IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment resolutions for protected WUR frames | | | | |
| Date: 2018-12-27 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Alfred Asterjadhi | Qualcomm Inc. | 5775 Morehouse Dr, San Diego, CA 92109 | +1-858-658-5302 | aasterja@qti.qualcomm.com |
| Jouni Malinen | Qualcomm Inc. |  |  |  |
| Soo Bum Lee | Qualcomm Inc. |  |  |  |

Abstract

This submission proposes resolutions for multiple comments related to TGba D1.0 with the following CIDs (56 CIDs):

* 20, 21, 90, 143, 144, 145, 324, 338, 466, 467,
* 468, 486, 571, 572, 573, 592, 643, 644, 645, 646,
* 682, 759, 760, 806, 807, 808, 809, 812, 813, 814,
* 828, 881, 892, 893, 894, 895, 896, 897, 898, 899,
* 900, 901, 902, 903, 904, 905, 906, 907, 908, 909,
* 1187, 1247, 1248, 1249, 1250, 1251

Revisions:

* Rev 0: Initial version of the document

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGba Draft. This introduction is 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** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 20 | Albert Petrick | 59.65 | Clarify term |  | Rejected –  The comment fails to provide enough details for the CRC to be able to address the comment.  Please submit the comment with some more information, e.g., what is the term to be clarified. |
| 21 | Albert Petrick | 60.31 | Clarify term |  | Rejected –  The comment fails to provide enough details for the CRC to be able to address the comment.  Please submit the comment with some more information, e.g., what is the term to be clarified. |
| 90 | Alfred Asterjadhi | 44.07 | 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. | As in comment. |  |
| 143 | Alfred Asterjadhi | 59.35 | Explicitly call out which WUR frames can be protected and which ones cannot. And also that when protection is used then it is used all the times between that AP and WUR STA. Also clarify what is meant with "current Key ID" in this subclause, from both the transmitters perspective and from the recipients perspective. | As in comment. |  |
| 144 | Alfred Asterjadhi | 59.32 | There are some redundancies across this subclause in terms of normative behavior and descriptions. Please ensure that duplicates and redundant descriptions are removed. | As in comment. |  |
| 145 | Alfred Asterjadhi | 60.53 | 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. | As in comment. |  |
| 324 | Ihtisham Khalid |  | Relevant to the security and privacy, implications include wake up procedures. Hostile wake ups can have serious concerns over battery drainage and false functioning of systems in case of association with the attacker. Intruder can eavesdrop privacy information in WUR packets. | Document IEEE 802.11-17/0411 highlighted some considerations about Wake-up receiver security. It seems as if draft 1.0 lacks consistency is this respect. Analysis of this document in these respects may be helpful in tackling issues at later stages. |  |
| 338 | Ihtisham Khalid | 62.01 | Only abbreviation is used for "BPN" | please mention full form when it is used for the first time in text. | Revised –  Agree in principle with the comment. Proposed resolution is to clarify that this is the IPN and, which is already used in full form in the baseline.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 338. |
| 466 | John Buffington | 59.58 | terms WUR IGTK and WUR TK are not defined. | The first use of both "WUR IGTK" and "WUR TK" need to be defined or added to section 3.4. | Revised –  Agree in principle with the comment. The first time IGTK and TK are already mentioned in clause 12 of baseline. However, since they are also going to be used independently for WUR PPDUs then it is beneficial to call them out here as well.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 466. |
| 467 | John Buffington | 60.21 | Abbreviation "AP" should be "WUR AP". | Replace both instances of "AP" with "WUR AP". | Accepted  Note to TGba editor: This is already part of D1.1, hence no further changes are necessary. |
| 468 | John Buffington | 61.02 | "implementation specific value" needs to be defined. | The specification refers to an "implementation specific value" which should be defined, or at minimum given a reference that identifies a reasonable set of values. |  |
| 486 | Joseph Levy | 60.38 | A non-AP STA can not receive a WUR PPDU, only a WURx can receive a WRU PPDU, this should be clear in the text. The 802.11 MAC does not know what to do with a WRU PPDU, this needs to be handled by an entity that understands WUR procedures and actions. The non-AP STA is not even awake when the WUR PPDU is received, it needs to be woken up by some entity, probably the SME, it is likely that the SME in a WUR device should be capable of waking up the non-AP STA when the WURx receives a WUR PPDU addressed to the WURx. | Fix the protected WUR frame reception so that the WURx is the entity receiving the PPDU and it is clear what entity the WURx sends the information to and what actions are taken. | Revised –  All these normative behaviors are under clause WUR MAC specification, i.e., they are performed by a WUR STA. In any case in the cited portion of by the comment the proposed resolution is to replace non-AP STA with WUR non-AP STA.  Note to TGba editor: This is already part of D1.1, hence no further changes are necessary.  TGba editor: Please replace “non-AP STA” with WUR non-AP STA”. |
