IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment Resolutions for clause 30.9.2 and 30.9.3 Protected WUR frames – part 2 | | | | |
| Date: 2019-05-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
| Lei Huang |  |  |  |
| Yoshio Urabe |  |  |  |
| Alfred Asterjadhi | Qualcomm Inc. |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGba comment collection (TGba Draft 2.0).

* CIDs:
  + 2314, 2315, 2316, 2317
  + 2319, 2320, 2323,
  + 2324, 2325, 2326, 2327
  + 2559, 2582, 2583, 2587, 2588, 2589 (17 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 |
| 2559 | Po-Kai Huang | 78.65 | 30.9.3.1 | Is the temporal key here mean WUR IGTK and WUR PTK? Similar question to page 79 line 7. | Propose to directly say WUR IGTK or WUR PTK. | **Revised.**  Agree with the commenter. Since the integrity keys for protected WUR frames are negotiated separately, it is better to directly say WUR IGTK or WUR TK.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2559. |
| 2582 | Rojan Chitrakar | 77.56 | 30.9.2 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitly refer to the KEY ID associated with the WUR keys. | change "current Key ID value" to: the corresponding WUR IGTK or WUR TK Key ID value" | **Accepted.** |
| 2583 | Rojan Chitrakar | 77.60 | 30.9.2 | How is the RC is initialized before the first protect WUR frame is received needs to be defined. Is it equal to the IPN when the link is established or is it provided during the 4 way/group key handshake? | Clarify how the RC is initialized before the first protect WUR frame is received | **Revised.**  Agree with the commenter that it should be clarified how the replay counters (RC) are initialized. In addition, it is also clarified that separate RCs are maintained for WUR IGTK and WUR TK.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2583. |
| 2587 | Rojan Chitrakar | 78.6 | 30.9.2 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitly refer to the KEY ID associated with the WUR keys. | change "current Key ID value" to: the corresponding WUR IGTK or WUR TK Key ID value" | **Accepted.** |
| 2588 | Rojan Chitrakar | 80.1 | 30.9.3.2 | Explicit update of BPN would only be needed when the Common IPN subfield is 0. | Clarify that Explicit update of BPN only applies when the Common IPN subfield is 0. | **Rejected.**  The group has expressed the desire that the BPN update procedure is applicable for both types of IPNs. |
| 2315 | MARC EMMELMANN | 62.47 | 31.8.3.2 | Explicit update of BPN would only be needed when the Common IPN subfield is 0. | 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. | **Rejected.**  The group has expressed the desire that the BPN update procedure is applicable for both types of IPNs. |
| 2316 | MARC EMMELMANN | 62.42 | 31.8.3.2 | should locally store BPN bit range be [17:56], because on L18 it says BPN is from bit 17 to 56? | 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. | **Rejected.**  In D2.0 BPN has been changed to IPN so the bit range [9:56] is correct. |
| 2317 | MARC EMMELMANN | 61.64 | 31.8.3.1 | 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 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. | **Rejected.**  TSF based protection can be used for broadcast WUR wake-up frames. |
| 2319 | MARC EMMELMANN | 61.2 | 31.8.2 Protected WUR frame reception | "implementation specific value" needs to be defined. | 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. | **Rejected.**  Implementation specific value means that the value is chosen based on whatever consideration of the implementers. |
| 2320 | MARC EMMELMANN | 60.61 | 31.8.2 | TSF update process should not be part of protected WUR frame reception. The protected reception should detect/filter corrupted frames, and then normal frame processing (including WUR Beacon processing, etc.) should happen, so that all these details can be kept in only one place in the Standard | 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. | **Rejected.**  If the protected WUR frames carry TSF, it is beneficial for a WUR STA to update its local TSF timer based on the received TSF and will help the WUR STA maintain TSF accuracy. |
| 2323 | MARC EMMELMANN | 60.55 | 31.8.1 | If the MIC value does not match, the STA should not proceed to the next step (Update the RC). | 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. | **Rejected.**  The issue is already resolved in D2.0. If the MIC value does not match, the BIP procession is terminated for this reception. |
| 2324 | MARC EMMELMANN | 60.53 | 31.8.2 | The following text (4th bullet point) should have an exit statement. Namely, if MIC error occurs, the rest of the procedure shall not be performed. If the result does not match the received MIC value, then the receiver shall discard the frame and increment its internal MIC error counter by 1. | 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. | **Rejected.**  The issue is already resolved in D2.0. If the MIC error occurs, the BIP procession is terminated for this reception. |
| 2325 | MARC EMMELMANN | 60.49 | 31.8.2 | dot11RSNAStatsCMACWURReplays is not defined. | 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. | **Rejected.**  The issue is already resolved in D2.0. dot11RSNAStatsCMACWURReplays is defined in D2.0. |
| 2326 | MARC EMMELMANN | 60.49 | 31.8.2 | If the replay protection failed (i.e. if the IPN is less than or equal to the RC), the STA should not proceed to the next step (construct AAD). | 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. | **Rejected.**  The issue is already resolved in D2.0. If the replay protection fails, the BIP procession is terminated for this reception. |
| 2327 | MARC EMMELMANN | 60.46 | 31.8.1 | How is the RC is initialized before the first protect WUR frame is received needs to be defined. Is it equal to the IPN when the link is established or is it provided during the 4 way/group key handshake? | 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 it should be clarified how the replay counters (RC) are initialized. In addition it is also clarified that separate RCs are maintained for WUR IGTK and WUR TK.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2327. |

