IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment Resolution on clause 30.9.2 and 30.9.3 Protected WUR frames | | | | |
| Date: 2019-07-08 | | | | |
| 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 2.0).

* CIDs: 3206, 3258, 3265, 3266, 3267, 3268, 3269, 3270, 3271, 3272, 3279, 3280, 3281, 3282, 3283, 3284, 3389, 3275, 3276 (19 CIDs)

Revisions:

* Rev 0: Initial version of the document.

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 | Page | Line | Clause | Comment | Proposed Change | Resolution |
| 3206 | Massinissa Lalam | 70 | 61 | 9.4.2.300 | Where is defined "BPN"? | Please add BPN definition if not already present | **Rejected.**  The acryonym BPN stands for base packet number and is defined in the baseline (REVmd\_D2.0) |
| 3258 | Po-Kai Huang | 71 | 30 | 9.4.2.300 | This sentence seems to be redundant after the sentence in line 26. | Remove the sentence in line 30. | **Rejected.**  Although related, the the two sentences are describing two different subfields. Similar texts also exist for other subfields such as the WUR Group ID List subfield or the Recommended WUR Parameters subfield. |
| 3389 | Yunsong Yang | 71 | 1 | 9.4.2.300 | If the WUR Protection element only carries the BPN, not the entire WTK PN or WIGTK PN, it may result in a corner case where the BPNs are synchronized between the AP and STA, but the PPNs may be all "0" and all "1" at the AP and STA, respectively. And the next WUR Wake-up frame may cause the STA to carryover in its PPN and thus its BPN becomes BPN+1 and thus out of synch with the AP again. The element is transmitted using the main radio. Why not just carry the entire PN to avoid such corner case? | Change the BPN field in Figure 9-776p to a 6-octet PN field. And change the description associated with this field throughout the draft accordingly. | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. Since the difference between PN and BPN is only 1 octet, the increase in overhead is minimal.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3389. |
| 3265 | Rojan Chitrakar | 70 | 59 | 9.4.32.300 | The WUR Protection element is used solely for the purpose of updating the BPN. Also, instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, it is better to rename this element as WUR PN Update element. | Replace all occurance of "WUR Protection" when used in context of the element name with "WUR PN Update" throughout the next revision of the 11ba draft | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. To align with the purpose of the element, WUR Protection element is renamed as WUR PN Update element.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3265. |
| 3266 | Rojan Chitrakar | 71 | 2 | 9.4.32.300 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, it is better to rename the BPN field as PN field. | Replace the BPN field as PN field in Figure 9-776p and throughout the next revision of the 11ba draft. Also change the octets of the field to "0 or 6". | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The BPN field is renamed as PN field.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3266. |
| 3267 | Rojan Chitrakar | 71 | 15 | 9.4.32.300 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, it is better to rename the BPN Present field as PN Present field. | Replace the BPN Present field as PN Present field in Figure 9-776q and throughout the next revision of the 11ba draft. | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The BPN Present field is renamed as PN Present field.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3267. |
| 3268 | Rojan Chitrakar | 71 | 23 | 9.4.32.300 | WUR TK and WUR IGTK are no longer used in 11ba draft | Change the sentence to: "The Key ID subfield contains the Key ID corresponding to the WTK or WIGTK." | **Accepted.** |
| 3269 | Rojan Chitrakar | 71 | 37 | 9.4.32.300 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, the BPN field should carry the entire 6 octets of the PN. | Replace the BPN field as PN field in Figure 9-776r and modify the figure by adding one the PN0 field such that B0 - B7 carry the PN0 and B40 - B 47 carry the PN6. | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The BPN field is renamed as PN field and PN0 is added to the figure.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3269. |
| 3270 | Rojan Chitrakar | 71 | 47 | 9.4.32.300 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, the BPN field should carry the entire 6 octets of the PN. | Modify the sentence as: "The PN field contains the PN corresponding to integrity key indicated by the Key ID subfield in the Key Info field." | **Accepted.** |
| 3271 | Rojan Chitrakar | 71 | 53 | 9.6.34.2 | The WUR Protection element is used solely for the purpose of updating the BPN. Also, instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, it is better to rename this field as WUR PN Update. | Replace the Information field as: WUR PN Update (optional) (see 9.4.2.300 (WUR PN Update element)) | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The WUR Protection field is renamed as WUR PN Update field.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3271. |
| 3272 | Rojan Chitrakar | 72 | 23 | 9.6.34.2 | The WUR Protection element is used solely for the purpose of updating the BPN. Also, instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. To align with the purpose, it is better to rename this field as WUR PN Update. | Modify the sentence as: The WUR PN Update field contains one or more WUR PN Update elements as defined in 9.4.2.294 (WUR PN Update element). | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The WUR Protection field is renamed as WUR PN Update field.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3272. |
| 3279 | Rojan Chitrakar | 125 | 46 | 29.103.2 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. | Change the sentence to: When the most recently received WUR Operation element has the Common PN subfield equal to 0, the WTPN or WIPN may be updated explicitly through a secure WUR Mode Setup request/response exchange as described in 29.10.3.3 (WUR PN update procedure). | **Accepted.** |
| 3280 | Rojan Chitrakar | 125 | 51 | 29.103.3 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. As such the the WUR BPN update procedure should be called WUR PN update procedure. | Change "BPN update" to: "PN update" throughout the next revision of the 11ba draft. | **Revised.**  Agree with the commenter that it is better to update the entire PN instead of just the BPN to prevent BPN mis-match due to rollovers. The WUR BPN Update procedure is renamed as WUR PN Update procedure.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3280. |
| 3281 | Rojan Chitrakar | 125 | 54 | 29.103.3 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. | Change the sentence to: The WUR PN Update procedure enables a WUR AP and a WUR non-AP with WUR frame protection negotiated with the WUR AP to update the locally stored PN at the WUR non-AP STA. | **Accepted.** |
| 3282 | Rojan Chitrakar | 125 | 58 | 29.103.3 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. | Revise the paragraph to state that the AP may indicate the entire PN maintained by the AP instead of the BPN. | **Revised.**  Agree with the commenter that AP may indicate the entire PN maintained by the AP instead of the BPN.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3282. |
| 3283 | Rojan Chitrakar | 125 | 64 | 29.103.3 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. | Revise the paragraph to state that the non-AP STA shall update the entire PN maintained by the STA instead of the BPN. | **Revised.**  Agree with the commenter that the non-AP STA shall update the entire PN maintained by the STA instead of the BPN.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3283. |
| 3284 | Rojan Chitrakar | 126 | 11 | 29.103.3 | Instead of just updating the 5 octets BPN, it would be better to update the entire 6 octet PN. | Revise the paragraph to state that the AP may indicate the entire PN maintained by the AP instead of the BPN. | **Revised.**  Agree with the commenter that AP may indicate the entire PN maintained by the AP instead of the BPN.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3284. |
| 3275 | Rojan Chitrakar | 122 | 22 | 29.1 | Replace "WUR integrity group temporal key (IGTK)" with WIGTK. | Replace "WUR integrity group temporal key (IGTK)" with WIGTK. | **Revised.**  Agree with the commenter that "WUR integrity group temporal key (IGTK)" should be replaced with WIGTK. In addition, the first occurance of WIGTK (4.10.3.2) is spelt out in full.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3275. |
| 3276 | Rojan Chitrakar | 122 | 25 | 29.1 | Replace "WUR temporal key (TK)" with WTK. | Replace "WUR temporal key (TK)" with WTK. | **Revised.**  Agree with the commenter that "WUR temporal key (TK)" should be replaced with WTK. In addition, the first occurance of WTK (4.10.3.2) is spelt out in full.    TGba editor to make the changes shown in 11-19/1069r0 under all headings that include CID 3276. |

