### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11ba D3.1 MAC Comment Resolution for Key ID of WUR Broadcast frame | | | | |
| Date: 2019-08-23 | | | | |
| 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 comments of TGba Draft D3.1 with the following CIDs:

3262, 3187

Revisions:

* Rev 0: Initial version of the document.

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 TGba D3.1 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGba D3.1 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **P.L** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 3262 | Po-Kai Huang | 80.7 | 9.10.3.2 | It is useful to indicate the key ID used for the protected broadcast addressed WUR wake-up frame so that during the transient period of Key update protected braodcast addressed WUR wake-up frame can still be processed by all releveant WUR non-AP STAs properly. | Use one bit in the Miscellaneous subfield to indicate the key ID used for the protected broadcast addressed WUR wake-up frame so that during the transient period of Key update protected braodcast addressed WUR wake-up frame can still be processed by all releveant WUR non-AP STAs properly. | Revised -  Agree in principle with the commenter.  TGba editor to make the changes shown in 11-19/1456r0 under all headings that include CID 3262. |
| 3187 | MARC EMMELMANN |  |  | When the key is WUR IGTK, WUR AP may only update some STAs to the new WUR IGTK with new key ID, and some STAs still use old WUR IGTK with old key ID. As a reuslt, the definition of current Key ID is different for different STAs | Picking up on comment 2330. The comment was invalidly rejected. The comment identified a specific technical issues that was not considered nor resolved in a previous letter ballot. The comment identifies a technical document (comment reslution spreadsheet of privious letter ballots) which included in depth instructions that can be immediately adopted to satisfy the comment.  It should also be noted, that during the process of comment resolution of the privious ballot, the TG choose again to discard comments without due discussion / consideration for the reason of going to recirculation (see minutes, stating: In order to address all comments, Po-Kai has collected the 16 CIDs that have not been addressed elsewhere. All are rejected, and large majority of the comments are rejected based on being invalid comments.)  It should also be noted that the TG choose for some comments which picked up on previous -- falsely rejcted comments -- to have a proper discussion and address the issues. So the reason for rejection does not hold.  Specifically, the rejectedc comment stated: Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.  The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised -  Agree in principle with the commenter. Key ID indication is now added in WUR broadcast and group addressed frame.  TGba editor to make the changes shown in 11-19/1456r0 under all headings that include CID 3187. |

**Discussion:** *None.*

**Propose:** Revised for CID 3262, 3187 per discussion and editing instructions in 11-19/1166r0.

***TGba editor: Change 9.10.3.2 WUR Wake-up frame format as follows:***

* WUR Wake-up frame format

(…exsiting texts…)

The Miscellaneous subfield is only present in the broadcast or group addressed FL WUR Wake-up frame. The format of Miscellaneous subfield is shown in Figure 9-993f (Miscellaneous subfield). The Miscellaneous subfield is reserved in FL WUR Wake-up frames that are neither broadcast addressed nor group addressed.

NOTE – A broadcast addressed WUR Wake-up frame is always a FL WUR Wake-up frame. (#3262, #3187)

|  |  |  |  |
| --- | --- | --- | --- |
|  | B0 | B1 | B2 |
|  | Group Addressed BU | Key ID | Reserved |
| Bits: | 1 | 1 | 1 |

* Miscellaneous subfield (#3262, #3187)

The Group Addressed BU subfield is set to 1 to indicate that one or more group addressed frames are buffered at the AP corresponding to the BSSID indicated in the ID field. Otherwise, the Group Addressed BU subfield is set to 0. The Group Addressed BU subfield is reserved in a group addressed FL WUR Wake-up frame. (#3262, #3187)

If the FL WUR Wake-up frame is broadcast addressed or group addressed, and the Protected subfield of the Frame Control field is set to 1, the Key ID subfield is set to 0 to indicate that the WIGTK identifier of the WIGTK used to compute the MIC is 8. If the Protected subfield of the Frame Control field is set to 1, the Key ID subfield is set to 1 to indicate that the WIGTK identifier of the WIGTK used to compute the MIC is 9. Otherwise, the Key ID subfield is reserved. (#3262, #3187)

(…exsiting texts…)

***TGba editor: Change 29.10 Protected WUR frames as follows:***

29.10 Protected WUR frames

(…exsiting texts…)

A WUR non-AP STA that installs the WTK (see 12.7.6 (4-way handshake)) shall use the WTK to process all subsequently received protected individually addressed WUR wake-up frames. A WUR non-AP STA shall identify the appropriate WIGTK and associated state based on the Key ID subfield of the received protected broadcast or group addressed FL WUR wake-up frames. If no such WIGTK exists, silently drop the frame and terminate BIP processing for this reception. A WUR non-AP STA shall use the lastest installed WIGTK to process all subsequently received protected group addressed VL WUR wake-up frame.

(#3262, #3187)

(…exsiting texts…)

**29.10.1 Protected WUR frame transmission**

A WUR AP that sends a protected WUR frame shall follow the rules in 12.5.4.5 (BIP transmission) except that the WUR AP shall:

—Select the appropriate integrity key associated to protected WUR frames (see 29.10 (Protected WUR frames)), Key ID that is equal to the corresponding WIGTK or WTK Key ID value, a WUR PN that is generated and partially included in the WUR frame as defined in 29.10.3.1 (Generation of the PN by a WUR AP). If the Miscellaneous subfield is present in the protected WUR Wake-up frame, the Key ID subfield is set to the value representing the corresponding WIGTK (see 9.10.3.2 (WUR Wake-up frame format)).(#3262, #3187)

—Construct the AAD as defined in Figure 29-2 (AAD construction for WUR frames).

—Compute an integrity value over the concatenation of AAD, the Frame Body field (if present), and the WUR PN, and insert the 16-bit truncated output, which is the MIC, into the FCS field of the WUR frame. The integrity value is computed using AES-128-CMAC.

—Transmit the protected WUR frame.

A WUR AP that sends a protected group addressed VL WUR wake-up frame should only include WUR ID(s) of the WUR non-AP STA(s) that have already been provided with the WIGTK used to protect the group addressed VL WUR wake-up frame. (#3262, #3187)

**29.10.3.1 Generation of the PN by a WUR AP**

A WUR AP that intends to transmit protected WUR frames shall set the Common PN subfield in the WUR Operation element it transmits to 0 if it intends to maintain separate PN counters for each WIGTK and WTK and shall set the Common PN subfield to 1 if it intends to maintain a common PN for all protected WUR frames generated within its BSS. (#3262, #3187)