**Discussion:** None

**Propose:**

Revised for CIDs 2314, 2327, 2559, 2583, 2589 as per discussion and editing instructions in 11-19/0729r0.

* Protected WUR frames
* Protected WUR frame reception (CIDs 2327, 2583)

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

A WUR non-AP STA with WUR frame protection negotiated that receives a protected WUR Wake-up frame shall follow the rules in 12.5.4.6 (BIP reception) except that the WUR non-AP STA shall:

* Use the appropriate integrity key associated to protected WUR Wake-up frames (see 30.9 (Protected WUR frames)), and associated state based on Key ID equal to the current Key ID value.
* Perform replay protection on the received WUR Wake-up frame as defined in 12.5.4.4 (BIP replay protection) except that the WUR non-AP STA shall construct the IPN locally as defined in 30.9.3.2 (Construction of the IPN by a WUR non-AP STA) and the WUR non-AP STA shall maintain a separate replay counters (*RC*) for each WUR IGTK and WUR TK when the most recently received WUR Operation element has the Common IPN subfield equal to 0. The WUR non-AP STA shall initialize the replay counter to the initial value of the corresponding IPN prior to any update due to WUR Wake-up frames. The WUR non-AP STA shall also initialize the replay counter to the initial value of the corresponding IPN when it resets the WUR IGTK or WUR TK. If IPN is less than or equal to the corresponding *RC* then the WUR non-AP STA shall discard the WUR Wake-up frame, increment its internal dot11RSNAStatsCMACWURReplays counter by 1, and terminate BIP processing for this reception. (#2327, #2583)
* Construct the AAD as defined in Figure 30-2 (AAD construction for WUR frames).
* Extract and save the received MIC value from the FCS field of the WUR Wake-up frame and compute a verifier over the concatenation of AAD, Frame Body field (if present), and the locally constructed IPN. If the result does not match the received MIC value, then the receiver shall discard the frame, increment its internal MIC error counter by 1, and terminate BIP processing for this reception.(#2586)
* Update the *RC* for the integrity key associated to protected WUR Wake-up frames identified by Key ID equal to the current Key ID value with the corresponding IPN. (#2327, #2583)
* If the Common IPN subfield is equal to 1, update the local TSF timer as follows:

**…**

***TGba editor: Insert the following sentence at the end of the subclause:***

A WUR non-AP STA with WUR frame protection negotiated shall discard received WUR Wake-up frames that are not protected.

