IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for remaining Protected WUR frames CIDs |
| Date: 2019-09-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
| Lei Huang |  |  |  |
| Yoshio Urabe |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGba comment collection (TGba Draft 3.0).

* CIDs: 3179, 3191, 3188, 3278 (4 CIDs)

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Editorial changes based on feedback during presentation.
1. **Introduction**

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 Draft. The introduction and the explanation of the proposed changes are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGba 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 | Clause  | Page | Line | Comment | Proposed Change | Resolution |
| 3179 | MARC EMMELMANN |  |  |  | TSF timer based security protection mechanism can be used by all the WUR frames. however, PN based security protect mechanism can not be used by broadcast WUR wake up frame. | Picking up on comment 2317. 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 with the commenter that as of D3.0 PN based protection cannot be used to protect broadcast WUR wake up frames. PN based protection is added for broadcast WUR wake up frames. TGba editor to make the changes shown in 11-19/1644r1 under all headings that include CID 3179. |
| 3191 | MARC EMMELMANN |  |  |  | Evaluate if sending only 8 MSBs of the PPN is sufficient to protect broadcast WUR Wake Up frames. If it is possible then allow the TD Control to carry the 8 MSBs of the PPN when the frame is broadcast and protected. | Picking up on comment 2346. 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.**Even though only 8 bits of PPN is carried in broadcast WUR wake up frames, the remaining bits of the IPN are also used in the calculation of the MIC, so the security is not compromised. Note that only 8 bits are also sent in WUR waku-up frames when the TSF based protection is used. PN based protection is added for broadcast WUR wake up frames, however in order to simplify the IPN generation procedure, the bit order of the PPN carried in the WUR wake up frames is rearranged by swapping the Counter and sequence Number sub-fields of the Type Dependent Control field. TGba editor to make the changes shown in 11-19/1644r1 under all headings that include CID 3191. |
| 3188 | MARC EMMELMANN |  |  |  | It is not clear why counter of broadcast WUR wake-up frame is not protected. Could attacker send a forged broadcast WUR wakeup frame within 32 TUs after the original one and trigger all STAs to power up PCR? | Picking up on comment 2332. 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 with the commenter the counter field of broadcast WUR wake-up frames should also be protected. The counter subfield is included in the AAD field during the MIC computation. TGba editor to make the changes shown in 11-19/1644r1 under all headings that include CID 3188. |
| 3278 | Rojan Chitrakar | 29.103.2 | 125 | 25 | At the AP side, the PN is incremented by 1 for each transmitted WUR frame (Ref: P124L46), however there is no procedure defined for the increment of the locally store PN/BPN at the non-AP STA. When the PPN in a received WUR frame is lesser than the last received PPN, it indicates a PPN roll over and as such the local BPN should be incremented by 1 before constructing the local PN, else the PN used by the AP and the non-AP STA will not be the same. | Add one more bullet:The portion of the PN corresponding to the BPN shall be incremented by 1 when the PPN in the received WUR frame is less than the local PPN. | **Revised.**Agree with the commenter the PPN roll over case is currently not handled. Text is added to handle the case of PPN roll over. TGba editor to make the changes shown in 11-19/1644r1 under all headings that include CID 3278. |

**Discussion:** None

**Propose:**

Revised for CIDs 3179, 3191, 3188, 3278 as per discussion and editing instructions in 11-19/1644r1.

* WUR Wake-up frame format (CIDs 3179, 3191)

***TGba editor: Modify the section as the following (Track Changes ON):***

The frame format of the WUR Wake-up frame is defined in Figure 9-993a (WUR frame format).

The Frame Control field is defined in 9.10.2.1.1 (Frame Control field).

The Length Present subfield is set to 1 if the Frame Body field is present and is set to 0 otherwise.

