IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed spec text for WUR frame format | | | | |
| Date: 2018-08-27 | | | | |
| 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 |
| Soo Bum Lee | Qualcomm Inc. |  |  |  |
| Jouni Malinen | Qualcomm Inc. |  |  |  |
| George Cherian | Qualcomm Inc. |  |  |  |
| Menzo Wentink | Qualcomm Inc. |  |  |  |
| Po-Kai Huang | Intel |  |  |  |

Abstract

This submission proposes draft for secure WUR frames.

Revisions:

* Rev 0: Initial version of the document. Contains changes to the spec to fix some remaining TBDs for the secure WUR frames, for VL WUR frames, added spec text for a passed motion, and some editorials here and there.
* Rev 1: Incorporated suggestions during the presentation and removed changes related to the Frame Body field format for VL WUR Wake Up frames. Changes in green.

**Straw Poll 1: Do you support to adopt the spec changes as shown in doc 11-18/1599r1?**

**Result: 3Y, 0N, 3A.**

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.***

**9.10 MAC frame format for WakeUp Radio (WUR) frames**

**9.10.1 Basic components**

Each Wake-Up Radio (WUR) frame consists of the following basic components:

—A *MAC header*, which comprises frame control, address, and type dependent (TD) control fields;

—A variable-length *frame body*, which, if present, contains information specific to the frame *type*;

—An *FCS*, which contains either a 16-bit CRC or a 16-bit MIC.

9.10.2 General WUR frame format

Figure 9-747a (WUR frame format) depicts the general MAC frame format for WUR frames.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0   B7 | B8  B19 | B20  B31 |  |  |
|  | Frame Control | Address | TD Control | Frame  Body | FCS |
| Bits: | 8 | 12 | 12 | variable | 16 |
| * WUR frame format | | | | | |

The MAC header of the WUR frame consists of the Frame Control, Address, and TD Control fields, and is defined in 9.10.2.1 (MAC header).

The Frame Body field is optionally present in certain WUR frame types and is defined in 9.10.2.4 (Frame Body field).

The FCS field is defined in 9.10.2.5 (Frame Check Sequence (FCS) field).

The MAC header and the last field (FCS) constitute the minimal WUR frame format and are present in all WUR frames, including reserved types.

A WUR frame that does not have a Frame Body field is referred to as a minimal-length (ML) WUR frame. A WUR frame that has a Frame Body field is referred to as a variable-length (VL) WUR frame.

NOTE—An ML WUR frame can be sent to any WUR STA while a VL WUR frame can only be sent to a WUR STA that has declared support of its reception (see X.Y.Z).

**9.10.2.1 MAC header**

**9.10.2.1.1 Frame Control field**

The format of the Frame Control field is illustrated in Figure 9-747b (Frame Control field format of WUR frame).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0   B2 | B3 | B4  B6 | B7 |
|  | Type | Length Present | Length/Misc | Protected |
| Bits: | 3 | 1 | 3 | 1 |

The Type field indicates the type of the WUR frame, as defined in Table 9-429a (WUR frame types).

|  |  |
| --- | --- |
| * WUR frame types | |
| Type | Type description |
| 0 | WUR Beacon |
| 1 | WUR Wake Up |
| 2 | WUR Vendor Specific |
| 3 | WUR Discovery |
| 4-7 | Reserved |

The Length Present field indicates whether the Length/Misc field contains the Length field or not.

The Length/Misc field contains the Length field when the Length Present field is set to 1 and the Misc field when the Length Present field is set to 0.

The Length field contains the length of the Frame Body field as defined in 9.10.2.4 (Frame Body field). The Misc field is reserved unless explicitly stated otherwise.

The Protected field indicates whether the information carried in the WUR frame has been processed by a message integrity check (MIC) algorithm. The Protected field is set to 1 if the WUR frame is protected uti­lizing the MIC algorithm as defined in 31.8 (Protected WUR frames); otherwise it is set to 0.

9.10.2.2 Address field

The Address field contains an identifier for the WUR frame, which is selected from Table 9-429b (Identifi­ers of WUR frames). The identifier depends on the type of WUR frame (see 9.10.3 (Format of individual WUR frame types)).

|  |  |
| --- | --- |
| * Identifiers of WUR frames | |
| Address field | Identifier description |
| Transmit ID | Identifier of the transmitting AP (see 31.3.2 (Transmit ID)) |
| Group ID | Identifier of a group of receiving WUR STAs (see 31.3.3(Group ID)) |
| WUR ID | Identifier of an individual receiving WUR STA (see 31.3.4 (WUR ID)) |
| OUI1 | The 12 MSBs of the OUI (see 9.4.1.31 (Organization Identifier field)) |

9.10.2.3 TD Control field

The Type Dependent (TD) Control field contains control information that depends on the WUR frame type (see 9.10.3 (Format of individual WUR frame types)).