* Generation and construction of IPN for WUR frames
* Generation of the IPN by a WUR AP (CID 2559 xxx)

***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 IPN subfield in the WUR Operation element it transmits to 0 if it intends to maintain separate IPN counters for WUR IGTK and WUR TK and shall set the Common IPN subfield to 1 if it intends to maintain a common IPN for all protected WUR frames generated within its BSS. The IPN for WUR IGTK is known as WIPN and the IPN for WUR TK is known as WTPN. When the Common IPN subfield is set to 1 WIPN and WTPN are derived in the same way and are equal.

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

—If the Common IPN subfield is equal to 1:

* IPN = PN0||PN1||PN2||PN3||PN4||PN5 = TSF timer [9: 56], where the TSF timer is obtained as defined in 30.5.1 (General).
* The IPN shall never repeat for protected WUR frames generated using the same WUR IGTK or WUR TK (#2559)
* 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 IPN subfield is equal to 0:
* IPN = PN0||PN1||PN2||PN3||PN4||PN5, where IPN shall be incremented by one for each transmitted WUR frame using the same WUR IGTK or WUR TK. (#2559)
* The IPN shall never repeat for protected WUR frames generated using the same WUR IGTK or WUR TK (#2559)
* The WUR AP shall include PN0||PN1[0:3] (i.e., the PPN) in the Type Dependent Control field of the WUR Wake-up frame, if the WUR Wake-up frame is not broadcasted

**…**

* Construction of the IPN by a WUR non-AP STA (CID 2559)

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

**…**

* If the Common IPN subfield is equal to 0, the IPN is obtained as follows:
* The IPN is obtained as PPN||BPN, where PPN is equal to the value of the Type Dependent Control field of the received WUR frame, and BPN is retrieved from the locally stored BPN at the receiver for the corresponding WUR IGTK or WUR TK (#2559)
* PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN

**…**

**CRs for CIDs 2314, 2589: Option 1**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page.Line | Clause | Comment | Proposed Change | Resolution |
| 2589 | Rojan Chitrakar | 80.1 | 30.9.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | Define a new element for this purpose (update of BPN) for WUR. Use WUR Mode setup frames to perform the exchange. | **Revised.**  Agree with the commenter. A new element is defined for the purpose of updating of BPN and Key ID. The element can be included in WUR Mode setup frames.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2589. |
| 2314 | MARC EMMELMANN | 62.47 | 31.8.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | 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. A new element is defined for the purpose of updating of BPN and Key ID. The element can be included in WUR Mode setup frames.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2314. |

**Discussion:** There are two different views on how to achieve update of BPN and Key IDs:

Option 1: Use WUR Mode setup frames for the update.

Option 2: Re-use the header compression procedure (from 802.11ah) for the update.

This section proposes Option 1 i.e. use WUR Mode setup frames for the update.

**Propose:**

Revised for CIDs 2314, 2589 as per discussion and editing instructions in 11-19/0729r0.

* Construction of the IPN by a WUR non-AP STA (CID 2589, 2314)

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

The BPN and the Key ID may be updated explicitly through a WUR Mode Setup request/response exchange. The WUR non-AP STA may send 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 Protection element that indicates a Key ID corresponding to the integrity key currently used by the WUR non-AP STA and the corresponding locally stored BPN.

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 Protection 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 Protection element indicating the Key ID and BPN maintained by the WUR AP. All optional sub-fields of the WUR Parameters field in the WUR Mode element may be omitted. (#2314, #2589) (#338, #903, #904, #1250)

* Frame formats (CID 2589, 2314)

*TGba editor: Insert the following new clause after 9.4.2.293 (WUR Discovery element):*

9.4.2.294 WUR Protection element

The WUR Protection element is used to update the BPN and Key ID maintained by a WUR non-AP STA. The format of the WUR Protection element is shown in Figure 9-xxx (WUR Protection element format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Key Info | BPN | |
| Octets: | 1 | 1 | 1 | 1 | 0 or 5 | |
| Figure 9-xxx - WUR Protection 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-xxx (Key ID field).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 B3 | | B4 | B5 B7 | |
|  | Key ID | | BPN Present | Reserved | |
| Bits: | 4 | | 1 | 3 | |
|  | | Figure 9-xxx Key Info field format | | |

The Key ID subfield contains the Key ID corresponding to the WUR TK or WUR IGTK.

