IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment resolutions for Clause 29.10 |
| Date: 2019-08-12 |
| 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 |

Abstract

This submission proposes resolutions for multiple comments related to TGba D3.0 with the following CIDs (7 CIDs):

* 3277, 3278, 3411, 3412, 3413, 3414, 3415

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Note that CID 3278 needs to be resolved. It is a pending item as of this revision.

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** |
| 3277 | Rojan Chitrakar | 123.38 | Similar to the update of the local TSF, the locally stored PN should also be updated. | Add one more bullet:If the Common PN subfield is equal to 0, replace the local WIPN or WTPN with the locally constructed PN used to receive the WUR frame. | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested change and adds a reference to the subclause where the construction of the PN is described.TGba editor to make the changes shown in 11-19/1060r1 under all headings that include CID 3277. |
| 3278 | Rojan Chitrakar | 125.25 | At the AP side, the PN is incremented by 1 for each transmitted WUR frame (Ref: P124L46), however there is no procedure defined for the increment of the locally store PN/BPN at the non-AP STA. When the PPN in a received WUR frame is lesser than the last received PPN, it indicates a PPN roll over and as such the local BPN should be incremented by 1 before constructing the local PN, else the PN used by the AP and the non-AP STA will not be the same. | Add one more bullet:The portion of the PN corresponding to the BPN shall be incremented by 1 when the PPN in the received WUR frame is less than the local PPN. |  |
| 3411 | Yunsong Yang | 121.18 | Protected WUR Frame Support subfield value should be verified in the security context during 4-way handshake or Re(Association) procedure. Therefore, it is more important for both the WUR AP and WUR non-AP STA to indicate its capability of protected WUR frame support by including the Protected WUR Frame Support subfield in the RSN Extension element (RSNXE) that is newly created in the REVmd. | Add the Protected WUR Frame Support subfield to the Extended RSN Capabilities field in the RSN Extension element that is newly created in the REVmd. Change "the WUR Capabilities element" on both P121L18 and P121L22 to "the RSNXE". | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested changes of replacing WUR Capabilities element with RSNXE. Note that not all changes are accounted in this document, since other changes pertaining to other subclauses are addressed in another document (see 11-19/1430). TGba editor to make the changes shown in 11-19/1060r1 under all headings that include CID 3411. |
| 3412 | Yunsong Yang | 121.26 | WUR frame protection being negotiated should also be conditioned on that the capability of protected WUR frame support of the other party is successfully verified in the security context during 4-way handshake or (Re)Association procedure. | Add the Protected WUR Frame Support subfield to the Extended RSN Capabilities field in the RSN Extension element that is newly created in the REVmd. Change "respective WUR Capabilities elements" on L26 to "respective RSNXEs". And add the following to the end of this paragraph (before the period): ", and it is successfully verified that the WUR Frame Protection Support subfield is 1 in the Extended RSN Capabilities field in the RSNXE received during the 4-way handshake, FT 4-way handshake, FT fast BSS transition protocol, or the (Re)Association Request and (Re)Association Response frames of FILS authentication. Otherwise, WUR frame protection is not negotiated between the WUR AP and the WUR non-AP STA". | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested changes, with some additional clarifications to the sentence to make it clearer. Note that not all changes are accounted in this document, since other changes pertaining to other subclauses are addressed in another document (see 11-19/1430). TGba editor to make the changes shown in 11-19/1060r1 under all headings that include CID 3412. |
| 3413 | Yunsong Yang | 122.22 | The abbreviation of "WUR integrity group temporal key (IGTK)" and "WUR temporal key (TK)" have been defined in the draft and this location is not the first place that these two terms appear in the draft. Therefore, we should just use the abbreviations of WIGTK and WTK here. And both keys are distinct from all legacy key. Therefore, the word "separate" in both sub-bullets are redundant. | Change the sub-bullet on L22 to read: "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);". And change the sub-bullet on L26 to read: "Individually addressed WUR Wake-up frames shall be protected using a WTK that is negotiated as defined in 12.7.6 (4-way handshake)." | Accepted |
| 3414 | Yunsong Yang | 122.33 | The sequence of the components of the AAD construction is inconsistent with Figure 29-2. | Change the bullet to read: "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, 4 reserved bits, and the Embedded BSSID field, which is equal to the 16 MSBs of the compressed BSSID (see 29.5.2 (Compressed BSSID)), as shown in Figure 29-2 (AAD construction for WUR frames)." | Accepted |
| 3415 | Yunsong Yang | 124.55 | The "Common IPN field" is referred to as the "Common PN field" in other places. Need to use a common term for this field. | Change "Common IPN field" to "Common PN field" on L55 and L61. | Accepted |

**Discussion: *None.***

* Protected WUR frames

WUR frame protection cannot be applied until the PTKSA (see 12.6.1.1.6 PTKSA) and WIGTKSA (12.6.1.1.11 (WIGTKSA)) have been established.