**Discussion:** None

**Propose:**

Revised for CIDs 3389, 3265, 3266, 3267, 3269, 3271, 3272, 3280, 3282, 3283, 3284, 3275, 3276 as per discussion and editing instructions in 11-19/1069r0.

* IEEE Std 802.11 and IEEE Std 802.1X-2010 (CIDs 3275, 3276)
* Infrastructure functional model overview
* AKM operation with AS(#2318, #2334, #2421, #2333, #2335, #2336, #2578)

***Change the 2nd paragraphs as follows:***

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

A 4-way handshake or FT 4-way handshake utilizing EAPOL-Key frames is initiated by the Authenticator to do the following:

* Confirm that a live peer holds the PMK.
* Confirm that the PMK is current.
* In the case of fast BSS transition, derive PMK-R0s and PMK-R1s.
* Derive a fresh pairwise transient key (PTK) from the PMK or, in the case of fast BSS transition, from the PMK-R1, the derived PTK including the wake-up radio temporal key (WTK) if WUR frame protection is negotiated. (#3276)
* Install the pairwise encryption and integrity keys.
* Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
* If management frame protection is negotiated, transport the IGTK and the IGTK packet number (IPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP.
* If beacon protection is enabled, transport the BIGTK and the BIGTK packet number (BIPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP.
* If WUR frame protection is negotiated, transport the wake-up radio integrity group temporal key (WIGTK) and the WIGTK packet number (WIPN) from the Authenticator to the Supplicant and install these values in the STA and, if not already installed, in the AP. (#3275)
* Verify that the RSN capabilities negotiated are valid as defined in 9.4.2.24.4 (RSN capabilities).
* Confirm the cipher suite selection.
* Elements (CIDs 3265)
* General

***Insert the following new rows into Table 9-94 (Element IDs) (header row shown for convenience):***

***TGba editor: Modify Table 9-94 (Element IDs) as the following (Track Changes ON):***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * Element IDs | | | | |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| ... |  |  |  |  |
| WUR PN Update | 255 | 87 | Yes | No |

* WUR PN Update element (CIDs 3389, 3265, 3266, 3267, 3269)

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

The WUR PN Update element is used to update the PN maintained by a WUR non-AP STA. The format of the WUR PN Update element is shown in Figure 9-776p (WUR PN Update element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Key Info | PN |
| Octets: | 1 | 1 | 1 | 1 | 0 or 6 |
| * WUR PN Update element format | | | | | |

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Key Info field is 1 octets and is illustrated in Figure 9-776q (Key Info field format).

|  |  |  |  |
| --- | --- | --- | --- |
|  | B0            B3 | B4 | B5                   B7 |
|  | Key ID | PN Present | Reserved |
| Bits: | 4 | 1 | 3 |
| * Key Info field format | | | |

The Key ID subfield contains the Key ID corresponding to the WTK or WIGTK. (#3268)

The PN Present subfield is set to 1 if the PN field is present in the WUR PN Update element and is set to 0 otherwise.