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

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

The BPN field is 5 octets and is illustrated in Figure 9-xxx (BPN field).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | B0 B7 | | B8 B15 | B16 B23 | B24 B31 | B32 B39 |
|  | PN1 | | PN2 | PN3 | PN4 | PN5 |
| Bits: | 8 | | 8 | 8 | 8 | 8 |
|  | | Figure 9-xxx BPN field format | | | | | |

The BPN field contain the portion of the IPN corresponding to the BPN i.e. PN1||PN2||PN3||PN4||PN5 for the integrity key indicated by the Key ID subfield in the Key Info field. When the Common IPN subfield of the WUR Operation element is equal to 1, the PN1 subfield contains PN1 of the IPN. When the Common IPN subfield of the WUR Operation element is equal to 0, bits 4 to 7 of the PN1 subfield contains PN1[4:7] of the IPN while bits 0 to bits 3 are reserved.

* WUR Mode Setup frame format

***TGba editor: Modify Table 9-524b as the following (Track Changes ON):***

|  |  |
| --- | --- |
| * WUR Mode Setup frame Action field format | |
| Order | Information |
| 1 | Category |
| 2 | WUR Action |
| 3 | Dialog Token |
| 4 | WUR Mode element (see 9.4.2.292 (WUR Mode element)) |
| 5 | WUR Operation element (optional) (see 9.4.2.291 (WUR Operation element)) |
| 6 | WUR Protection element (optional) (see 9.4.2.294 (WUR Protection element)) |

***TGba editor: Insert the following sentence at the end of the subclause:***

The WUR Protection element field contains a WUR Protection element as defined in 9.4.2.294 (WUR Protection element). (#2589, #2314)

* WUR power management procedure
* WUR mode setup

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

**…**

A WUR AP may assign the WUR channel to WUR non-AP STAs or select the data rate of the transmitted WUR PPDU based on the values contained in the Recommended WUR Parameters subfields received from these WUR non-AP STAs.(#Ed, #2696, #2697, #2752)

A WUR AP may indicate the WUR security parameters to a WUR non-AP STA with WUR frame protection negotiated by including one or more WUR Protection element in the WUR Mode Setup frames.

A WUR non-AP STA with WUR frame protection negotiated with the WUR AP and that receives the WUR Mode Setup frames that includes a WUR Protection element shall use the integrity key corresponding to the Key ID indicated in the Key Info field to receive corresponding protected WUR wake-up frame from the WUR AP (see 30.9 (Protected WUR frames)). If the BPN field is present in the WUR Protection element, the WUR non-AP STA shall also update the locally stored BPN value corresponding to the Key ID indicated in the Key Info field. (#2589, #2314)

After a WUR non-AP STA has negotiated WUR service with a WUR AP, the WUR AP may update the WUR parameters with the WUR non-AP STA in WUR mode, or WUR Mode Suspend by using the PCR component to initiate and complete a successful frame exchange, which includes an unsolicited WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response”, or “Enter WUR Mode Suspend Response”, from the WUR AP and an Ack frame from the WUR non-AP STA. The WUR non-AP STA that sent the ACK frame in response to the unsolicited WUR Mode Setup frame shall update the WUR parameters to the parameters included in the recieved WUR Mode Setup frame. The STA may tear down WUR operation if the STA doesn’t intend to use the parameters. After a WUR non-AP STA has negotiated WUR service with a WUR AP, the WUR AP may update the WUR parameters with the WUR non-AP STA in WUR mode, or WUR Mode Suspend by using the PCR component to initiate and complete a successful frame exchange, which includes an unsolicited WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response”, or “Enter WUR Mode Suspend Response”, from the WUR AP and an Ack frame from the WUR non-AP STA. The WUR non-AP STA that sent the ACK frame in response to the unsolicited WUR Mode Setup frame shall update the WUR parameters to the parameters included in the recieved WUR Mode Setup frame. The STA may tear down WUR operation if the STA doesn’t intend to use the parameters. After a WUR non-AP STA has negotiated WUR power management service with a WUR AP, the WUR AP may update the WUR parameters with the WUR non-AP STA in WUR mode by initiating and completing a successful frame exchange, which includes an unsolicited WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response” from the WUR AP and an Ack frame from the WUR non-AP STA as described in Table 30-2 (WUR Mode Setup/Teardown frame transmission). The WUR AP may also update the WUR security parameters with the WUR non-AP STA in WUR mode by initiating and completing a successful frame exchange, which includes an unsolicited WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response” and includes one or more WUR Protection element from the WUR AP and an Ack frame from the WUR non-AP STA. (#2589, #2314)