| 571 | Li-Hsiang Sun | 60.08 | 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? | Add counter field in AAD in case of broadcast WUR wake-up frame is protected |  |
| 572 | Li-Hsiang Sun | 62.16 | Can the WUR beacon be protected? | Add description to construct IPN from the TD field of WUR beacon frame, or add a requirement indicating WUR beacon is never protected | Revised –  Whether WUR Beacon frame can be protected needs further investigation. For now, the proposed resolution is to specify that the Protected subfield is set to 0 for WUR Beacon frames.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 572. |
| 573 | Li-Hsiang Sun | 62.42 | should locally store BPN bit range be [17:56], because on L18 it says BPN is from bit 17 to 56? | change to [17:56] |  |
| 592 | Mark Hamilton | 60.61 | 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 | The instructions here (for a Common IPN field equal to 1) should indicate that TSF updating proceeds, as per 31.4.3. Merge differences between 31.8.2 and 31.4.3 (if any) into 31.4.3. |  |
| 643 | Michael Montemurro | 59.31 | If the intention of clause 31.8 is to leverage existing IEEE 802.11 encapsulation mechanisms, these clauses should be moved to Clause 12. Placing clauses at this location makes it difficult to evaluate whether these mechanisms introduce security vulnerabilities. | Move the contents of 31.8 to the appropriate locations of Clause 12. |  |
| 644 | Michael Montemurro | 61.41 | Why are two IPN mechanisms required for WUR? Why can't the encapsulation be consistent with other encapsulation mechanisms and use the mechanism when Common IPN = 0. | Remove the Common IPN field and all requirements for mechanisms associated with Common IPN field set to 1. | Rejected –  The Common IPN = 1 allows the AP to enable a mode where the message integrity check is per RA (i.e., per STA), while more beneficial since it is per RA, TA, it is also more complex because the AP needs to maintain the status (separate IPNs for each) for different connections. In the Common IPN = 0 the AP is simpler because the AP is using its internal clock to construct the IPN. |
| 645 | Michael Montemurro | 61.44 | "Couple" should be "duple" | Replace "<Address, Embedded BSSID> couple" with "<Address, Embedded BSSID> duple" | Accepted |
| 646 | Michael Montemurro | 61.31 | Given that the WUR connection between the STA and the AP are a separate communications connection for a separate purpose (WUR), WUR should use a separately derived key. | Provide separate key derivation for WUR encapsulation and BIP keys. It can be based on the existing STA-AP Security Association |  |
| 682 | Ming Gan | 61.64 | 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. | Make PN based security protection mechanism complete. |  |
| 759 | Nehru Bhandaru | 59.58 | It is not clear how WUR IGTK and WUR TK are negotiated. Does that require a separate handshake? | Specify an key descriptor element KDE for WUR IGTK. Also derive WUR TK instead of a separate handshake that seems unnecessary. See 11-18/1313r0 |  |
| 760 | Nehru Bhandaru | 59.64 | CMAC may be an overkill since the output MIC is truncated to 16 bits | Use something simple like sip hash | Rejected –  The intention is to use an existing architecture rather than designing a new one. The proposal is to use a minimal set of the CMAC components from the PCR for WUR counterpart. |
| 806 | Peter Ecclesine | 61.44 | the term couple is Undefined: for each <Address, Embedded BSSID> couple and | for each <Address, Embedded BSSID> tuple and | Revised –  Proposed resolution is to replace with duple.  TGba editor: Please replace “couple” with “duple”. |
| 807 | Peter Ecclesine | 61.60 | the term couple is Undefined: key and <Address, Embedded BSSID> couple. | key and <Address, Embedded BSSID> tuple. | Revised –  Proposed resolution is to replace with duple.  TGba editor: Please replace “couple” with “duple”. |
| 808 | Peter Ecclesine | 61.63 | the term couple is Undefined: key and <Address, Embedded BSSID> couple. | key and <Address, Embedded BSSID> tuple | Revised –  Proposed resolution is to replace with duple.  TGba editor: Please replace “couple” with “duple”. |
