### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11be D0.3 CR for 12.4 | | | | |
| Date: 2021-02-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation | 2200 Mission College Blvd, Santa Clara, CA 950542200 |  | po-kai.huang@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

2864, 2284, 2285, 2286, 2487, 2576, Mark’s comments

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Editorial revision.
* Rev 2: Further revision based on the received feedback.
* Rev 3: Editorial revision based on comments received offline.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbe D0.3 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D0.3 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **P.L** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 2864 | Stephen McCann | 112.30 | 12.4.1 | An "AP STA" is an "AP". | Change all occurances of "AP STA" to "AP". | Revised –  The cited texts are in the baseline, but ok to revise since this is an editorial revision.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2864 |
| 2284 | Michael Montemurro | 113.32 | 12.4.3 | This should just be MLD AP since that is the identity of the Authenticator. | Change "AP or APs affiliated with the AP MLD, respectively," to "AP MLD" | Revised –  The referered sentence is about the setting of “the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element”, which is an element sent by the APs of the AP MLD. However, given the number of comments on the paragraph, we separate the description to another paragraph for clarity and emphasize that dot11RSNAConfigPasswordValueTable is maintained by the MLD.  We also clarify that each AP affiliated with the AP MLD will have the same dot11RSNAConfigPasswordValueTable, so that there is no ambiguity on how this work for AP MLD.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2284 |
| 2285 | Michael Montemurro | 113.32 | 12.4.3 | I hope for MLD operations that with MLDs this is still a BSS. | Delete "or an AP MLD" | Revised –  BSS operation based on the baseline is defined as an STA that is synchronized with the AP, but it is understood that AP MLD may not have each affiliated APs synchronized and have the same clock, so we technically can not call an AP MLD an BSS.  However, given the number of comments on the paragraph, we separate the description to another paragraph for clarity.  We also clarify that each AP affiliated with the AP MLD will have the same dot11RSNAConfigPasswordValueTable, so that there is no ambiguity on how this work for AP MLD.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2284 |
| 2286 | Michael Montemurro | 113.32 | 12.4.3 | This should just be MLD AP since that is the identity of the Authenticator. | Replace "or Aps affiliated with the AP MLD" with "or AP MLD" | Revised –  The referered sentence is about the setting of “the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element”, which is an element sent by the APs of the AP MLD. However, given the number of comments on the paragraph, we separate the description to another paragraph for clarity.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2284 |
|  | Mark Rison | 113.32 | 12.4.3 | "32 In an infrastructure BSS or an AP MLD" -- A BSS and an MLD are not the same kind of thing. | delete and change “with the AP MLD, respectively,” to “with an AP MLD” | Revised –  Given the number of comments on the paragraph, we separate the description to another paragraph for clarity.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2284 |
| 2487 | Po-Kai Huang | 114.64 | 12.4.5.2 | The formula of val computation needs to be specified between two MLDs. Simply changing (STA-A-MAC, STA-B-MAC) to (MLD-A-MAC, MLD-B-MAC) for the formula between two MLDs | Changing (STA-A-MAC, STA-B-MAC) to (MLD-A-MAC, MLD-B-MAC) for the formula between two MLDs. | Revised –  We revise the texts toward that direction. The reason is that SAE is authenticate the owner of the password, which is identified by the MLD MAC address under MLD context. As a result, we can simply use MLD MAC address in the computation.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2487 |
| 2576 | Rojan Chitrakar | 114.63 | 12.4.5.2 | It is not apparent how the two MLDs find out each other's MLD MAC Addresses. Presumably, AP MLD would advertise its MLD MAC Address in Beacon/Probe Response frames and non-AP MLD would include its MLD MAC Address in the Authentication frame. However, can't find this information explicitely anywhere in D0.3. Clause 9 only mentions that ML element may be carried in Beacon/ Probe Response frames and Authentication frames but the content of ML element in these frames are not explained in clause 35. | Explain how the two MLDs would find out each other's MLD MAC Addresses for the PWE generation in SAE. | Rejected –  We clarify below that discovery of MLD address has been addressed in other places of the spec.  An authentication frame sent by a STA affiliated with an MLD includes an ML element that indicates the MLD MAC address of that MLD (see 35.3.5.4 Usage and rules of Basic variant Multi-link element in the context of multi-link setup). A Beacon frame sent by an AP affiliated with an AP MLD includes an ML element that indicates the MLD MAC address of that AP MLD, when that Beacon frame indicates SAE AKM (see 35.3.4.3 (Multi-link element usage rules in the context of discovery). A Probe Response frame sent by an AP affiliated with an AP MLD includes an ML element that indicates the MLD MAC address of the AP MLD in response to a MLD Probe Request frame (see 35.3.4 (Discovery of an AP MLD)). |
|  | Mark Rison | 114.63 | 12.4.5.2 | "between two STAs or MLD-A-MAC and MLD-B-MAC shall be used in the computation of val" is not clear | say MAC-A and MAC-B in the equation, and then in the “where” below describe how they map in the MLD and non-MLD cases | Revised –  We revise the texts toward that direction.  TGbe editor to make the changes shown in 11-21/0260r3 under all headings that include CID 2487 |

**Discussion:** *None.*

**Propose:**

***TGax editor: Change 12.4 Authentication using a password as follows (track change on):***

* Authentication using a password
* SAE overview

***Insert the following two paragraphs as the first two paragraphs of the subclause:***

In 12.4 (Authentication using a password), the reference of a “STA” means that the “STA” is not affiliated with an MLD unless specified otherwise.

