IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution for SPP A-MSDU Support  |
| Date: 2022-03-01 |
| Author: |
| Name | Affiliation | Address | Phone | Email |
| Emily Qi | Intel  |  |  | Emily.h.qi@intel.com |
| Johnanes Berg | Intel  |  |  | johannes.berg@intel.com |
| Ido Ouzieli | Intel |  |  | ido.ouzieli@intel.com |
| Mark Rison | Samesung |  |  | m.rison@samsung.com |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
| Mark Himilton | Ruckus/CommScope |  |  | mark.hamilton2152@gmail.com |
|  |  |  |  |  |

Abstract

This contribution addresses the issue of how SPP A-MSDU could be negotiated without causing interoperability issues with misbehaving deployed STAs.

##### The proposed changes are based on REVme D1.0.

##### Revision history:

##### R0 – initial version

R1

**Discussion:**

[https](https://protect2.fireeye.com/v1/url?k=a0f52ae9-ff6e13af-a0f4a1a6-0cc47a3003e8-b69def78add67d87&q=1&e=cb3b5a5e-a2a1-4c7e-94b1-581dc55814fc&u=https%3A%2F%2Fpapers.mathyvanhoef.com%2Fusenix2021.pdf)[://papers.mathyvanhoef.com/usenix2021.pdf](https://protect2.fireeye.com/v1/url?k=68ac9564-3737ac22-68ad1e2b-0cc47a3003e8-7b2ff43b976c80bf&q=1&e=cb3b5a5e-a2a1-4c7e-94b1-581dc55814fc&u=https%3A%2F%2Fpapers.mathyvanhoef.com%2Fusenix2021.pdf) has identified the issue of supporting SPP A-MSDU, see:

*By default the A-MSDU flag, which informs a receiver how to parse the encrypted payload of a frame, is not authenticated (recall Section 2.1). Only when the sender and receiver support Signaling and Payload Protected (SPP) A-MSDUs is the A-MSDU flag authenticated [33, §11.17]. However, none of the devices we tested support this feature, meaning in practice the A-MSDU flag is never authenticated. This is problematic because nearly all devices we tested do support receiving A-MSDUs, meaning they can be tricked into processing normal frames as A-MSDUs, and vice versa.*

In IEEE 802.11-2020, two bits are defined in the RSN Capabilies field:

— Bit 10: **SPP A-MSDU Capable**. A STA sets the SPP A-MSDU Capable subfield of the RSN
Capabilities field to 1 to signal that it supports signaling and payload protected A-MSDUs (SPP
A-MSDUs) (see 10.11 (A-MSDU operation)). Otherwise, this subfield is set to 0.

— Bit 11: **SPP A-MSDU Required.** A STA sets the SPP A-MSDU Required subfield of the RSN Capabilities field to 1 when it allows only SPP A-MSDUs (i.e., does not send or receive payload protected A-MSDUs (PP A-MSDUs) (see 10.11 (A-MSDU operation)). Otherwise, this subfield is
set to 0.

However, the SPP A-MSDU STA behaviors haven’t been implemented or implemented incorrectly. Some implementations copy the bits from the AP’s RSNE, and hence would falsely signal support.

Also, the mandatory A-MSDU STA behaviors defined in Table 10-13 (A-MSDU STA behavior for RSN associations) are impossible for STA to be compliant. For example, in the second row of Table 10-13, a legacy STA (i.e. STA1 with both SPP A-MSDU capble and SPP A-MSDU required equal to 0) cannot understand STA2’s SPP A-MSDU required bit and STA 1 cannot obey the rules: “Shall not transmit PP A-MSDU” and “Shall discard received (PP and SPP) A-MSDU”.

This submission proposes an alternative mechanism for negotiating support for SPP A-MSDU. A new bit “SPP A-MSDU Capable” is defined in the Extended RSN Capabilities field of the RSNX element similarly to what was done with PBAC (See 22/0082r2, CID 1002).

For mandating SPP A-MSDU, it could be done with a single bit (“SPP A-MSDU Capable”) and a shall statement saying something like <the next great PHY name> STA shall indicate SPP A-MSDU Capable = 1 and leave this to the new PHY capable things rather than a BSS-specific property for all STAs.

Note that the “SPP A-MSDU Capable” bit is only for HT STA (non-DMG STA). DMG STAs always use SPP A-MSDU.