| 809 | Peter Ecclesine | 62.35 | the term couple is Undefined: for the <Address, Embedded BSSID> couple | for the <Address, Embedded BSSID> tuple | Revised –  Proposed resolution is to replace with duple.  TGba editor: Please replace “couple” with “duple”. |
| 812 | Peter Ecclesine | 61.41 | STAs have no intentions. There are sixn uses of 'intends' in the text. Rewrite text to say what STAs do. | A WUR AP that will transmit protected WUR frames | Rejected –  The comment fails to identify a technical issue. The term “intends to” is widely used in the baseline standard (please refer to IEEE802.11-2016). |
| 813 | Peter Ecclesine | 61.44 | STAs have no intentions. There are six uses of 'intends' in the text. Rewrite text to say what STAs do. | to 1 if it will maintain a common ... | Rejected –  The comment fails to identify a technical issue. The term “intends to” is widely used in the baseline standard (please refer to IEEE802.11-2016). |
| 814 | Peter Ecclesine | 61.48 | STAs have no intentions. There are six uses of 'intends' in the text. Rewrite text to say what STAs do. | The WUR AP that will transmit ... | Rejected –  The comment fails to identify a technical issue. The term “intends to” is widely used in the baseline standard (please refer to IEEE802.11-2016). |
| 828 | Po-Kai Huang | 60.24 | When the key is WUR IGTK, WUR AP may only update some STAs to the new WUR IGTK with new key ID, and some STAs still use old WUR IGTK with old key ID. As a reuslt, the definition of current Key ID is different for different STAs | Have an indication in broadcast WUR frame to indicate current key ID. Most likely, the indication will be in misc field. |  |
| 878 | Rojan Chitrakar | 32.00 | It would be good if the WUR protection capability of a WUR STA is verified during Message 2 and 3 of the 4-way handshake used to negotiate WUR TK (as is done for management frame protection - 802.11-2016-P1193 last paragraph). The "Protection Support" bit then is better shifted/copied to the RSN capabilities field of the RSNE. Otherwise, the WUR capabilities element may need to be carried in Message 2 and 3 of the 4-way handshake just for this one bit. | Either move or create a copy of the "Protection Support" bit in the RSN capabilities field of the RSNE. |  |
| 881 | Rojan Chitrakar | 43.09 | Can WUR Beacon frames be protected? Please clarify | If WUR Beacon frames can also be protected, add description of which fields are used for PPN etc. If WUR Beacon frames cannot be protected, add the below sentence: The Protected subfield in the Frame Control field is reserved. | Revised –  Whether WUR Beacon frame can be protected needs further investigation. For now, the proposed resolution is to specify that the Protected subfield is set to 0 for WUR Beacon frames.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 881. |
| 892 | Rojan Chitrakar | 59.51 | 12.5.4 should also mention that BIP is also used for protection of WUR frames. | Add texts in 12.5.4.1 (BIP overview) that BIP is also used for protection of WUR frames and add reference to 31.8 (Protected WUR frames). |  |
| 893 | Rojan Chitrakar | 59.58 | It should be clarified when exactly does the negotiation of integrity keys (WUR IGTK) and (pairwise WUR TK) takes place? Is it right after Association, or does it only happen after a successful WUR mode setup? Adding a figure of the handshaking used to exchange WUR keys would be very helpful. | as in comment |  |
| 894 | Rojan Chitrakar | 59.58 | Similar to management frame protection, WUR frame protection should also be added to the RSNA establishment procedure | Add text in each relevant sections of 12.2.4 (RSNA establishment) to specify the steps taken by a STA to program the WUR TK and WUR IGTK used to protect WUR frames: "If the STAs negotiate protection of WUR frames, the SME programs the WUR TK and pairwise cipher suite into the WUR MAC for protection of individually addressed WUR frames. It also installs the WUR IGTK and IPN for protection of broadcast and group addressed WUR frames. |  |
| 895 | Rojan Chitrakar | 60.24 | What is the "current Key ID value"? An AP may have may Keys installed, its better to explicitely 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" |  |
| 896 | Rojan Chitrakar | 60.30 | MIC field is not defined in "..., and insert the truncated output into the MIC field of the WUR frame." | Change to: "IPN, and insert the 16-bit truncated output (MIC) into the FCS field of the WUR frame." |  |
| 897 | Rojan Chitrakar | 60.42 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitely 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" |  |
| 898 | Rojan Chitrakar | 60.46 | 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 |  |
| 899 | Rojan Chitrakar | 60.49 | dot11RSNAStatsCMACWURReplays is not defined. | Added definition of dot11RSNAStatsCMACWURReplays in Annex C. |  |
| 900 | Rojan Chitrakar | 60.49 | 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). | Add to the end of the paragraph: "..., and terminate BIP processing for this reception." |  |
