IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions to LB243 CIDs related to Protected WUR frames |
| Date: 2019-11-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Yunsong Yang | Self |  |  | yunsongyang1@gmail.com |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |

Abstract

This contribution proposes resolutions to resolve 6 LB243 comments (CIDs 4053 to 4058) related to the Protected WUR frames.

Revisions:

* Rev 0: Initial version of the document.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4053 | 27.22 | It is unclear as to when the WUR AP and WUR non-AP STA agree on using WUR Wake-up frames. If this occurs after the frame sequence to establish the WUR mode, which results in the WRU AP and WUR non-AP STA being in WUR mode, how is the required 4-way to be performed by a WUR non-AP STA in WUR mode, where it does not transmit or receive non-WUR PPDUs? | Clarify when the 4-way hand shake occurs, so that it is understood that the WUR AP and WUR non-AP STA are not in WUR mode when this had shake happens. | **Revised.**The timing sequence of association, EAP authentication, 4-way handshake, and unblocking 802.1X Controlled Port is described in the baseline standard subclause 4.10.3.2. The 4-way handshake can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the 4-way handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the 4-way handshake (in which case message 1 of the 4-way handshake, which is encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The concern that the 4-way handshake can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4053. |

**Discussion:**

First of all, inserting the new bullet in question doesn’t affect the timing of when the 4-way handshake occurs. The sequence of events regarding association, EAP authentication, 4-way handshake, and unblocking the 802.1X Controlled Port is clearly described in REVmd subclause 4.10.3.2.

The commenter seemingly considers that entering the WUR mode by the WUR non-AP STA means that the WUR non-AP STA is unable to transmit or receive regular 802.11 frames, citing (during offline discussion) the following definition of the WUR mode in subclause 3.2 as a support for such a view:

“**wake-up radio (WUR) mode:** A negotiation status between a WUR AP and a WUR non-AP STA in which the WUR power state of the WUR non-AP STA alternates between the WUR awake state and the WUR doze state based on the negotiated WUR parameters.”

Therefore, the commenter is concerned that the 4-way handshake can not be completed if the WUR non-AP STA successfully negotiates its WUR mode during association.

First, in P802.11ba D4.0, Table 29-1 (P114), “Status …” column indicates that the WUR non-AP STA enters the WUR mode after receiving a “successful” Enter WUR Mode response. However, such a status bears no weight on whether the WUR non-AP STA can receive the regular 802.11 frame or not. In fact, it states the following on P118L26 in P802.11ba D4.0:

“NOTE 1—A WUR non-AP STA can be in the awake or doze state as defined in 11.2.1 (General) while in the power save mode if the WUR non-AP STA is in WUR mode or WUR mode suspend. A WUR non-AP STA can be in active mode or power save (PS) mode as defined in 11.2.3.2 (Non-AP STA power management modes) if the WUR non-AP STA is in WUR mode or WUR mode suspend.”

As to the first sentence in the comment, P802.11ba D4.0, on P117L25, specifies that:

“If a WUR non-AP STA is in WUR mode, then:

—The negotiated WUR parameters between the WUR AP and the WUR non-AP STA are maintained by the WUR AP.

—A WUR AP shall schedule for transmission a WUR Wake-up frame for the WUR non-AP STA during an on duration that is negotiated with the WUR non-AP STA to notify the WUR non-AP STA that the WUR AP intends to have operation with the WUR non-AP STA as described in 29.9.2 (WUR AP operation) and 29.9.3 (WUR non-AP STA operation) if the WUR non-AP STA is in the doze state (see 11.2.1 (General)). …”

So, it is clear from the text highlighted above that the WUR AP may begin the use of WUR Wake-up frame towards the WUR non-AP STA when two conditions are simultaneously met: 1) The WUR non-AP STA is in the WUR mode, meaning that the WUR non-AP STA and WUR AP has completed the WUR Mode Setup negotiation; and 2) The WUR non-AP STA is in a PS mode doze state.

As to the second sentence in the comment, REVmd D2.4 (on P2172) states the following:

“**11.2.3.2 Non-AP STA power management modes**

A non-AP STA can be in one of two power management modes:

— Active mode: The STA receives and transmits frames at any time. The STA remains in the awake state.

— Power save (PS) mode: The STA enters the awake state to receive or transmit frames. The STA remains in the doze state otherwise.”

