protected Sector ID Feedback frames instead of Sectorized Group ID List and Sector ID Feedback frames, respectively and

— discard any individually addressed Sectorized Group ID List or Sector ID Feedback frame received from the peer STA, with which management frame protection is negotiated.

STAs that exchange individually addressed Protected Sectorized Group ID List or Protected Sector ID Feedback frames shall follow the rules defined in 12.6.19 (Protection of robust Management frames).

When management frame protection is not negotiated or the Extended S1G Action Protection field in the RSNXE transmitted by either STA is set to 0, the STAs shall not use the Protected Sectorized Group ID List nor the Protected Sector ID Feedback frame.

*Proposed change : insert text into clause 10.2.3.2*

The S1G AP may set the STA Type subfield of EDCA Parameter Set elements to any value that is less than 3 if it indicates support for both sensor STAs and non-sensor STAs as described in 10.61 (S1G flow control).

When an S1G AP assigns EDCA Parameters, if management frame protection is negotiated and both STAs set the Extended S1G Action Protection field in the RSNXE that they transmit to 1, the STAs shall

— use individually addressed Protected EDCA Parameter Set frames instead EDCA Parameter Set frames and

— discard any individually addressed EDCA Parameter Set frame received from the peer STA, with which management frame protection is negotiated.

STAs that exchange individually addressed Protected EDCA Parameter Set frames shall follow the rules defined in 12.6.19 (Protection of robust Management frames).

When management frame protection is not negotiated or the Extended S1G Action Protection field in the RSNXE transmitted by either STA is set to 0, the STAs shall not use the Protected EDCA Parameter Set frame.

An S1G AP may assign to an S1G STA EDCA parameters different from the ones in dot11EDCATable, by sending to the STA an EDCA Parameter Set frame with an EDCA Parameter Set element with the Override field equal to 1. An S1G STA receiving an EDCA Parameter Set element with the Override field equal to 1 shall update its MIB values of the EDCA parameters based on the values indicated by the EDCA Parameter Set element.

*Proposed change : for annex B, FT48*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FT48 | S1G Action frame | 9.6.25 (S1G Action frame details) | (RL1 OR S1GM6.13 OR S1GM30 ):M | Yes o No o N/A o |
| FT48.1 | Reachable Address Update frame | 9.6.25 (S1G Action frame details) | RL1:M | Yes o No o N/A o |
| FT48.2 | Relay Activation Request frame |  | RL1:O | Yes o No o N/A o |
| FT48.3 | Relay Activation Response frame |  | RL1:M | Yes o No o N/A o |
| FT48.4 | Protected TWT Setup frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FT48.5 | Protected TWT Teardown frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FT48.6 | Protected TWT Information frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FT48.7 | Protected AID Switch Request frame | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.8 | Protected AID Switch Response frame | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.9 | Protected Sync Control | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.10 | Protected STA Information Announcement | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.11 | Protected EDCA Parameter Set | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.12 | Protected EL Operation | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.13 | Protected Sectorized Group ID List | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FT48.14 | Protected Sector ID Feedback | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |

*Proposed change : for annex B, FR49*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FR49 | S1G Action frame | 9.6.25 (S1G Action frame details) | (CFAP AND CFS1G):O | Yes o No o N/A o |
| FR49.1 | Reachable Address Update frame | 9.6.25 (S1G Action frame details) | RL1:M | Yes o No o N/A o |
| FR49.2 | Relay Activation Request frame | 9.6.25 (S1G Action frame details) | RL1:M | Yes o No o N/A o |
| FR49.3 | Relay Activation Response frame | 9.6.25 (S1G Action frame details) | RL1:M | Yes o No o N/A o |
| FR49.4 | Protected TWT Setup frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FR49.5 | Protected TWT Teardown frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FR49.6 | Protected TWT Information frame | 9.6.25 (S1G Action frame details) | S1GM6.13:M | Yes o No o N/A o |
| FR49.7 | Protected AID Switch Request frame | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.8 | Protected AID Switch Response frame | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.9 | Protected Sync Control | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.10 | Protected STA Information Announcement | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.11 | Protected EDCA Parameter Set | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.12 | Protected EL Operation | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.13 | Protected Sectorized Group ID List | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |
| FR49.14 | Protected Sector ID Feedback | 9.6.25 (S1G Action frame details) | S1GM30:M | Yes o No o N/A o |

*Proposed change : for annex B, insert the following after S1GM29*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \*S1GM30 | Extended S1G Action Protection | 9.4.2.241 (RSN Extension element (RSNXE)) | CFS1G:O | Yes o No o N/A o |

*Proposed change : for annex C*

Dot11S1GStationConfigEntry ::=

 SEQUENCE {

 …,

 dot11S1GDACTImax Unsigned32,

 dot11ProtectedTWTOperationsImplemented TruthValue,

 dot11ExtendedS1GActionProtectionOperationsImplemented TruthValue

 }

dot11ExtendedS1GActionProtectionOperationsImplemented OBJECT-TYPE

 SYNTAX TruthValue

 MAX-ACCESS read-only

 STATUS current

 DESCRIPTION

 "This is a capability variable.

 Its value is determined by device capabilities.

 This attribute indicates whether the entity is capable of extended S1G action protection."

 ::= { dot11S1GStationConfigEntry <ANA> }

*Proposed additional change : for annex C*

dot11S1GComplianceGroup OBJECT-GROUP

 OBJECTS {

 …,

 dot11S1GDACTImax,

 dot11ProtectedTWTOperationsImplemented,

 dot11ExtendedS1GActionProtectionOperationsImplemented }

 STATUS current

**References:**

1. [↑](#footnote-ref-1)