The ID field of the FL WUR Wake-up frame contains one of the following:

* The WUR ID when the frame is individually addressed to a WUR non-AP STA (see 29.5.5 (WUR ID)).
* The WUR group ID when the frame is group addressed to all WUR non-AP STAs belonging to the group identified by the WUR group ID (see 29.5.4 (WUR Group ID)).
* The transmitter ID when the frame is a broadcast addressed frame transmitted by the WUR AP identified by the transmitter ID (see 29.5.3 (Transmitter ID)).
* The nontransmitter ID when the frame is a broadcast addressed frame transmitted by the WUR AP identified by the nontransmitted ID when dot11MultiBSSIDImplemented is true (see 29.5.6 (Nontransmitter ID)).

The ID field of the VL WUR Wake-up frame contains a WUR group ID when the frame is group addressed to one or more WUR non-AP STAs that are identified by the WUR IDs included in the Frame Body field and belong to the group identified by the WUR group ID (see 29.5.4 (WUR Group ID)).(#3197)

The Type Dependent Control field of a WUR Wake-up frame contains the Sequence Number subfield and the Counter subfield as defined in 9-993e (Type Dependent Control field of WUR Wake-up frame).

|  |  |  |
| --- | --- | --- |
|  | B0             B7 | B8                   B11 |
|  |  Sequence Number | Counter |
| Bits: | 8 | 4 |
| * Type Dependent Control field of WUR Wake-up frame
 |

The Counter subfield:

* Contains the BSS Update Counter field if the WUR Wake-up frame is broadcast addressed. The BSS Update Counter field is defined as an unsigned integer initialized to 0 that incre-ments when a critical update to the BSS parameters has occurred (see 29.9.2 (WUR AP operation)), or
* Contains PN1[0:3](see 31.8 (Protected WUR frames)) if the WUR Wake-up frame is not broadcast addressed, the Protected subfield in the Frame Control field is 1, and the most recently sent WUR Operation element has the Common PN subfield equal to 0, or
* Is reserved otherwise.

The Sequence Number subfield:

* Contains the TSF timer [9: 16] if the Protected subfield in the Frame Control field is 1 and the most recently sent WUR Operation element has the Common PN subfield equal to 1 (see 29.10.3.1 (Generation of the PN by a WUR AP)), or
* Contains PN0 (see 29.10 (Protected WUR frames)) if the Protected subfield in the Frame Control field is 1, and the most recently sent WUR Operation element has the Common PN subfield equal to 0, or
* Is reserved otherwise.

***TGba editor: Move the description of the Sequence Number subfield in front of the description of the counter subfield to maintain the order:***

…

* Protected WUR frames (CIDs 3188)

***TGba editor: Modify the section as the following (Track Changes ON):***

…

The WUR AP shall protect the WUR Wake-up frame using the BIP protocol as defined in 12.5.4 (Broadcast/multicast integrity protocol (BIP)) except that:

* The WUR AP shall use BIP-CMAC-128 to provide data integrity and replay protection and shall use an integrity key to compute the MIC of the WUR Wake-up frame, which is defined below:
* Broadcast and group addressed WUR Wake-up frames shall be protected using a separate WIGTK that is negotiated as defined in 12.7.7 (Group key handshake)(#3275)
* Individually addressed WUR Wake-up frames shall be protected using a separate WTK that is negotiated as defined in 12.7.6 (4-way handshake).(#3276)
* The CMAC output for BIP-CMAC-128 shall be truncated to 16 bits: MIC = Truncate-16 (CMAC Output). The MIC shall be included in the FCS field of the protected WUR Wake-up frame.
* The AAD shall have a length of 40 bits consisting of the following:
* the Frame Control, and the ID field, which are obtained from the WUR Wake-up frame,
* the Counter field which is obtained from the Type Dependent Control field of the WUR Wake-up frame if it is broadcast addressed; otherwise it is reserved, and
* the Embedded BSSID field, which is equal to the 16 MSBs of the compressed BSSID (see 29.5.2 (Compressed BSSID)).
* The AAD is as shown in Figure 29-2 (AAD construction for WUR frames).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0          B7 | B8                B19 | B20             B23 | B24             B39 |
|  | Frame Control | ID | Counter | Embedded BSSID |
| Bits: | 8 | 12 | 4 | 16 |
| * AAD construction for WUR frames
 |

* + - 1. Generation of the PN by a WUR AP (CIDs 3179, 3191)

***TGba editor: Modify the section as the following (Track Changes ON):***

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 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.