9.10.2.4 Frame Body field

The Frame Body field is a variable-length field that contains information specific to individual WUR frame types.

The Frame Body field is not present when the Length Present subfield of the Frame Control field is 0 (i.e., within ML WUR frames) and is present when the Length Present subfield of the Frame Control field is 1 (i.e., within VL WUR frames).

The length of the Frame Body field is in units of octets and is equal to 2 x (*L* + 1), where *L* is the value of the Length subfield in the Frame Control field. The minimum length and the maximum length of the Frame Body field are 2 octets and 16 octets, respectively.

**9.10.2.5 Frame Check Sequence (FCS) field**

**9.10.2.5.1 General**

The FCS field contains a 16-bit CRC when the Protected subfield in the Frame Control field is 0 and con­tains a 16-bit MIC when the Protected subfield in the Frame Control field is 1.

The CRC is calculated as defined in 9.10.2.5.2 and the MIC is calculated as defined in 31.8.

**9.10.2.5.2 Cyclic Redundancy check (CRC)**

The CRC is calculated over all the fields of the Frame Control, Address, TD Control, Frame Body field (if present), and Embedded BSSID field (if present). These fields are referred to as the *calculation fields*.

NOTE 1—The Embedded BSSID field, if present, is part of the *calculation fields* but is not part of the fields of the WUR frame transmitted over the *WM*.

NOTE 2 —The Frame Body field is present in the *calculation fields* only when the WUR frame is a VL WUR frame (see 9.10.2.4 (Frame Body field)); otherwise, the Frame Body field is not present.

The Embedded BSSID field, if present, is the last field of the *calculation fields*. The Embedded BSSID field is 16 bits in length and contains the 16 LSBs of the compressed BSSID, which is defined in 31.3.1 (General).

The CRC is the 1s complement of the remainder generated by the modulo 2 division of the *calculation fields* by the polynomial *x16+x12+x5+1*, where the shift-register state is preset to all 1s.

NOTE—The order of transmission of bits within the FCS field is defined in 9.2.2 (Conventions).

The *calculation fields* are processed in the order they would have been transmitted.

A schematic of the CRC processing is shown in Figure 9-747c (CRC-16 implementation for WUR MPDUs), where the SERIAL DATA INPUT consists of the *calculation fields (BL, BL-1…, B1, B0),* with *BL* being the most significant bit of the *calculation fields*. The CRC computation and transmission is the same as the one depicted in Figure 16-3 (CRC-16 implementation).



**Figure 9-747c – CRC-16 implementation for WUR MPDUs**

**9.10.3 Format of individual WUR frame types**

**9.10.3.1 WUR Beacon frame format**

The frame format of the WUR Beacon frame is as defined in Figure 9-747a (WUR frame format).

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

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.

**9.10.3.2 WUR Wake Up frame format**

The frame format of the WUR Wake Up frame is as defined in Figure 9-747a (WUR frame format).

The Frame Control field is as defined in 9.10.2.1.1 (Frame Control field), with the Length Present subfield set to 1 if the Frame Body field is present and the Length Present subfield set to 0 otherwise.

The Address field of the WUR Wake Up frame contains a WUR ID if the Wake Up frame is individually addressed, a group ID if the frame is group addressed and the transmit ID if the frame is broadcast.The TD Control field of a WUR Wake Up frame contains the Counter subfield and the Sequence Numbersub­field as defined in Figure 9-963d (TD Control field of WUR Wake Up frame).

The Counter subfield :

* Contains the BSS Update Counter field if the WUR Wake Up frame is broadcasted. The BSS Update Counter field is defined as an unsigned integer initialized to 0, that incre­ments when a critical update to the PCR’s BSS parameters has occurred,
* Contains the 4 LSBs of the PPN (see 31.8 (Protected WUR frames)) if the WUR Wake Up frame is not broadcast, the Protected field in the Frame Control field is 1 and the most recently sent WUR Operation element has the Common IPN subfield equal to 0,
* Is reserved otherwise.

The Sequence Number subfield:

* Contains the TSF timer [9: 16] if the Protected field in the Frame Control field is 1 and the most recently sent WUR Operation element has the Common IPN subfield equal to 1. The TSF timer is obtained as defined in 31.4.1 (General),
* Contains the 8 MSBs of the PPN (see 31.8 (Protected WUR frames)) if the WUR Wake Up frame is not broadcasted the Protected field in the Frame Control field is 1 and the most recently sent WUR Operation element has the Common IPN subfield equal to 0,
* Is reserved otherwise.

