IEEE P802.11
Wireless LANs

|  |
| --- |
| OCT issues |
| Date: 2019-01-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

IEEE P802.11-REVmd/D2.0 extended on-channel tunneling in a way that is both confusing and also overly generic to the point of allowing operations that could result in undesired operations and potentially even new security issues due to enabling new vectors for potential man-in-the-middle attacks.

The naming of the new Public Action frame is problematic since we now have two frames with the exact same name: On-channel Tunnel Request frame (see 9.6.7.47 and 9.6.20.7). It is unclear which one of those frames is beging referenced. Furthermore, 9.6.7.47 seems to be using "robust On-channel Tunnel Request frame" and "non-robust On-channel Tunnel Request frame" to talk about these frames in a manner that is not fully consistent with the use of robust management frames. Furthermore, these "robust" and "non-robust" are not part of the frame names.

It looks the goal here was to provide an option of sending out an On-channel Tunnel Request frame in non-associated state (the original On-channel Tunnel Request frame is a Class 3 frame and would not allow that use case). Based on my understanding of this use case, this new frame is supposed to be allowed to be used only as an individually addressed frame targeting a specific AP on one band (mainly, 2.4 GHz or 5 GHz) when performing operations targeting another band of the same set of collocated APs (mainly, a radio on 6 GHz). The added text in REVmd/D2.0 did not clarify this or added the constraints to cover this need without opening possibility of group-addressed requests or tunneling to a not-collocated AP. These constraints should be added to avoid misuse of this new extended functionality.

It looks like main new use case of discovery of a BSS information through active scanning does not actually work since responding to a Probe Request frame is an operation which does not have an OCT MLME primitive (in fact, there is no MLME primitive at all for sending Probe Response frame). The current text implies that only frames that have an OCT MLME primitive can be tunneled using On-channel Tunnel Request frame.

When tunneling a Probe Response frame, the description of the Timestamp field processing needs to be clearer. That field needs to be reserved since TR-MLME may not be able to synchronize with NT-MLME to get the correct TSF value and the update of that value when sending the Public Action frame would be unclear at best (the Timestamp field is in a different offset within the On-channel Tunnel Request frame and transmitted by a different radio).

This contribution proposed changes to address these issues.

*Change 6.3.89.2.2 as shown:*

**6.3.89.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-OCTunnel.request(

PeerSTAAddress,

OCT MMPDU,

Multi-band peer,

Multi-band Source)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| PeerSTAAddress | MAC Address | Any valid individual MAC address | Specifies the MAC address of the STA to which the On-channel Tunnel Request frame is transmitted. |
| OCT MMPDU | OCT MMPDU structure | As defined in the On-channel Tunnel Request frame format (see 9.6.20.7 (On-channel Tunnel Request frame format)) | The OCT MMPDU carries the MMPDU to be tunneled to the specified MLME entity of the specified STA. |
| Multi-band peer | Multi-band element | As defined in the Multi-band element format (see 9.4.2.138 (Multi-band element)) | The Multi-band element identifies the peer MLME entity that should receive the OCT MMPDU. |
| Multi-band Source | Multi-band element | As defined in the Multi-band element format (see 9.4.2.138 (Multi-band element)) | The Multi-band element identifies the MLME entity that generated (i.e., is the source) of the OCT MMPDU. |

*Change 6.3.89.3.2 as shown:*

**6.3.89.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-OCTunnel.indication(

PeerSTAAddress,

OCT MMPDU,

Multi-band local,

Multi-band Source,

Tunnelex RXVECTOR)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| PeerSTAAddress | MAC Address | Any valid individual MAC address | Specifies the MAC address of the STA from which the On-channel Tunnel Request frame was received. |
| OCT MMPDU | OCT MMPDU structure | As defined in the On-channel Tunnel Request frame format (see 9.6.20.7 (On-channel Tunnel Request frame format)) | The OCT MMPDU carries the MMPDU that is being tunneled to the local MLME entity. |
| Multi-band local | Multi-band element | As defined in the Multi-band element format (see 9.4.2.138 (Multi-band element)) | The Multi-band element identifies the local MLME entity that should receive the OCT MMPDU. |
| Multi-band Source | Multi-band element | As defined in the Multi-band element format (see 9.4.2.138 (Multi-band element)) | The Multi-band element identifies the MLME entity that generated (i.e., is the source) of the OCT MMPDU. |
| Tunneled RXVECTOR | RXVECTOR | As defined by the PHY of the STA | Contains a copy of the RXVECTOR that the PHY passes to the MAC upon reception of the On-channel Tunnel Request frame. |

