IEEE P802.11
Wireless LANs

|  |
| --- |
| 11be D2.0 CR for Miscellaneous CIDs II |
| Date: 2022-11-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

 10068, 11072, 11073, 11939, 13601, 14101

Revisions:

* Rev 0: Initial version of the document.

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 TGbe D2.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe D2.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 10068 | Thomas Derham | 11.13 | 327.32 | Several mechanisms (including SA Query referenced here, but also 4-way handshake and others) are adopted by 11be MLDs and require verification of OCI element. However OCI element only supports indicating the operating channel for a single link. | Allow multiple OCI elements to be present and validated (one per link), or extend OCI element to indicate information for multiple links. Note that, while Beacon Protection feature also allows a STA to validate channel information advertised by an AP in beacons, it has different security properties compared to OCV due to use of a group (not unicast) key and provides only one-way detection of multi-channel attacks. | Rejected –Related CID 14100, 10678, 10679 are discussed in 11-22-1356r6, and the discussions are provided below. * *The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.*
* *The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.*
* *In addition to the baseline, operating channel validation is defined and explained in* [*https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx*](https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx)
* *OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.*
* *ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.*
* *Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.*
* *At this point, there is no agreement on changes to the draft to address these comments. More work is required to determine if any additional changes to the draft are required to address these comments*

Since the comment requests similar change. We reject the comment since the comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 11072 | Po-Kai Huang | 13.7.1 | 377.23 | OCI subelement needs to be redesigned for MLO include link ID and information for 320 MHz verification because 320 MHz may have 320 MHz-1 or 320 MHz-2. . | Define MLO OCI subelement. Ideally, follow the format of OCI subelement to include link ID and change "Frequency Segment 1Channel Number" to simply "Channel center frequeny of 320 MHz", which is set to channel center frequency of 320 MHz when 320 MHz is used and 0 otherwise. Also, no need for OCT related information to start with. | Rejected –Related CID 14100, 10678, 10679 are discussed in 11-22-1356r6, and the discussions are provided below. * *The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.*
* *The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.*
* *In addition to the baseline, operating channel validation is defined and explained in* [*https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx*](https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx)
* *OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.*
* *ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.*
* *Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.*
* *At this point, there is no agreement on changes to the draft to address these comments. More work is required to determine if any additional changes to the draft are required to address these comments*

Since the comment requests similar change. We reject the comment since the comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 11073 | Po-Kai Huang | 11.13 | 327.43 | OCI element needs to be redesigned for MLO include link ID and information for 320 MHz verification because 320 MHz may have 320 MHz-1 or 320 MHz-2. . | Define MLO OCI element. Ideally, follow the format of OCI element to include link ID and change "Frequency Segment 1 Channel Number" to simply "Channel center frequeny of 320 MHz", which is set to channel center frequency of 320 MHz when 320 MHz is used and 0 otherwise. Also, no need for OCT related information to start with. | Rejected –Related CID 14100, 10678, 10679 are discussed in 11-22-1356r6, and the discussions are provided below. * *The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.*
* *The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.*
* *In addition to the baseline, operating channel validation is defined and explained in* [*https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx*](https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx)
* *OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.*
* *ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.*
* *Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.*
* *At this point, there is no agreement on changes to the draft to address these comments. More work is required to determine if any additional changes to the draft are required to address these comments*

Since the comment requests similar change. We reject the comment since the comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 11939 | Jarkko Kneckt | 11.13 | 327.17 | The current channel validation information contains channel information and procedure only for a single link. This is not suitable setup for multi-link operation, where a non-AP MLD may have more than 1 link with the AP MLD. The operating channel validation should be done in association, fast transition, SA Query, AP channel Switch, ML Reconfiguration. | Please add OCV support for multiple links or define alternative mechanism for all links operating channel validaton. | Rejected –Related CID 14100, 10678, 10679 are discussed in 11-22-1356r6, and the discussions are provided below. * *The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.*
* *The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.*
* *In addition to the baseline, operating channel validation is defined and explained in* [*https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx*](https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx)
* *OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.*
* *ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.*
* *Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.*
* *At this point, there is no agreement on changes to the draft to address these comments. More work is required to determine if any additional changes to the draft are required to address these comments*

Since the comment requests similar change. We reject the comment since the comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 13601 | Yongho Seok | 35.3 | 404.49 | For the multi-link operation, the OCI element should carry more than one {Operating Class, Primary Channel Number, Frequency Segmen 1 Channel Number} tuples for each link. | As in the comment. | Rejected –Related CID 14100, 10678, 10679 are discussed in 11-22-1356r6, and the discussions are provided below. * *The cited text for both comment reference the table updates that include the MLO KDEs and suggests another KDE needs to be added or modified to provide an OCI KDE, presumably for each link.*
* *The proposed resolution doesn’t describe what this new or modified KDE would contain or how it would be used.*
* *In addition to the baseline, operating channel validation is defined and explained in* [*https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx*](https://mentor.ieee.org/802.11/dcn/17/11-17-1807-12-000m-defense-against-multi-channel-mitm-attacks-via-operating-channel-validation.docx)
* *OCV is applied to security protocols defined in the 802.11 standard where an MITM could impersonate an endpoint on another channel.*
* *ML probe response cannot be protected because it is a class 1 frame and is used in a pre-association stated where there is no security association.*
* *Given that MLO security protocols are executed on the same link, OCV as specified in the base standard should work without modification.*
* *At this point, there is no agreement on changes to the draft to address these comments. More work is required to determine if any additional changes to the draft are required to address these comments*

Since the comment requests similar change. We reject the comment since the comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 14101 | Li-Hsiang Sun | 35.3.14.1 | 449.48 | "An MLD may transmit an individually addressed MMPDU that is a Class 3 frame that is intended for an associated MLD through any STA affiliated with the associated MLD with a setup link subject to additional constraints (see 35.3.7 (Link management))."For such MMPDU contains OCI element, it should only be sent on the link indicated in OCI element | As in comment | Revised – The following note is added by CID 12815 to clarify that if the management frame does not have correct content, then it will be discarded. *NOTE – If a buffered MMPDU  that is intended for one (#12242)non-AP STA affiliated with a non-APMLD (#10581)(see Table 11-3 (Bufferable/nonbufferable classification of MMPDUs)), the MMPDU does not carry information in the framebody to determine the intended destination non-AP STA affiliated with the non-AP MLD or does not have correct content to be transmitted to another non-AP STA affiliated with a non-AP MLD, and the MMPDU needs to be transmitted due to reception of a PS-Poll frame or a U-APSD trigger frame from another non-AP STA affiliated with an associated non-AP MLD that is in power save mode, then the MMPDU needs to be discarded. (#12815)*There are other management frame including OCI element like association request/response, SA Query request/response, WNM sleep mode request/response needs to have correct content as well. We simply add a note that we need to have correct content to tranmsit those frames in a specific link.TGbe editor to make the changes shown in 11-22/2033r0 under all headings that include CID 14101 |

**Discussion: None**

**35.3.14.1 General**

(…existing texts…)

An MLD may transmit an individually addressed MMPDU that is a Class 3 frame that is intended for an
associated MLD (#12646)to any STA affiliated with the associated MLD operating on a setup link through an
STA affiliated with the MLD operating on the setup link subject to additional constraints (see 35.3.7 (Link
management)).

NOTE – The class 3 managmenet frame that is intended for an associated MLD needs to have correct content to be transmitted through a setup link.(#14101)