| 901 | Rojan Chitrakar | 60.55 | If the MIC value does not match, the STA should not proceed to the next step (Update the RC). | Add to the end of the paragraph: "..., and terminate BIP processing for this reception." |  |
| 902 | Rojan Chitrakar | 60.59 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitely 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" |  |
| 903 | Rojan Chitrakar | 62.01 | Does the AP also need BPN? | Clarify whether it is local BPN or IPN. If it is BPN, provided definition of BPN for AP. | Revised –  Agree in principle with the comment. Proposed resolution is to specify that the IPN is the one initialized, rather than the BPN.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 903. |
| 904 | Rojan Chitrakar | 62.05 | Does the AP also need BPN? | Clarify whether it is local BPN or IPN. If it is BPN, provided definition of BPN for AP. | Revised –  Agree in principle with the comment. Proposed resolution is to specify that the IPN is the one initialized, rather than the BPN.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 904. |
| 905 | Rojan Chitrakar | 62.38 | "The locally stored BPN at the WUR non-AP STA is initialized to 0..." What abou the PPN? Doesn't it need to be initialized, or is it only set when the first protected WUR frame is received? | Clarify how the PPN is initialized as it may have an impact on the intial RC value. | Revised –  Agree in principle with the comment. Proposed resolution is to specify that the IPN is the one initialized, rather than the BPN.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 905. |
| 906 | Rojan Chitrakar | 62.42 | The initial value of BPN should be local TSF time [17:56] | change to: "The locally stored BPN at the WUR non-AP STA is initialized to the value of the local TSF time [17:56] ..." | Revised –  Agree in principle that there is an inconsistency. The proposed resolution is to clarify that the overall IPN, which includes the BPN, which is inline with the TSF timer [9: 56] value.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 906. |
| 907 | Rojan Chitrakar | 62.42 | What abou the PN0? Doesn't it need to be initialized, or is it only set when the first protected WUR frame is received? | Clarify how the PN0 is initialized as it may have an impact on the intial RC value. | Revised –  Agree in principle with the comment. Proposed resolution is to specify that the IPN is the one initialized, rather than the BPN.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 907. |
| 908 | Rojan Chitrakar | 62.47 | 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. |  |
| 909 | Rojan Chitrakar | 62.47 | 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. |  |
| 1187 | yujin noh | 59.32 | if needed, replace WUR STA with WUR non-AP STA like subclauses above in 31.8. For example, starting sentence with "An AP may transmit a protected WUR frame address to a WUR STA....", a WUR STA should be a WUR non-AP STA to be consistent through the spec. | as in comment | Revised –  TGba editor: Please replace “WUR STA” with “WUR non-AP STA” throughough this subclause. |
| 1247 | Yunsong Yang | 59.59 | The separate WUR IGTK is not specified in this draft nor in the baseline document. | Provide the specification of the WUR IGTK in the draft. And add a definition of it to clause 3.2. |  |
| 1248 | Yunsong Yang | 59.60 | The separate WUR TK is not specified in this draft nor in the baseline document. | Provide the specification of the WUR TK in the draft. And add a definition of it to clause 3.2. |  |
| 1249 | Yunsong Yang | 60.58 | The bullets on L58 and L60 shouldn't be at the same level as the previous bullets, because they are executed only when the MIC values match under the previous bullet. | Make the bullets on L58 and L60 sub-bullets of the previous bullet with the condition that the MIC values match. And the modify the indentations of the subsequent sub-bullets accordingly. |  |
| 1250 | Yunsong Yang | 62.01 | It is uncler what the link refers to in "The local BPN at the WUR AP is initialized to 0 when the link is established". Does it refer to the WUR configuration or the association with the STA? The same question exist in L5, L38, and L43 on the same page. | Please make it clear in all cited places. | Revised –  Agree in principle with the comment. Proposed resolution clarifies that the IPNs are initialized to 0 when the WUR mode link is established (and provided reference) in all cited locations. Also clarified that in this case it is transmitted (AP) rather than received.  TGba editor to make the changes shown in 11-18/2145r0 under all headings that include CID 1250. |
| 1251 | Yunsong Yang | 62.61 | "shall" should be "may", given the statement is "set ... to any value..." | Change "shall" to "may". | Accepted |