In 12.4 (Authentication using a password), when referring to MLD authentication, the reference of “SME” means the entity that manages the MLD.

***Change the now-shifted third paragraph and split it into two paragraphs as follows:***

STAs, both APs (#2864) and non-AP STAs, may authenticate each other by proving possession of a password. MLDs, both AP MLDs and non-AP MLDs, may authenticate each other by proving possession of a password.

Authentication protocols that employ passwords need to be resistant to off-line dictionary attacks.

(…existing texts….)

***Change the now-shifted seventh paragraph as follows:***

The parties involved are called *STA-A* and *STA-B* between two STAs or called *MLD-A and MLD-B* between two MLDs. They are identified by their MAC addresses, STA-A‑MAC and STA-B-MAC, respectively, between two STAs or by their MLD MAC addresses MLD-A‑MAC and MLD-B-MAC, respectively, between two MLDs. STAs or MLDs begin the protocol when they discover a peer by receiving Beacon or Probe Response frame(s), or when they receive an Authentication frame indicating SAE authentication from a peer.

* Representation of a password

***Change as follows:***

Passwords are used in SAE to deterministically compute a secret element in the negotiated group, called a password element. The input to this process needs to be in the form of a binary string. For the protocol to successfully terminate, it is necessary for each side to produce identical binary strings for a given password, even if that password is in character format. There is no canonical binary representation of a character and ambiguity exists when the password is a character string. To eliminate this ambiguity, a STA or an MLD shall represent a character-based password as a UTF-8 string that is processed according to the OpaqueString profile of IETF RFC 8265, the output of which is an octet string. The octet string representation of the password, after being processed, is stored in the dot11RSNAConfigPasswordValueTable. When a “password” is called for in the description of SAE that follows the credential from the dot11RSNAConfigPasswordValueTable is used.

Similarly, to address ambiguity when identifying passwords, a STA or an MLD shall represent a password identifier as a UTF-8 string that is processed according to the UsernameCasePreserved profile of IETF RFC 8265, the output of which is an octet string that is stored in the dot11RSNAConfigPasswordValueTable. When a “password identifier” is called for in the description of SAE that follows, the identifier from the dot11RSNAConfigPasswordValueTable is used.

In an infrastructure BSS for which an SAE AKM is indicated, the AP shall set the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if any entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier, and shall set it to 0 otherwise. Similarly, an AP shall set the SAE Password Identifiers Used Exclusively subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if every entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier and shall set it to 0 otherwise. (#2284)

dot11RSNAConfigPasswordValueTable of each AP affiliated with an AP MLD shall be the same as the dot11RSNAConfigPasswordValueTable of an AP MLD. (#2284)

For an AP MLD that supports SAE AKM, each AP affiliated with the AP MLD shall indcate SAE AKM. (#2284)

Each AP affiliated with an AP MLD shall follow the same setting rule of an AP not affiliated with an AP MLD to set the value of the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element and the SAE Password Identifiers Used Exclusively subfield of the Extended Capabilities field of the Extended Capabilities element. (#2284)

(…existing texts….)

* SAE protocol
* PWE and secret generation

***Change the second paragraph as follows:***

When a STA or an MLD supports directly hashing to a group element (according to 12.4.4.2.3 (Hash-to-curve generation of the password element with ECC groups) or 12.4.4.3.3 (Direct Generation of the password element with FFC groups)) it computes a secret element, PT, offline at provisioning time for all groups it wishes to support with that password. Prior to initiating SAE to a STA or an MLD which also supports the direct form of hashing to a group element, or upon receipt of an SAE Commit message indicating it was generated using a direct form of hashing to a group element, it shall generate the PWE by hashing the two peer MAC addresses to produce a digest, reducing the digest modulo the order of the particular group, *r*, interpreting the reduced digest as an integer and using it with the secret element to generate the PWE:

*val = H(0n, MAX(A-MAC, B-MAC) || MIN(A-MAC, B-MAC))*

*(#2487) val = val* modulo *(r – 1) + 1*

*PWE = scalar-op(val, PT)*

where

* 0n is a salt of all zeros whose length equals the length of the digest from the hash function used to instantiate H() (see Table 12-1 (Hash algorithm based on length of prime)).
* *A-MAC* is the peer STA MAC address, *STA-A-MAC*, for SAE authentication between peer STAs, or is the peer MLD MAC address,  *MLD-A-MAC*,for SAE authentication between peer MLDs. *(#2487)*
* *B-MAC is the peer STA MAC address, STA-B-MAC, for SAE authentication between peer STAs, or is the peer MLD MAC address, MLD-B-MAC, for SAE authentication between peer MLDs. (#2487)*

(…existing texts….)