REVmd D2.4 further states the following:

(on P2172L41) “A non-AP STA shall be in active mode upon (re)association, …”

(on P2172L53) “To change power management modes a STA shall inform the AP by completing a successful frame exchange (as described in Annex G) that is initiated by the STA. This frame exchange shall include a Management frame, Extension frame or Data frame from the STA, and an Ack or a BlockAck frame from the AP. The Power Management subfield(s) in the Frame Control field of the frame(s) sent by the STA in this exchange indicates the power management mode that the STA shall adopt upon successful completion of the entire frame exchange, …”

Therefore, the WUR AP keeps track of the power management status of the WUR non-AP STA (and its WUR parameters if the WUR Mode Setup negotiation is done during association) when executing the EAP authentication and 4-way handshake procedures after association. The 4-way handshake is initiated by the AP with message 1. Message 1 is encapsulated in an EAPOL-Key frame, which is carried in an 802.11 data frame. If the WUR non-AP STA is in Active mode or a PS mode awake state, for obvious reasons, the 4-way handshake can be completed. If the WUR non-AP STA has negotiated the WUR mode and has entered a PS mode doze state, transmitting the data frame that carries message 1 to the WUR non-AP STA would trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit message 1. Such wake-up procedure is already defined in P802.11ba (Subclause 29.9).

Therefore, the concern that the 4-way handshake can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be modified in order to avoid misunderstanding of what it means by being in the WUR mode. The proposed text changes are shown at the end of this document.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4054 | 28.36 | It is unclear as to when the WIGTK and WIPN are sent from the Authenticator to the Supplicant. The WIGTK and WIPN must be sent prior to starting the WUR mode as during the WUR mode no non WUR PPDUs are exchanged between the WUR AP and WUR non-AP STA. | Clarify when the WIGTK and WIPN are sent for the Authenticator to the Supplicant. | **Revised.**The bullet in question and the revised Figure 4-32 on the following page clearly describes that the WIGTK and WIPN can be distributed to and installed at the Supplicant (i.e., the WUR non-AP STA), as a part of the 4-way handshake, or more specifically, in message 3 of the 4-way handshake. Adding WIGTK and WIPN as new group key and PN that can be distributed during the 4-way handshake doesn’t affect the timing of the 4-way handshake.The 4-way handshake can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the 4-way handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the 4-way handshake (in which case messages 1 and/or 3, both of which are encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The concern that the WIGTK and WIPN can not be distributed is not warranted.However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4054. |

**Discussion:**

4.10.3.3 describes AKM operations using password or PSK, comparing to the AKM operations using PMK as described in 4.10.3.2. The inserted new bullet in question (and the revised Figure 4-32) specifies the WIGTK and WIPN being distributed to and installed at the Supplicant (i.e., the WUR non-AP STA), as a part of the 4-way handshake. The other aspects as to the timing of WIGTK and WIPN distribution and the use of WUR Wake-up frames remain the same as previously discussed for CID 4053. Therefore, the concern that the WIGTK and WIPN can not be distributed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be modified (same changes as for CID 4053) in order to avoid misunderstanding of what it means by being in the WUR mode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4055 | 30.50 | It is unclear as to when the WIGTK and WIPN are sent from the Authenticator to the Supplicant. The WIGTK and WIPN must be sent prior to starting the WUR mode as during the WUR mode no non WUR PPDUs are exchanged between the WUR AP and WUR non-AP STA. | Clarify when the WIGTK and WIPN are sent for the Authenticator to the Supplicant. | **Revised.**The bullet in question and the revised Figure 4-32 on the previous page clearly describes that the WIGTK and WIPN can be distributed to and installed at the Supplicant (i.e., the WUR non-AP STA), as a part of the 4-way handshake, or more specifically, in message 3 of the 4-way handshake. Adding WIGTK and WIPN as new group key and PN that can be distributed during the 4-way handshake doesn’t affect the timing of the 4-way handshake.The 4-way handshake can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the 4-way handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the 4-way handshake (in which case messages 1 and/or 3, both of which are encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The concern that the WIGTK and WIPN can not be distributed is not warranted.However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4055. |

**Discussion:**

4.10.3.4 describes an alternative AKM operations using PSK. The inserted new bullet in question (and the revised Figure 4-32) specifies the WIGTK and WIPN being distributed to and installed at the Supplicant (i.e., the WUR non-AP STA), as a part of the 4-way handshake. The other aspects as to the timing of WIGTK and WIPN distribution and the use of WUR Wake-up frames remain the same as previously discussed for CID 4053. Therefore, the concern that the WIGTK and WIPN can not be distributed is not warranted. And, no further clarification is necessary. However, the definition of the WUR mode in subclause 3.2 can be modified (same changes as for CID 4053) in order to avoid misunderstanding of what it means by being in the WUR mode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4056 | 90.53 | It is unclear as to when the successful group key handshake, successful 40-way handshake, successful FT 4-way handshake, the Reassociation Response frame of the fast BSS transition protocol or successful FILS authentication occur to establish the WIGTKSA. These actions must occur prior to starting WUR mode operation, as frames can not be exchanged during WUR mode operation. | Clarify when WIGTKSA is established as a result of a successful group key handshake, successful 40-way handshake, successful FT 4-way handshake, the Reassociation Response frame of the fast BSS transition protocol or successful FILS authentication occur. | **Revised.**WIGTKSA is added merely as a new type of security association that could be the result of successful 4-way handshake or similar procedures named in the text. However, it doesn’t change the timing of when the 4-way handshake or similar procedure occur.The 4-way handshake can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the 4-way handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the 4-way handshake (in which case message 1, which is encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The same is true for the other similar procedures named in the inserted text. The concern that the 4-way handshake or similar procedures can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4056. |

**Discussion:**

In the inserted bullet in question, WIGTKSA is added as a new type of security association that could be the result of successful 4-way handshake or similar procedures named in the text. However, it doesn’t change the timing of when 4-way handshake or similar procedure occur.

As discussed for CID 4053, the concern that the 4-way handshake or similar procedures can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be modified (same changes as for CID 4053) in order to avoid misunderstanding of what it means by being in the WUR mode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4057 | 91.11 | It is unclear as to when a WUR non-AP STA would receive a WIGTK in a valid message. If the WUR non-AP STA is in WUR mode there is no method to send such a message. This needs to be clarified. | Clarify when a WIGTK is to be received. | **Revised.**The sentence in question clearly describes that the WIGTK is received in message 3 of 4-way handshake or similar frame/message in similar procedures named in the inserted text. The 4-way handshake can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the 4-way handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the 4-way handshake (in which case messages 1 and/or 3, both of which are encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The same is true for the other similar procedures named in the inserted text. The concern that WIGTK can not be delivered is not warranted. However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4057. |

**Discussion:**

The sentence in question clearly describes that the WIGTK is received in message 3 of 4-way handshake or similar frame/message in similar procedures named in the inserted text.

As discussed for CID 4053, the concern that WIGTK can not be delivered is not warranted. However, the definition of the WUR mode in subclause 3.2 can be modified (same changes as for CID 4053) in order to avoid misunderstanding of what it means by being in the WUR mode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 4058 | 92.10 | Clarify when the a second key exchange can occur, as such a key exchange can not happen when a WUR mode is active. | Clarify when a second key exchange can occur to distribute a subsequent WIGTK. | **Revised.**The sentence in question adds WIGTK as another group key that can be included in the group key handshake, which can be completed in both of the following situations:1. If the WUR non-AP STA is in Active mode or PS mode awake state before the group key handshake;
2. If the WUR non-AP STA has negotiated the WUR mode during association and has entered a PS mode doze state before the group key handshake (in which case message 1, which is encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The concern that the group key handshake can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be further clarified in order to avoid misunderstanding of what it means by being in the WUR mode. TGba editor to make the changes shown in 11-19/1818r0 under all headings that include CID 4058. |

**Discussion:**

Using the group key handshake (as a second key exchange) to distribute a subsequent GTK is a legacy behavior. The sentence in question merely adds WIGTK as another group key that can be included in the group key handshake.

Similar to the discussion for CID 4053, the group key handshake, which is initiated by the AP by transmitting message 1, can be completed in both of the following situations:

1. If the WUR non-AP STA is in Active mode or PS mode awake state;
2. If the WUR non-AP STA has negotiated the WUR mode and has entered a PS mode doze state (in which case message 1, which is encapsulated in a data frame, from the WUR AP can trigger the WUR AP to wake up the WUR non-AP STA using a WUR Wake-up frame first and then transmit the data frame). Such wake-up operation is same as the wake-up operation defined in subclause 29.9.

The concern that the group key handshake can not be completed is not warranted. However, the definition of the WUR mode in subclause 3.2 can be modified (same changes as for CID 4053) in order to avoid misunderstanding of what it means by being in the WUR mode.

 ---- Text Changes ----

**3.2 Definitions specific to IEEE Std 802.11**

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 4053, 4054, 4055, 4056, 4057, 4058):***

**wake-up radio (WUR) mode:** A negotiation status between a WUR AP and a WUR non-AP STA in which, if the WUR non-AP STA is also in a power save mode doze state, the WUR power state of the WUR non-AP STA alternates between the WUR awake state and the WUR doze state based on the negotiated WUR parameters.