**Discussion: *…***

**9.10.3.1 WUR Beacon frame format**

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 572, 881):***

The frame format of the WUR Beacon frame is as defined in Figure 9-963a (WUR frame format).

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

The Protected subfield of the Frame Control field is set to 0.*(#572, 881)*

The Address field of the WUR Beacon frame is set to the transmit ID.

The TD Control field contains the partial TSF that is generated as defined in 31.4.1 (General).

The Frame Body field is not present in the WUR Beacon frame.

* Protected WUR frames

A WUR AP may transmit a protected WUR frame addressed to a WUR non-AP STA that has set the Protection Support field in the WUR Capabilities element it transmits to 1; otherwise the AP shall not transmit a protected WUR frame to the STA.

A WUR AP may transmit a protected WUR frame addressed to more than one WUR non-AP STAs if all the WUR non-AP STAs have set the Protection Support field in the WUR Capabilities element they transmit to 1.

The WUR AP shall set the Protected subfield of the Frame Control field of transmitted WUR frames to 1 if the WUR frame is protected; otherwise the WUR AP shall set the Protected subfield of the Frame Control field of the WUR frame to 0.

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 466):***

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

* The WUR AP shall use BIP-CMAC-128 to provide data integrity and replay protection and shall use an integrity key, exchanged via the PCR, to compute the MIC of the WUR frame.
* Broadcast and group addressed WUR frames shall be protected using a separate wake up radio (WUR) integrity group temporal key (IGTK) that is negotiated as defined in 12.7.7 (Group key handshake) and individually addressed WUR frames shall be protected using a separate pairwise wake up radio (WUR) temporal key (TK) that is negotiated as defined in 12.7.6 (4-way handshake).*(#466)*
* 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 frame.

The AAD shall have a length of 40 bits consisting of the Frame Control, the ID field, the Embedded BSSID field of the WUR frame, and 4 reserved bits as shown in Figure 31-2 (AAD construction for WUR frames).

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

* Protected WUR frame transmission

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

* Select the appropriate integrity key associated to protected WUR frames (see 31.8 (Protected WUR frames)), Key ID that is equal to the current Key ID value, an IPN that is generated and partially included in the WUR frame as defined in 31.8.3.1 (Generation of the IPN by a WUR AP).
* Construct the AAD as defined in Figure 31-2 (AAD construction for WUR frames).
* Compute an integrity value over the concatenation of AAD, the Frame Body field (if present), and the IPN, and insert the truncated output into the MIC field of the WUR frame. The integrity value is computed using AES-128-CMAC. The 16-bit truncated output is the MIC.
* Transmit the protected WUR frame.
* Protected WUR frame reception

A WUR non-AP STA that receives a protected WUR 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 frames (see 31.8 (Protected WUR frames)), and associated state based on Key ID equal to the current Key ID value.
* Perform replay protection on the received WUR 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 31.8.3.2 (Construction of the IPN by a WUR non-AP STA). The WUR non-AP STA shall use a replay counter, *RC*, that is equal to the IPN prior to any update due to the WUR frame. If IPN is less than or equal to *RC* then the WUR non-AP STA shall discard the WUR frame and increment its internal dot11RSNAStatsCMACWURReplays counter by 1.
* Construct the AAD as defined in Figure 31-2 (AAD construction for WUR frames).
* Extract and save the received MIC value from the FCS field of the WUR 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 and increment its internal MIC error counter by 1.
* Update the *RC* for the integrity key associated to protected WUR frames identified by Key ID equal to the current Key ID value to the IPN.
* If the Common IPN subfield is equal to 1, update the local TSF timer as follows:
  + The received partial TSF timestamp, obtained from the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame, is adjusted to consider the WUR non-AP STA’s delay as shown below:
    - Create a temporary timestamp by concatenating the received partial TSF timestamp with 9 bits containing an implementation specific value that represents the assumed value of bit posi­tion 0 to 8 of temporary timestamp;
    - Add an amount equal to the receiving STA’s delay through its local PHY components plus the time since the first bit of the Partial TSF field was received at the MAC/PHY interface to the temporary timestamp
    - The adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporary timestamp.
  + If the most significant bit (MSB) of the adjusted value of the received partial TSF timestamp is not equal to the bit 16 of the local TSF timer then the value of bits 17 to 63 of the local TSF timer shall be adjusted to account for roll over as follows:
    - The value shall be increased by one unit (modulo 247) if LT [9:16] > AT and LT [9:16] > AT + 27
    - The value shall be decreased by one unit (modulo 247) if LT [9:16] < AT and LT [9:16] < AT–27

where AT is the adjusted value of the received partial TSF timestamp and LT [9:16] is the value of bits 9 to 16 of the local TSF timer