After a WUR non-AP STA has negotiated WUR power management service with a WUR AP, the WUR AP may update the WUR parameters with the WUR non-AP STA in WUR mode suspend by initiating and completing a successful frame exchange, which includes an unsolicited WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Suspend Response” from the WUR AP and an Ack frame from the WUR non-AP STA as described in Table 30-2 (WUR Mode Setup/Teardown frame transmission).

The WUR non-AP STA that sent the Ack frame in response to the unsolicited WUR Mode Setup frame shall update the WUR parameters to the parameters included in the received WUR Mode Setup frame. If the unsolicited WUR Mode Setup frame included a WUR Protection element, the WUR non-AP STA shall also update the WUR security parameters. The WUR non-AP STA shall use the integrity key corresponding to the Key ID indicated in the Key Info field to receive corresponding protected WUR wake-up frame from the WUR AP (see 30.9 (Protected WUR frames)). If the BPN field is present in the WUR Protection element, the WUR non-AP STA shall also update the locally stored BPN value corresponding to the Key ID indicated in the Key Info field. The WUR non-AP STA may teardown WUR operation as described below if the WUR non-AP STA doesn’t intend to use the parameters. (#2589, #2314)

**…**

* (CID 2589, 2314)

Protocol Implementation Conformance Statement (PICS) -proforma

* Wake-up Radio (WUR) features

*TGba editor: Change Table B.4.36.1 as follows (Track Change ON):*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * WUR MAC features | | | | |
| Item | Protocol capability | References | Status | Support |
|  | Are the following MAC protocol features supported? |  |  |  |
| **…** |  |  |  |  |
| WURM10 | Protected WUR frames | 30.9 (Protected WUR frames) | CFWUR:O | Yes  No  N/A  |
| WURM10.1 | Signaling of WUR security parameters in WUR Mode Setup | 9.6.34.2 (WUR Mode Setup frame format),  9.4.2.294 (WUR Protection element) | (CFWUR AND WURM10):M | Yes  No  N/A  |

**CRs for CIDs 2314, 2589: Option 2**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page.Line | Clause | Comment | Proposed Change | Resolution |
| 2589 | Rojan Chitrakar | 80.1 | 30.9.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | Define a new element for this purpose (update of BPN) for WUR. Use WUR Mode setup frames to perform the exchange. | **Revised.**  After much discussions it was decided to reuse the Header Compression procedure originally defined in 802.11ah for the update of WUR BPN and Key ID.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2589. |
| 2314 | MARC EMMELMANN | 62.47 | 31.8.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | 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.**  After much discussions it was decided to resue the Header Compression procedure originally defined in 802.11ah for the update of WUR BPN and Key ID.    TGba editor to make the changes shown in 11-19/0729r0 under all headings that include CID 2314. |

**Discussion:**

This section proposes Option 2 i.e. re-use the header compression procedure (from 802.11ah) for the update.

**Propose:**

Revised for CIDs 2314, 2589 as per discussion and editing instructions in 11-19/0729r0.

* Construction of the IPN by a WUR non-AP STA (CID 2589, 2314)

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

The BPN and the Key ID may be updated explicitly through a secure header compression request/response exchange by using only the WUR Protection Update field of the exchange as defined in 10.59 (Generation of PV1 MPDUs and header compression procedure). (#2314, #2589) (#338, #903, #904, #1250)

* Frame formats (CID 2589, 2314)

9.4.2.213 Header Compression element

*TGba editor: Modify Figure 9-713 as follows (Track Change ON):*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Header Compresson Control | A3  (optional) | A4  (optional) | CCMP Update  (optional) | WUR Protection Update (optional) |
| Octets: | 1 | 1 | 1 | 0 or 6 | 0 or 6 | 0 or 5 | 0 or 1 or 6 |
| Figure 9-713 – Header Compression element format | | | | | | | | |