The WUR AP that intends to transmit a protected WUR frame shall construct the PN as follows:

* If the Common PN subfield is equal to 1:
* PN = PN0||PN1||PN2||PN3||PN4||PN5 = TSF timer [9: 56], where the TSF timer is obtained as defined in 29.6.1 (General).
* The PN shall never repeat for protected WUR frames generated using the same WIGTK or WTK
* The WUR AP shall include PN0, i.e., the PPN, which is equal to its TSF timer [9: 16], in the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame
* If the Common PN subfield is equal to 0:
* PN = PN0||PN1||PN2||PN3||PN4||PN5, where PN shall be incremented by one for each transmitted WUR frame using the same WIGTK or WTK.
* The PN shall never repeat for protected WUR frames generated using the same WIGTK or WTK
* If the WUR Wake-up frame is not broadcast addressed:
* PPN = PN0||PN1[0:3]. The WUR AP shall include PN0 (i.e., the 8 LSBs of the PPN) in the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame. The AP shall include PN1[0:3] (i.e., the 4 MSBs of the PPN) in the Counter subfield of the Type Dependent field of the WUR Wake-up frame
* If the WUR Wake-up frame is broadcast addressed:
* PPN = PN0. The WUR AP shall include PN0 (i.e., the PPN) in the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame.

…

* + - 1. Construction of the PN by a WUR non-AP STA (CIDs 3179, 3191, 3278)

The full PN is not present in protected WUR frames, depending on (#Ed)the Common PN subfield of the most recently received WUR Operation element, and is constructed locally at the WUR non-AP STA as follows:

* If the Common PN subfield is equal to 1, the PN is obtained as follows:
* PN0 is set as the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame
* BPN is set as the value of bits 17 to 56 of the local TSF timer
* If the most significant bit (MSB) of the PN0 is not equal to the bit 16 of the local TSF timer then the value BPN shall be adjusted to account for roll over as follows:

— The value shall be increased by one unit (modulo 240) if LT[9:16] > PN0 and LT[9:16] > ((PN0 + 27) (modulo 28))

— The value shall be decreased by one unit (modulo 240) if LT[9:16] < PN0 and LT[9:16] < ((PN0 – 27) (modulo 28))

where LT[9:16] is the value of bits 9 to 16 of the local TSF timer

* The PN=PN0||BPN where PN1||PN2||PN3||PN4||PN5 = BPN
* If the Common PN subfield is equal to 0, the PN is obtained as follows:
* If the WUR Wake-up frame is not broadcast addressed:
* The PN is obtained as PPN||BPN, where PPN is equal to (#Ed)the Type Dependent Control field of the received WUR frame, and BPN is retrieved from the locally stored PN at the receiver for the corresponding WIGTK or WTK.
* PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN.
* If the WUR Wake-up frame is broadcast addressed:
* The PN is obtained as PPN||BPN, where the PPN is equal to the Sequence Number subfield of the Type Dependent Control field of the received WUR frame, and BPN is retrieved from the locally stored PN at the receiver for the corresponding WIGTK or WTK.
* PN0 = PPN, and PN1||PN2||PN3||PN4||PN5 = BPN.
* The portion of the computed PN corresponding to the BPN shall be incremented by 1 to account for roll over when the PPN in the received WUR frame is less than the portion of the locally stored PN corresponding to the PPN. (#3278)

…

…