* + The bits 9 to 16 of the STA’s local TSF timer shall be set to the adjusted value of the received partial TSF timestamp.

NOTE—Before the adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporary timestamp, the temporary timestamp may be further compensated for a clock drift offset (*cdo*) between the WUR AP and the WUR non-AP STA, which is determined by multiplying the estimated clock drift (*ecd*) by the time between receiving the latest TSF from the WUR AP and the time at which the WUR frame is received from the WUR AP, where the *ecd* is determined based on two or more received TSF values from the WUR AP and comparing these to the internal TSF at the WUR non-AP STA.

* Generation and construction of IPN for WUR frames
* Generation of the IPN by a WUR AP

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 645, 806-809):***

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 each <ID, Embedded BSSID> duple 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 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 31.4.1 (General).
* The IPN shall never repeat for protected WUR frames generated using the same temporal key
* 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 temporal key and <ID, Embedded BSSID> duple.
* The IPN shall never repeat for protected WUR frames generated using the same temporal key and <ID, Embedded BSSID> duple
* 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*(#645, 806-809)*

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 338, 903, 904, 1250):***

The local (IPN) at the WUR AP is initialized to 0 when the WUR mode link is established (see 31.6.2 (WUR Mode Setup)), and the most recently transmitted WUR Operation element has the Common IPN subfield equal to 0.

The local IPN at the WUR AP is initialized to the value of the local TSF timer [9: 56] when the WUR mode link is established (see 31.6.2 (WUR Mode Setup)), and the most recently transmitted WUR Operation element has the Common IPN subfield equal to 1.*(#338, 903, 904, 1250)*

* Construction of the IPN by a WUR non-AP STA

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 645, 806-809):***

The full IPN is not present in protected WUR frames, depends on the value of the Common IPN subfield of the most recently received WUR Operation element and is constructed locally at the STA as follows:

* If the Common IPN subfield is equal to 1, the IPN 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

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

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

* The IPN=PN0||BPN where PN1||PN2||PN3||PN4||PN5 = BPN
* 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 <ID, Embedded BSSID> duple
* PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN*(#645, 806-809)*

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 905, 906, 907, 1250):***

The locally stored IPN at the WUR non-AP STA is initialized to 0 when the WUR mode link is established (see 31.6.2 (WUR Mode Setup)), and the most recently received WUR Operation element has the Common IPN subfield equal to 0.

The locally stored IPN at the WUR non-AP STA is initialized to the value of the local TSF timer [9: 56] when the WUR mode link is established (see 31.6.2 (WUR Mode Setup)), and the most recently received WUR Operation element has the Common IPN subfield equal to 1.*(#905, 906, 907, 1250)*

The BPN and the Key ID may be updated explicitly through a secure header compression request/response exchange by using only the CCMP Update field of the exchange as defined in 10.59 (Generation of PV1 MPDUs and header compression procedure).

31.9 WUR FDMA operation

A WUR non-AP STA whose dot11WURChannelSwitchImplemented is true shall set the WUR Channel Switching Support subfield of the WUR Capabilities Information field of the WUR Capabilities element that it transmits to 1.

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 1251):***

When a WUR AP receives a WUR Capabilities element of which the WUR Channel Switching subfield of the WUR Capabilities Information field is equal to 1, the WUR AP may*(#1251)* set the WUR Channel Offset subfield of the WUR Parameters field of the WUR Mode element that it transmits to any value as defined in Table 9-318c (Subfields of WUR Parameters field from WUR AP), subject to the negotiated WUR duty cycle schedule does not overlap with the TWBTTs at which the WUR AP schedules for transmission WUR…

3.4 Abbreviations and acronyms

**TGba Editor: *Insert the following acronyms as follows (#CID 466):***

WUR IGTK wake up radio integrity group temporal key

WUR TK wake up radio temporal key *(#466)*