*TGba editor: Modify Figure 9-714 as follows (Track Change ON):*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | B0 | B1 | B2 | B3 | B4 | B5 | B6 B7 |
|  | | Request/  Response | Store A3 | Store A4 | CCMP Update Present | PV1 Data Type 3 Supported | WUR Protection Update Present | Reserved |
| Bits: | | 1 | 1 | 1 | 1 | 1 | 1 | 2 |
|  | Figure 9-714 – Header Compression Control field | | | | | | | | |

*TGba editor: Modify the following paragraphs as follows (Track Change ON) :*

**…**

The PV1 Data Type 3 Supported subfield is set to 1 to indicate that reception of PV1 frames with Type field equal to 3 is enabled. Otherwise, it is set to 0.

The WUR Protection Update subfield is set to 1 in the header compression request to indicate the receiving WUR non-AP STA to update the base packet number (BPN) and Key ID fields and is set to 1 in the header compression response to confirm the update of the fields or to indicate MIC failure on a received protected WUR frame. Otherwise, it is set to 0 in the header compression request to indicate no WUR Protection update request and is set to 0 in the header compression response to indicate no WUR Protection update confirmation.

The A3 field in the Header Compression element is present if the Request/Response subfield is 0 and the Store A3 subfield is 1. Otherwise, it is not present.

**…**

*TGba editor: Insert the following at the end of the subclause:*

The WUR Protection Update field in the Header Compression element is present if the WUR Protection Update subfield is set to 1. Otherwise, it is not present.

The WUR Protection Update field is either 1 octet or 6 octets and is shown in Figure 9-xxx (WUR Protection Update field).

|  |  |  |
| --- | --- | --- |
|  | Key Info | BPN  (optional) |
| Octets: | 1 | 0 or 5 |
| **Figure 9-xxx WUR Protection Update field** | | |

The Key Info field is 1 octets and is illustrated in Figure 9-xxx (Key ID field).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 B3 | | B4 | B5 B7 | |
|  | Key ID | | BPN Present | Reserved | |
| Bits: | 4 | | 1 | 3 | |
|  | | Figure 9-xxx Key Info field | | |

The Key ID subfield contains the Key ID corresponding to the WUR TK or WUR IGTK.

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

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

The BPN field is 5 octets and is illustrated in Figure 9-xxx (BPN field).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 B7 | B8 B15 | B16 B23 | B24 B31 | B32 B39 |
|  | PN1 | PN2 | PN3 | PN4 | PN5 |
| Bits: | 8 | 8 | 8 | 8 | 8 |
| Figure 9-xxx BPN field | | | | | | |

The BPN field contain the portion of the IPN corresponding to the BPN i.e. PN1||PN2||PN3||PN4||PN5 for the integrity key indicated by the Key ID subfield in the Key Info field. When the Common IPN subfield of the WUR Operation element is equal to 1, the PN1 subfield contains PN1 of the IPN. When the Common IPN subfield of the WUR Operation element is equal to 0, bits 4 to 7 of the PN1 subfield contains PN1[4:7] of the IPN while bits 0 to bits 3 are reserved.

* Generation of PV1 MPDUs and header compression procedure (CID 2589, 2314)

*TGba editor: Modify the subclause as follows (Track Change ON) :*

**…**

The header compression procedure enables S1G STAs to store addresses and/or update security parameters at the receiver. (#1258)An S1G STA with dot11PV1MACHeaderOptionImplemented equal to true shall set dot11RSNAProtectedManagementFramesActivated to true and dot11RSNAUnprotectedManagementFramesAllowed to false. The header compression procedure enables WUR STAs to update WUR security parameters.

An S1G STA with dot11PV1MACHeaderOptionImplemented equal to true may include a Header Compression element in Header Compression frames. The STA may include the Header Compression element in (Re)Association Request frames and (Re)Association Response frames when management frame protection is not negotiated for the association. The STA may set the PV1 Data Type 3 Supported subfield in the Header Compression element to 1 to indicate that it supports reception of PV1 frames that have the Type subfield in the Frame Control field equal to 3.