The PN field in the WUR PN Update element is present if the PN Present subfield is set to 1. Otherwise, it is not present.

The PN field is 6 octets and is illustrated in Figure 9-776r (PN field format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0            B7 | | B8          B15 | B16          B23 | B24             B31 | B32             B39 | B40             B47 |
|  | PN0 | | PN1 | PN2 | PN3 | PN4 | PN5 |
| Bits: | 8 | | 8 | 8 | 8 | 8 | 8 |
|  | | * PN field format | | | | | |

The PN field contains the PN corresponding to the integrity key indicated by the Key ID subfield in the Key Info field.

* WUR Mode Setup frame format (CIDs 3265, 3271, 3272)

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

The WUR Mode Setup frame is an Action frame of category WUR. The Action field of a WUR Mode Setup frame contains the information shown in Table 9-524b (WUR Mode Setup frame Action field format).

|  |  |
| --- | --- |
| * WUR Mode Setup frame Action field format | |
| Order | Information |
| 1 | Category |
| 2 | WUR Action |
| 3 | Dialog Token |
| 4 | WUR Mode element (see 9.4.2.298 (WUR Mode element)) |
| 5 | WUR Operation element (optional) (see 9.4.2.297 (WUR Operation element)) |
| 6 | WUR PN Update (optional) (see 9.4.2.300 (WUR PN Update element))(#2589, #2314) |

...

The WUR PN Update field contains one or more WUR PN Update elements as defined in 9.4.2.300 (WUR PN Update element).

* Protected WUR frames (CIDs 3275, 3276)

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

...

(#2314, #2315, #2588, #2589)

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 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 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 Frame Control, and the ID field, which are obtained from the WUR Wake-up frame, the Embedded BSSID field, which is equal to the 16 MSBs of the compressed BSSID (see 29.5.2 (Compressed BSSID)), and 4 reserved bits as shown in Figure 29-2 (AAD construction for WUR frames).(#2518, #2820, #2420, #2339, #2557, #2821, #2322)

...

(#2589, #2314)

* WUR PN update procedure(#2314, #2315, #2588, #2589) (CIDs 3265, 3280, 3282, 3283, 3284)

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

The WUR PN Update procedure enables a WUR AP and a WUR non-AP with WUR frame protection negotiated with the WUR AP to update the locally stored PN at the WUR non-AP STA. (#3280)

When the most recently transmitted WUR Operation element has the Common PN subfield equal to 0, a WUR AP may indicate the PN maintained by the WUR AP to the WUR non-AP by including one or more WUR PN Update elements in the WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response.” (#3265, #3282)

When the most recently received WUR Operation element has the Common PN subfield equal to 0, the WUR non-AP STA that receives a WUR Mode Setup frame that includes a WUR PN Update element shall update the locally stored PN value corresponding to the Key ID indicated in the Key Info field to the received PN value. (#3265, #3283)

The WUR non-AP STA may request a PN update by sending a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Request” and includes a WUR PN Update element that indicates a Key ID corresponding to a integrity key currently used by the WUR non-AP STA and optionally includes the corresponding locally stored PN. (#3265, #3283)

When the most recently transmitted WUR Operation element has the Common PN subfield equal to 0, a WUR AP that receives a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Request” and that includes a WUR PN Update element shall respond with a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Response” and includes a WUR PN Update element indicating the PN maintained by the WUR AP corresponding to the requested Key ID if any of the following conditions apply: (#3265, #3284)

* The WUR non-AP STA has negotiated WUR power management service with the WUR AP
* The WUR non-AP STA has not negotiated WUR power management service with the WUR AP and the WUR AP accepts the negotiation

All optional sub-fields of the WUR Parameters field in the WUR Mode element may be omitted.



Protocol Implementation Conformance Statement (PICS) -proforma

* PICS proforma—IEEE Std 802.11-<year>
* Wake-up Radio (WUR) features (CIDs 3265, 3280)

***TGba editor: Modify table B.4.36.1 (WUR MAC features) as the following (Track Changes ON):***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * WUR MAC features (continued) | | | | |
| Item | Protocol capability | References | Status | Support |
|  | Are the following MAC protocol features supported? |  |  |  |
| ... |  |  |  |  |
| WURM10.1(#2589, #2314) | WUR PN Update procedure | 9.4.2.300 (WUR PN Update element), 29.10.3.3 (WUR PN update procedure) | (CFWUR and WURM10):O | Yes  No  N/A  |
| ... |  |  |  |  |