The Misc field of the broadcast WUR Wake Up frame contains the Group Addressed BU subfield and Reserved subfield as defined in Table 9-963e (Misc field of broadcast WUR Wake Up frame).

**Figure 9-963e—Misc field of broadcast WUR Wake Up frame**

The Group Addressed BU subfield is set to 1 when an AP has buffered group addressed BU(s). Otherwise, the Group Addressed BU subfield is set to 0.**9.10.3.3 WUR Discovery frame format**

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

The Protected subfield in the Frame Control field is reserved.

The format of the Frame Body field is as defined in Figure 9-747e (Frame Body Field format of WUR Discovery frame).

The Compressed SSID field contains 16 LSBs of the Short-SSID as defined in 9.4.2.171.2 (Calculating the Short-SSID).

The PCR Operating Channel field contains operating class and channel information as defined in 9.4.1.22 (Operating Class and Channel field).

9.10.3.4 WUR Vendor Specific frame format

The frame format of the WUR Vendor Specific frame is as defined in Figure 9-747a (WUR frame format).

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

The Protected subfield in the Frame Control field contains vendor specific information that is out of scope of the standard.

The Misc subfield in the Frame Control field, if present, contains vendors specific information that is out of scope of the standard.

The Address field is set to the 12 MSBs of the OUI (see 9.4.1.32 (Organization Identifier field)).

The TD Control field is set to the 12 LSBs of the OUI.

The Frame Body field, if present, contains vendor specific information that is out of scope of the standard.

**31.3 Setting the identifiers of WUR frames**

**31.3.1 General**

The Address field of WUR frames contains an identifier (ID) that is selected from the range 0 to 4095. Each identifier can be a transmit ID, which is obtained from the compressed BSSID (see 31.3.2 (Transmit ID)), group ID (see 31.3.3 (Group ID)), or a WUR ID (see 31.3.4 (WUR ID)).

The compressed BSSID is equal to the 32-bit CRC calculated over the BSSID contained in Beacon frames transmitted by the WUR AP (calculation is performed as defined in 9.2.4.8 (FCS field) where the BSSID is the *calculation fields*).

**31.3.2 Transmit ID**

A transmit ID identifies the AP transmitting the WUR frame. A WUR frame with transmit ID in the Address field is a broadcast WUR frame that is addressed to all the WUR STAs that are associated with the transmitting AP.

A WUR AP shall use the 12 MSBs of the compressed BSSID as the transmit ID of WUR frames it transmits.

**31.3.3 Group ID**

A group ID identifies a group of one or more WUR STAs and is selected from a group ID space, obtained from the identifier’s space. A WUR frame with group ID in the Address field is a group addressed WUR frame that is addressed to all the WUR STAs identified by that group ID.

The WUR AP shall ensure that the lowest group ID of the group ID space is randomly selected from the identifiers’s space.

A WUR AP may assign one or more group IDs to a WUR STA that has set the Supported Group IDs field of the WUR Capabilities element it transmits to a nonzero value. The AP shall not assign a group ID to a WUR STA that has set the Supported Group IDs field of the WUR Capabilities element it transmits to zero.

The WUR AP shall indicate the group IDs assigned to a WUR STA in the Group ID List subfield of the WUR Parameters field of the WUR Mode element that is sent to the STA. The AP shall ensure that the difference between the largest group ID and the lowest group ID assigned to the WUR STA does not exceed the value indicated in the Supported Group IDs field of the WUR Capabilities element sent by the WUR STA, where the comparison performed between the two identifiers is circular modulo *212.*

A WUR STA that has indicated support for group IDs shall obtain the assigned group IDs from the Group ID List field of the most recent WUR Mode element received from the WUR AP.

**31.3.4 WUR ID**

A wake-up radio (WUR) ID identifies the WUR STA that is the intended recipient of the WUR frame. A WUR frame with WUR ID in the Address field is an individually addressed WUR frame that is addressed to the WUR STA identified by that WUR ID.

A WUR AP shall assign to each WUR STA a WUR ID that uniquely identifies the WUR STA within the BSS of the AP. The AP shall either select the WUR ID randomly from the identifier’s space or calculate the WUR ID as *AID* + *transmit ID*, where the *AID* is the association identifier of the STA, the *transmit ID* is defined in 31.3.2 (Transmit ID) and the addition performed between the two identifiers is circular modulo *212*. The AP shall indicate the WUR ID assigned to a WUR STA in the WUR ID field of the WUR Mode element it sends to the STA.

A WUR STA shall obtain the WUR ID from the WUR ID field of the most recent WUR Mode element received from the WUR AP.