After association, an S1G STA with dot11PV1MACHeaderOptionImplemented equal to true may transmit Header Compression frames and PV1 frames. An S1G STA shall not transmit PV1 frames with Type subfield equal to 3 to a peer STA unless the PV1 Data Type 3 Supported subfield is 1 in the most recently received Header Compression element sent by the peer STA. An S1G STA in an IBSS shall not transmit PV1 frames with a value of the Type subfield equal to 0 or 1. After WUR frame protection has been negotiated between a WUR non-AP STA and a WUR AP, the WUR AP and the WUR non-AP STA may exchange Header Compression frames to update WUR security parameters.

NOTE—A PV1 frame is an (Ed)MPDU with Protocol Version field in the Frame Control field equal to 1 (see 9.8 (MAC frame format for PV1 frames(11ah))).

The header compression procedure uses a Header Compression element, which is referred to as a header compression request or a header compression response, depending on the Request/Response subfield setting of the Header Compression element.

A STA that transmits PV1 frames with Type subfield equal to 0 shall include the A3 field if the value of this field:

* Is not equal to the address identified by the A1 field and an A3 is not stored at the receiver
* Is not equal to the A3 stored at the receiver.

Otherwise, the A3 field shall not be included in the frame.

A STA that transmits PV1 frames with Type subfield equal to 0 shall include the A4 field if the value of this field:

* Is not equal to the address identified by the A2 field and an A4 is not stored at the receiver
* Is not equal to the A4 stored at the receiver.

Otherwise, the A4 field shall not be included in the frame.

An S1G STA indicates a request to store address fields by sending a header compression request with the Store A3 and/or Store A4 subfields equal to 1. Upon receipt of such a request, the receiving STA shall respond with a header compression response indicating which of the optional fields it stores, by setting the Store A3 and/or Store A4 subfields in the transmitted header compression response to 1. Stored address fields can subsequently be omitted from the MAC header of PV1 frames transmitted by the STA that sent the header compression request. Address A3 and/or A4 fields for which the header compression response indicated 0 are not stored at the receiver and cannot be omitted by the transmitter when the A3 and/or A4 fields contain values that are different from the A1 and/or A2 fields of the same.

An S1G STA indicates a request to update security parameters by sending a header compression request with the CCMP Update subfield equal to 1. The receiver STA shall respond with a header compression response acknowledging receipt of the updated security parameters. (#1259)The receiver STA shall compare the received BPN value to the current locally stored BPN value. If the received BPN value is greater than the locally stored BPN value, the receiver STA shall update the locally stored BPN value. Otherwise, the receiver STA shall not update the locally stored BPN value. A WUR AP indicates a request to update WUR security parameters by sending a header compression request with the WUR Protection Update subfield equal to 1. The receiver WUR non-AP STA shall respond with a header compression response acknowledging receipt of the updated WUR security parameters. If the BPN field is present in the Header Compression element, the WUR non-AP STA shall compare the received BPN value to the current locally stored BPN value corresponding to the Key ID indicated in the Key Info field. If the received BPN value is greater than the locally stored BPN value, the WUR non-AP STA shall update the locally stored BPN value. Otherwise, the WUR non-AP STA shall not update the locally stored BPN value. If the Key ID indicated in the Key Info field indicates a WUR TK that is different than the WUR TK that the WUR non-AP STA is currently using, the WUR non-AP STA shall start using the WUR TK corresponding to the Key ID indicated in the Key Info field to receive subsequent protected individually addressed WUR wake up frames. If the Key ID indicated in the Key Info field indicates a WUR IGTK that is different than the WUR IGTK that the WUR non-AP STA is currently using, the WUR non-AP STA shall start using the WUR IGTK corresponding to the Key ID indicated in the Key Info field to receive subsequent protected broadcast and group addressed WUR wake up frames.

After sending a header compression request, an S1G STA shall postpone the transmission of PV1 frames that do not include the fields that were requested to be stored to the recipient of the header compression request until it receives the corresponding header compression response.

