IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB272 CR for OST CID 1978 | | | | |
| Date: 2023-06-02 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Narengerile | Huawei | Shenzhen, China |  | narengerile@huawei.com |
| Ali Raissinia | Qualcomm Inc. |  |  | alirezar@qti.qualcomm.com |
| Anirudha Sahoo | NIST |  |  | anirudha.sahoo@nist.gov |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document proposes the comment resolution for CID 1978.

Rx: initial version on June 2nd, 2023.

R0: revised version on June 16th, 2023, based on offline discussions with Ali and Anirud. Thank you for your help and contribution.

R1: revised version on Jun 29th, 2023, based on offline discussions with Ali and Anirud. Thanks again for your contribution.

# CID 1978

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Comment** | **Proposed change** | **Proposed resolution** |
| 1978 | 173.22 | The protocol for sensing measurement setup has a race condition flaw under which it is not clear whether or not the operational parameters are established on both sides. The responder may send a successful response that arrives after the initiator timeout. The initiator acks the response, but then discards it as not matching something it started. The responder thinks it has operational paramters for a particular ID but the initiator does not. | Fix the protocol flaw. Perhaps a response to measurement using that ID. Also, define what happens if the same ID is used on a subsequent setup. | REVISED.  I agree with the commenter in principle.  Please refer to the modifications specified in 23/1030r1 (<https://mentor.ieee.org/802.11/dcn/23/11-23-1030-01-00bf-lb272-cr-for-ost-cid-1978.docx>) for CID 1978. |

**Discussions for CID 1978:**

The case described in the comment – ‘*The responder may send a successful response that arrives after the initiator timeout*’ – is possible to happen if the Sensing Frame Exchange Expiry timer at the sensing initiator and that at the sensing responder are not synchronized. In other words, the timer at the sensing initiator may already time out while the timer at the sensing responder is still running. As a result, we could have two cases:

1. Case 1: The sensing initiator receives a response frame after the timeout, with Status Code = SUCCEESS.
   * For the responder, a sensing measurement session with a certain MSID is successfully established.
   * For the initiator, the sensing measurement session with a certain MSID is not established.
2. Case 2: The sensing initiator receives a response frame after the timeout, with Status Code = REQUEST\_DECLINED or REJECTED\_WITH\_SUGGESTED\_CHANGES.
   * For both the initiator and the responder, the sensing measurement session with a certain MSID is not established.

Case 1 clearly demonstrates a misaligned status between the sensing initiator and the sensing responder. A possible consequence will be that the sensing initiator sends a second request with the same MSID. Even though the Dialog Token in the second request frame will be different, the responder can easily get confused because the responder is already running a measurement session identified with the same MSID with the same sensing initiator. And we know that a unique measurement session is identified by <MSID, MAC address of the sensing initiator>. To avoid such situation, we propose the following modifications.

**Modifications for CID 1978:**

***To TGbf Editor: Please add the following text after P134L17 in subclause 11.55.1.4 in D1.1.***

If the sensing initiator receives a Sensing Measurement Response frame with a status code equal to SUCCESS after *aSensingFrameExchangeExpiry* timeout period of sending the corresponding Sensing Measurement Request frame, the sensing initiator should send a Sensing Measurement Termination frame with the Measurement Session ID carried in the received Sensing Measurement Response frame. (#1978)

If the sensing responder receives a Sensing Measurement Request frame with a Measurement Session ID that corresponds to a measurement session that has not been terminated with the same sensing initiator, the sensing responder should not respond with a Sensing Measurement Response frame. (#1978)

# SP:

Do you agree to the comment resolutions provided for CID 1978 to be included in the latest 11bf Draft?

Y/N/A