A WUR AP that generates a WUR Wake Up frame that contains a Frame Body field with one or more STA Info fields shall order the STA Info fields so that the WUR IDs appear in increasing order. The AP shall not include the WUR ID of a WUR STA that does not support reception of VL WUR frames.

A WUR STA that supports reception of VL WUR frames may discard a received VL WUR Wake Up frame if either of the following is true:

* Immediately after locating a WUR ID field in the Frame Body field that is greater than the WUR ID assigned to it and no WUR ID equal to the WUR ID assigned to it was identified prior to it,
* Immediately after locating the last WUR ID field in the Frame Body field and the WUR ID is less than the WUR ID assigned to it.

31.8 Protected WUR frames

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

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

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

The 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 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 WUR IGTK that is negotiated as defined in 12.7.7 (Group key handshake) and individually addressed WUR frames shall be protected using a separate WUR TK that is negotiated as defined in 12.7.6 (4-way handshake).
* The CMAC output for BIP-CMAC-128 shall be truncated to 16 bits: MIC = Truncate-16 (CMAC Output). shall beincludedThe AAD shall have a length of 40 bits consisting of the Frame Control, the Address field, the Embed­ded BSSID field of the WUR frame, and 4 reserved bits shall be obtained as shown in Figure 31-2 (AAD construction for WUR MPDUs).

**31.8.1 Protected WUR frame transmission**

An AP that sends a protected WUR frame shall follow the rules in 12.5.4.5 (BIP transmission) except that the 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, and 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 MPDUs).
* 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.

**31.8.2 Protected WUR frame reception**

A WUR STA that receives a protected WUR frame shall follow the rules in 12.5.4.6 (BIP reception) except that the STA shall:

* Use the appropriate integrity key associated to protected WUR frames (see 31.8 (Protected WUR frame)), 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 STA shall construct the IPNlocally as defined in 31.8.3.2 (Construction of the IPN by a WUR STA). The STA shall use a replay counter, RC, that is equal to the IPN prior to any update due to the WUR frame. If IPNis less than or equal to RCthen the 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 MPDUs).
* 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 field is equal to 1, update the local TSF timer as follows:
  + - The received partial TSF timestamp, obtained from the Sequence Number subfield of the TD Control field of the WUR Wake Up frame, is adjusted to consider the WUR 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 temporal 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 temporal timer
      * The adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporal 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.

**31.8.3 Generation and construction of IPN for WUR frames**

**31.8.3.1 Generation of the IPN by a WUR AP**

A WUR AP that intends to transmit protected WUR frames shall set the Common IPN field in the WUR Operation element it transmits to 0 if it intends to maintain separate IPN counters for each <Address, Embedded BSSID> couple and shall set the Common IPN field to 1 if it intends to maintain a common IPN for all protected WUR frames generated within its BSS.

DISCUSSION NOTE: The granularity of the TSF timer included in the WUR frame with the below option is 512 us which means the AP cannot send bursts of high data rate WUR frames, since the PN shall never repeat. Another option is to shift to 5-15 which would give a granularity of 256 us which is less than the shortest WUR frame, as such this issue does not occur.

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

* If the Common IPN field 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 AP shall include PN0 (i.e., the PPN), which is equal to its TSF timer [9: 16], in the Sequence Number subfield of the TD Control field of the WUR Wake Up frame
* If the Common IPN field 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 <Address, Embedded BSSID> couple.
  + The IPN shall never repeat for protected WUR frames generated using the same temporal key and <Address, Embedded BSSID> couple
  + The AP shall include PN0||PN1[0:3] (i.e., the PPN) in the TD Control field of the WUR Wake Up frame, if the WUR Wake Up frame is not broadcasted

The local BPN at the WUR AP is initialized to 0 when the link is established and the most recently received WUR Operation element had the Common IPN subfield equal to 0.

The local BPN at the WUR AP is initialized to the value of the local TSF timer [9: 56] when the link is established and the most recently received WUR Operation element had the Common IPN subfield equal to 1.

**31.8.3.2 Construction of the IPN by a WUR STA**The full IPN is not present in protected WUR frames, depends on the value of the Common IPN field 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 TD Control field of the WUR Wake Up frame
    - BPN is set as the 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 PPN||BPN, where PPN is equal to the value of the TD Control field of the received WUR frame, and BPN is retrieved from the locally stored BPN at the receiver for the <Address, Embedded BSSID> couple
    - PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN

The locally stored BPN at the WUR STA is initialized to 0 when the link is established and the most recently received WUR Operation element had the Common IPN subfield equal to 0.

The locally stored BPN at the WUR STA is initialized to the value of the local TSF timer [9: 56] when the link is established and the most recently received WUR Operation element had the Common IPN subfield equal to 1.

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 10.54 (Generation of PV1 MPDUs and header compression procedure).