After receiving a header compression request, an S1G STA shall store and activate the included addresses it intends to store and/or the security information included in the header compression request before transmitting the corresponding header compression response. After receiving a header compression request, a WUR non-AP STA shall update the WUR security information included in the header compression request before transmitting the corresponding header compression response.

When no header compression response has been received in response to a header compression request within dot11HeaderCompressionResponseTimeout, an S1G STA shall transmit another header compression request.

A STA that receives a PV1 frame with one or more compressed addresses that it has not stored or which causes a decryption error should transmit an unsolicited header compression response to the transmitter of the PV1 frames, in which the Store A3, and Store A4 fields are all equal to 0. The unsolicited header compression response shall include the TID/ACI of the received PV1 frame in the TID/ACI subfield of the CCMP Update field if the received frame caused a decryption error, where the CCMP Update field shall indicate the stored values for the BPN and Key ID that correspond to the received PV1 frame. A WUR non-AP STA that receives a protected WUR frame which causes a MIC failure should transmit an unsolicited header compression response to the WUR AP, in which the Store A3, Store A4 and CCMP Update Present fields are all equal to 0. The unsolicited header compression response shall include the WUR Protection Update field, where the WUR Protection Update field shall include the stored values of the BPN and Key ID that correspond to the received WUR frame.

A STA that has previously transmitted PV1 frames of a given TID/ACI to a peer STA and that receives an unsolicited header compression response from the peer STA relative to that TID/ACI shall transmit a header compression request to the transmitter of the header compression response. The header compression request shall include all the addresses that the transmitting STA requests to be stored at the receiver and/or the security information that corresponds to the indicated TID/ACI. A WUR AP that has previously transmitted protected WUR frames to a WUR non-AP STA and that receives an unsolicited header compression response from the WUR non-AP STA shall transmit a header compression request to the transmitter of the header compression response. The header compression request shall include the security information that corresponds to the transmitted protected WUR frames.

* (CID 2589, 2314)

Protocol Implementation Conformance Statement (PICS) -proforma

* MAC protocol

*TGba editor: Change Table B.4.4.2 as follows (Track Change ON):*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * MAC frames | | | | |
| Item | MAC frame | References | Status | Support |
|  | Is transmission of the following MAC frames supported? | 9 (Frame formats) |  |  |
| ... |  |  |  |  |
| FT<Last\_assigned+6> | WUR Mode Teardown frame | 9.6.34.3 (WUR Mode Teardown frame format) | CFWUR:M | Yes  No  N/A  |
| FT<Last\_assigned+7> | Header Compression frame | 9.6.25.5 (Header Compression frame format) | (CFWUR AND WURM13):M | Yes  No  N/A  |
|  | Is reception of the following MAC frames supported? | 9 (Frame formats) |  |  |
| ... |  |  |  |  |
| FR<Last\_assigned+6> | WUR Mode Teardown frame | 9.6.34.3 (WUR Mode Teardown frame format) | CFWUR:M | Yes  No  N/A  |
| FR<Last\_assigned+7> | Header Compression frame | 9.6.25.5 (Header Compression frame format) | (CFWUR AND WURM13):M | Yes  No  N/A  |

* Wake-up Radio (WUR) features

*TGba editor: Change Table B.4.36.1 as follows (Track Change ON):*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * WUR MAC features | | | | |
| Item | Protocol capability | References | Status | Support |
|  | Are the following MAC protocol features supported? |  |  |  |
| **…** |  |  |  |  |
| WURM10 | Protected WUR frames | 30.9 (Protected WUR frames) | CFWUR:O | Yes  No  N/A  |
| WURM10.1 | Header compression procedure | 10.59 (Generation  of PV1  MPDUs and  header compression  procedure (  11ah)) | (CFWUR AND WURM10):M | Yes  No  N/A  |

**Straw Poll:**

Which option do you prefer for the CRs for CIDs 2314, 2589?

Option 1: Use WUR Mode setup frames for the update.

Option 2: Re-use the header compression procedure (from 802.11ah) for the update.

Abstain: