IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed spec text for WUR frame format |
| Date: 2018-05-01 |
| 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. |  |  |  |

Abstract

This submission proposes draft for secure WUR frames.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Incorporated feedback received from Rojan. Changes in green.
* Rev 2: Added motion text below
* Rev 3: With motion results.

**MOTION: Move to incorporate the proposed changes provided in document 11-18/0835r1 in the Draft 0.3 of TGba?**

**MOVED: Alfred Asterjadhi SECOND: Po-Kai Huang**

**Result: Passes with unanimous consent.**

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.***

* MAC frame format for Wake Up Radio (WUR) frames

9.10.1 Basic components

**TGba Editor: *Change the paragraphs below of this subclause as follows (#NO CID):***

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.
* General WUR frame format
* MAC header
* Frame Control field

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

**TGba Editor: *Change the figure below as follows (#NO CID):***

|  |  |  |  |
| --- | --- | --- | --- |
|  | B0   BX | BX+1  BY | B7 |
|  | Type | Length/Misc | Protected |
| Bits: | 3-4 | 3-4 | 1 |
| * Frame Control field format of WUR frame
 |

**TGba Editor: *Insert the paragraph below at the end of this subclause as follows (#NO CID):***

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.X (Secure WUR frames); otherwise it is set to 0.

* Frame Check Sequence (FCS) field

**TGba Editor: *Change the paragraphs below of this subclause as follows (#NO CID):***The FCS field contains a *TBD*-bit CRC. The FCS 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—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*.

The Frame Body field is present in the *calculation fields* only when the WUR frame is a variable-length WUR frame (9.10.2.4 (Frame Body field)); otherwise, the Frame Body field is not present.

The Embedded BSSID field is present in the *calculation fields* only for WUR frames that are post-association WUR frames; otherwise the Embedded BSSID field is not present. The Embedded BSSID field, if present, is the last field of the *calculation fields*. The size and contents of the Embedded BSSID field is *TBD*.

The FCS is the 1s complement of the remainder generated by the modulo 2 division of the *calculation fields* by the polynomial *TBD*, 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.

NOTE—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*.

A schematic of the processing is shown in Figure X (CRC-*TBD* implementation), 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*.

NOTE – THE CRC in the FCS is one of the CRC-8, CRC-16, or CRC-32. Which of these ones is still *TBD*.The FCS field contains a 16-bit CRC when the Protected field in the Frame Control field is 0 and contains a 16-bit MIC when the Protected field in the Frame Control field is 1.

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—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*.

The Frame Body field is present in the *calculation fields* only when the WUR frame is a variable-length WUR frame (see 9.10.2.4 (Frame Body field)); otherwise, the Frame Body field is not present.

The Embedded BSSID field is present in the *calculation fields* only for WUR frames that are post-association WUR frames; otherwise the Embedded BSSID field is not present. The Embedded BSSID field, if present, is the last field of the *calculation fields*. The size and contents of the Embedded BSSID field is TBD.

The CRC is the 1s complement of the remainder generated by the modulo 2 division of the *calculation fields* by the polynomial TBD, where the shift-register state is preset to all 1s. The MIC is generated as defined in 31.X (Secure WUR frames).

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 X (CRC-TBD implementation), 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*. A schematic of the MIC processing is shown in Figure Y (MIC-16 implementation for WUR MPDUs).

NOTE – THE CRC in the FCS is one of the CRC-8, CRC-16, or CRC-32. Which of these ones is still *TBD*.

* WUR Discovery frame format

**TGba Editor: *Insert the paragraph below in the appropriate location (#NO CID):***The FCS field contains a *TBD*-bit CRC. The FCS 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*.

The Protected subfield in the Frame Control field is reserved.

* WUR Vendor Specific frame format
* **TGba Editor: *Insert the paragraph below in the appropriate location (#NO CID):***The FCS field contains a *TBD*-bit CRC. The FCS 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*.

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

**TGba Editor: *Insert the subclause below (#NO CID):***The FCS field contains a *TBD*-bit CRC. The FCS 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*.

31.X 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. The MIC field is contained in the FCS field of the protected WUR frame.

The CMAC output for BIP-CMAC-128 shall be truncated to 16 bits: *MIC = Truncate-16 (CMAC Output)*.

The AAD has a length of 40 bits and shall consist of the Frame Control, the Address field, and the Embedded BSSID field of the WUR frame.The AAD is shown in Figure 31.AA (AAD construction for WUR MPDUs)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0   B7 | B8   B19 | B20 B23 | B24 B39 |
|  | Frame Control | Address | Reserved | Embedded BSSID |
| Bits: | 8 | 12 | 4 | 16 |

Figure 31-AA—AAD construction for WUR MPDUs

**31.X.1 Protected WUR frame transmission**

**AA Discussion:** The contents of the TD Control field of WUR Wake Up frames are not defined, as such how to obtain the IPN is left as TBD.

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, Key ID that is equal to 0, an IPN that is *TBD*.
* Construct the AAD as defined in 31.X.
* Compute an integrity value over the concatenation of AAD, and the Frame Body field (if present), 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.X.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, and associated state based on Key ID equal to 0.
* 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 *IPN* using a *TBD* method. The STA shall use a replay counter, *RC*, that is equal to *TBD*. If *IPN* is less than or equal to *RC* then the STA shall discard the WUR frame and increment its internal replay counter by 1.
* Construct the AAD as defined in 31.X.
* Extract and save the received MIC value from the FCS field of the WUR frame and compute a verifier over the concatenation of AAD and Frame Body field (if present). If the result does not mach 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 0 to the *IPN*.

**Straw Poll 1: Do you support to incorporate the spec text provided in 11-18/0835r1 and its inclusion to the latest TGba draft (D0.3)?**

**Result: 9Y, 0N, 3A.**