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 3411):***

WUR frame protection is enabled when dot11RSNAWURFrameProtectionActivated is true, and is disabled otherwise. When WUR frame protection is enabled at a WUR AP, the WUR AP shall advertise such capability by setting to 1 the Protected WUR Frame Support subfield of the RSNXE in its Beacon and Probe Response frames. When WUR frame protection is enabled at a WUR non-AP STA, the WUR non-AP STA shall indicate such capability by setting to 1 the Protected WUR Frame Support subfield of the RSNXE in its (Re)Association Request frames.*(#3411)*

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 3412):***

WUR frame protection shall be considered as successfully negotiated between the WUR AP and the WUR non-AP STA if management frame protection is negotiated, both parties set the Protected WUR Frame Support subfield to 1 in their respective RSNXEs in the (re)association procedure, and it is successfully verified that the WUR Frame Protection Support subfield is equal to 1 in the Extended RSN Capabilities field in the RSNXE received during the 4-way handshake, FT 4-way handshake, FT fast BSS transition protocol, or (re)association procedure of FILS authentication. Otherwise, WUR frame protection shall not be considered as successfully negotiated.*(#3412)*

If WUR frame protection is negotiated between a WUR AP and a WUR non-AP STA, the WUR AP may transmit a protected individually addressed WUR Wake-up frame or a protected broadcast or group addressed WUR Wake-up frames to the WUR non-AP STA; otherwise the AP shall not transmit a protected WUR Wake-up frame to the WUR non-AP STA. If a WUR non-AP STA negotiated WUR frame protection for an association, it shall discard any unprotected WUR Wake-up frames received from the WUR AP associated. If the non-AP STA did not negotiate WUR frame protection for an association, it shall discard any protected WUR Wake-up frames received from the WUR AP.

The WUR AP may transmit a protected WUR Wake-up frame addressed to more than one WUR non-AP STAs if WUR frame protection is negotiated with, and the WIGTK has been transported to, all the WUR non-AP STAs that are being addressed.(#3013)

NOTE—If the WUR non-AP STAs associated with a WUR AP consist of both WUR non-AP STAs that negotiated WUR frame protection and WUR non-AP STAs that did not negotiated WUR frame protection, the WUR AP can transmit a protected broadcast addressed WUR Wake-up frame and an unprotected broadcast addressed WUR Wake-up frame, in order to wake up all associated WUR non-AP STAs. If a WUR AP assigns a group ID to both WUR non-AP STAs that negotiated WUR frame protection and WUR non-AP STAs that did not negotiated WUR frame protection, the WUR AP can transmit a protected group addressed WUR Wake-up frame and an unprotected group addressed WUR Wake-up frame, both containing that group ID, in order to wake up that group of WUR non-AP STAs.

The WUR AP shall not transmit a protected individually addressed WUR Wake-up frame to the WUR non-AP STA until the WTK is installed at the WUR non-AP STA, and should not transmit a protected broadcast or group addressed WUR Wake-up frame until the WIGTK is installed at all WUR non-AP STAs, with which the WUR AP has negotiated WUR frame protection. The WUR non-AP STA shall discard any protected WUR frames received before the WTK and WIGTK are installed.

A WUR AP that installs the WTK for a WUR non-AP STA (see 12.7.6 (4-way handshake)) shall use the WTK to protect all subsequent individually addressed WUR wake-up frames transmitted to the WUR non-AP STA. A WUR AP that installs the WIGTK (see 12.7.6 (4-way handshake) or 12.7.7 (Group key handshake)) shall use the WIGTK to protect all subsequent protected broadcast or group addressed WUR wake-up frames.

A WUR non-AP STA that installs the WTK (see 12.7.6 (4-way handshake)) shall use the WTK to process all subsequently received protected individually addressed WUR wake-up frames. A WUR non-AP STA that installs the WIGTK (see 12.7.6 (4-way handshake) or 12.7.7 (Group key handshake)) shall use the WIGTK to process all subsequently received protected broadcast or group addressed WUR wake-up frames.

The WUR AP shall set the Protected subfield of the Frame Control field of transmitted WUR Wake-up 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.

A WUR STA with dot11RSNAWURFrameProtectionActivated equal to true shall set dot11RSNAProtectedManagementFramesActivated to true.

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 3413, 3414):***

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*(#3413)* 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*(#3413)* 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, 4 reserved bits, and the Embedded BSSID field, which is equal to the 16 MSBs of the compressed BSSID (see 29.5.2 (Compressed BSSID)), as shown in Figure 29-2 (AAD construction for WUR frames).*(#3414)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 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 29.10 (Protected WUR frames)), Key ID that is equal to the corresponding WIGTK or WTK Key ID value, a WUR PN that is generated and partially included in the WUR frame as defined in 29.10.3.1 (Generation of the PN by a WUR AP).
* Construct the AAD as defined in Figure 29-2 (AAD construction for WUR frames).
* Compute an integrity value over the concatenation of AAD, the Frame Body field (if present), and the WUR PN, and insert the 16-bit truncated output, which is the MIC, into the FCS field of the WUR frame. The integrity value is computed using AES-128-CMAC.
* Transmit the protected WUR frame.
* Protected WUR frame reception

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 3277):***

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 29.10 (Protected WUR frames)), and associated state based on Key ID equal to the corresponding WIGTK or WTK 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 PN locally as defined in 29.10.3.2 (Construction of the PN by a WUR non-AP STA), and the WUR non-AP STA shall maintain a separate replay counters (RC) for each WIGTK and WTK when the most recently received WUR Operation element has the Common PN subfield equal to 0. The WUR non-AP STA shall initialize the replay counter to the initial value of the corresponding PN 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 PN when it resets the WIGTK or WTK. If PN is less than or equal to 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.
* Construct the AAD as defined in Figure 29-2 (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 PN. 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.
* Update the *RC* for the integrity key associated to protected WUR Wake-up frames identified by Key ID equal to the corresponding WIGTK or WTK Key ID value with the corresponding PN.
* If the Common PN 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 WUR non-AP 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) (modulo 28))

— The value shall be decreased by one unit (modulo 247) if LT [9:16] < AT and LT [9:16] < ((AT–27) (modulo 28))

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 WUR non-AP STA’s local TSF timer shall be set to the adjusted value of the received partial TSF timestamp.
* If the Common PN subfield is equal to 0, update the local WIPN or WTPN to the locally constructed PN used to receive the WUR frame (see 29.10.23.2 (Constuction of the PN by a WUR non-AP STA))*(#3277)*

NOTE 1—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 between the WUR AP and the WUR non-AP STA, which is determined by multiplying the estimated clock drift 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 estimated clock draft 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.

NOTE 2—When the most recently received WUR Operation element has the Common PN subfield equal to 1, only a single common replay counter is maintained for both WIGTK and WTK.

* Generation and construction of PN for WUR frames

The PN for WIGTK is defined as WIPN and the PN for WTK is defined as WTPN. When the Common PN subfield in the WUR Operation element sent by the WUR AP is equal to 1 then WIPN and WTPN are derived in the same way and are equal.

* Generation of the PN by a WUR AP

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

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

* If the Common PN subfield is equal to 1:
* PN = PN0||PN1||PN2||PN3||PN4||PN5 = TSF timer [9: 56], where the TSF timer is obtained as defined in 29.6.1 (General).
* The PN shall never repeat for protected WUR frames generated using the same WIGTK or WTK
* The WUR AP shall include PN0, i.e., the PPN, which is equal to its TSF timer [9: 16], in the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame
* If the Common PN subfield is equal to 0:
* PN = PN0||PN1||PN2||PN3||PN4||PN5, where PN shall be incremented by one for each transmitted WUR frame using the same WIGTK or WTK.
* The PN shall never repeat for protected WUR frames generated using the same WIGTK or WTK
* 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 broadcast addressed

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 3415):***

If the most recently transmitted WUR Operation element has the Common PN*(#3415)* subfield equal to 0, the local WTPN at the WUR AP is initialized to 0 and the local WIPN at the WUR AP is initialized to the WIPN provided in the WIGTK KDE (Figure 12-47a (WIGTK KDE)) when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)).

If the most recently transmitted WUR Operation element has the Common PN*(#3415)* subfield equal to 1,the local WTPN and WIPN at the WUR AP, which are the same in this case, are initialized to the value of the local TSF timer [9: 56] when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)).

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

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

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

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

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

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

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

If the most recently received WUR Operation element has the Common PN subfield equal to 0, the locally stored WTPN at the WUR non-AP STA is initialized to 0 and the local WIPN at the WUR non-AP STA is initialized to the WIPN provided in the WIGTK KDE (Figure 12-47a (WIGTK KDE)) when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)).

If the most recently received WUR Operation element has the Common PN subfield equal to 1, the locally stored WTPN and WIPN, which are the same in this case, at the WUR non-AP STA is initialized to the value of the local TSF timer [9: 56] when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)).

If 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(#3279, #3265, #3280, #3282, #3284)).(#3279, #Ed)

* WUR PN update procedure(#3279, #3265, #3280, #3282, #3284)

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.(#3281)

If 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, #Ed)

If 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, #Ed)

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)

If 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, #Ed)

* 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 subfields of the WUR Parameters field in the WUR Mode element may be omitted.(#Ed)