**Proposed resolution:**

***TGm editor: make changes to 9.4.2.24.4 as follows:***

* RSN capabilities

***TGm editor: in Figure 9-350, change bit 10 (B10) from “SPP A‑MSDU Capable” to “Reserved”***

***TGm editor: in Figure 9-350, change bit 11 (B11) from “SPP A‑MSDU Required” to “Reserved”***

… …

***TGm editor: make changes to following bullets as shown below:***

* Bit 10: Reserved. ~~SPP A‑MSDU Capable. A STA sets the SPP A‑MSDU Capable subfield of the RSN Capabilities field to 1 to signal that it supports signaling and payload protected A‑MSDUs (SPP A‑MSDUs) (see 10.11 (A‑MSDU operation)). Otherwise, this subfield is set to 0.~~

Bit 11: Reserved. ~~SPP A‑MSDU Required. A STA sets the SPP A‑MSDU Required subfield of the RSN Capabilities field to 1 when it allows only SPP A‑MSDUs (i.e., does not send or receive payload protected A‑MSDUs (PP A‑MSDUs) (see 10.11 (A‑MSDU operation)). Otherwise, this subfield is set to 0.~~

… …

***TGm editor: please deprecate MIB variable dot11SPPAMSDURequired with the procedure described in Editorial Style Guide, see doc 11-09-1034.***

* RSN Extension element (RSNXE)

***TGm editor: Please insert a new row to Table 9-363 as shown below and accordingly update the content of the last row corresponding to ‘Reserved’ values:***

|  |
| --- |
| * Extended RSN Capabilities field
 |
| Bit | Information | Notes |
| <ANA> | SPP A‑MSDU Capable | A non-DMG STA sets the SPP A‑MSDU Capable subfield to 1 if dot11SPPAMSDUCapable is true. Otherwise, this subfield is set to 0. See 10.11 (A‑MSDU operation).  |

* A‑MSDU operation

***TGm editor: Please update 10.11 as shown follows: (starting at 2180.52 of D1.0)***

… …

~~When dot11RSNAActivated is true, a~~ A non-DMG STA indicates support for payload protected A‑MSDUs (PP A‑MSDUs) or signaling and payload protected A‑MSDUs (SPP A‑MSDUs), when dot11RSNAActivated is true, in its RSNXE. ~~during~~ ~~(re)association.~~ ~~On either (re)association,~~ ~~the~~ ~~associating~~ A non-DMG STA and its peer STA both determine and maintain a record of whether an encrypted A‑MSDU sent to its peer is to be a PP A‑MSDU or an SPP A‑MSDU based on the SPP A‑MSDU Capable~~and SPP A‑MSDU Required~~ subfield~~s~~ of the Extended RSN Capabilities field of the ~~RSNE (see 9.4.2.24.4 (RSN capabilities))~~ RSNXE (see 9.4.2.241 (RSN Extension element (RSNXE))). If a STA and its peer STA are DMG STAs or both have their SPP A-MSDU Capable subfields equal to 1, A‑MSDUs shall be transmitted as SPP A-MSDUs. Otherwise, A‑MSDUs shall be transmitted as PP A-MSDUs.

~~Table 10-13 (A‑MSDU STA behavior for RSN associations) defines behavior related to the transmission and reception of individually addressed A‑MSDUs of a first HT STA or S1G STA (STA1) that has successfully negotiated an RSNA (re)association with a second HT STA or S1G STA (STA2).~~ Reception and transmission of A‑MSDUs using a non-RSN association is unaffected by the value~~s~~ of the SPP A‑MSDU Capable subfield. ~~and SPP A‑MSDU Required subfields.~~

***TGm editor: Please delete Table 10-13 A‑MSDU STA behavior for RSN associations.***

* Construct AAD

***TGm editor: Please update 12.5.3.3.3 as shown follows: (starting at 3146.7 of D1.0)***

* (#217)QC – QoS Control field contains the MSDU priority, if present. The QC TID is used in the construction of the AAD. When in a non-DMG BSS, if both the STA and its peer have their SPP A-MSDU Capable subfields (see 9.4.2.241 (RSN Extension element (RSNXE))) equal to 1, the A-MSDU Present field is also used in the construction of the AAD. When in a DMG BSS, the A-MSDU Present field and A-MSDU Type field are also used in the construction of the AAD. The remaining QC fields are not used and are masked to 0 for the AAD calculation (for a non-DMG BSS, bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0; for a DMG BSS, bits 4 to 6 and bits 9 to 15). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDU Type bit 8 are used in the construction of the AAD, and the remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 9 to 15).