*Change 11.32.5 as shown:*

**11.32.5 On-channel Tunneling (OCT) operation**

A STA supports the OCT if the OCT Not Supported subfield within the STA's Multi-band element is 0. A STA should not perform OCT with a peer STA that does not support the OCT. A STA that does not support the OCT shall ignore a received OCT MMPDU.

OCT allows a STA of a multi-band capable device to transmit an MMPDU that was constructed by a different STA of the same device. An MMPDU transmitted this way is referred to as an *OCT MMPDU*. The MLME of the nontransmitting STA that constructs or is the destination of an OCT MMPDU is referred to as an NT-MLME . The MLME of the STA that transmits or receives an OCT MMPDU over the air is referred to as a TR-MLME. An NT-MLME that constructs an OCT MMPDU destined to a peer NT-MLME does so according to the capabilities of the STA that contains the peer NT-MLME.

NOTE—OCT can be used in conjunction with or independent from the FST setup protocol.

Figure 11-52 (On-channel tunneling procedure) depicts the overall OCT procedure. In this figure, <primitive> refers to the name of any of the MLME primitives defined in 6.3 (MLME SAP interface) that meets all of the following conditions:

 — Includes a peer Multi-band element. The peer Multi-band element is used to identify the peer NT-MLME.

— Includes a local Multi-band element. The local Multi-band element is used to identify the local TR-MLME.

An MLME primitive meeting all of the above conditions is referred to as an *OCT MLME primitive*.

NOTE—MLME-AUTHENTICATE, MLME-ASSOCIATE, and MLME-REASSOCIATE are examples of primitives that are OCT MLME primitives.

In addition to the OCT MLME primitives, OCT procedure is used to transmit a response to a received On-Channel Tunnel Request frame encapsulating a Probe Request frame. The Timestamp field of the Probe Response frame in an On-Channel Tunnel Request frame is reserved.

To perform the OCT procedure, the values of the Band ID, Channel Number and BSSID fields in a Multi-band element are used to identify an MLME. All other fields in the Multi-band element shall be reserved.

Except for the following cases, the values of the Band ID, Channel Number and BSSID fields in a Multi-band element are used by an NT-MLME to deliver messages to a TR-MLME through the OCTunnel.request primitive, and are used by a TR-MLME to deliver messages to an NT-MLME through the OCTunnel.indication primitive:

— If the BSSID field is the wildcard BSSID, an MLME (either TR-MLME or NT-MLME) shall not use the BSSID field in selecting the MLME to deliver a message and shall, instead, invoke the corresponding primitive for all MLMEs that match the Band ID and Channel Number fields.

— If the OCT MLME request primitive is the MLME-SCAN.request primitive with ScanType parameter set to ACTIVE and that includes the ChannelList parameter, the NT-MLME shall not use the Channel Number field within the Multi-band local parameter of the MLME-SCAN.request primitive in selecting the TR-MLME to deliver a message and shall, instead, invoke the OCTunnel.request primitive at the TR-MLME(s) that match the Band ID field and BSSID field within Multi-band local parameter, and the channels specified in the ChannelList parameter.

— If the Channel Number field is 0 and the OCT MLME request primitive is not the MLME-SCAN.request primitive with ScanType parameter set to ACTIVE and that includes the ChannelList parameter, an MLME (either TR-MLME or NT-MLME) shall not use the Channel Number field in selecting the MLME to deliver a message and shall, instead, invoke the corresponding primitive for all MLMEs that match the Band ID and BSSID fields.

— If the Channel Number field is 0 and the OCT MLME request primitive is not the MLME-SCAN.request primitive with ScanType parameter set to ACTIVE and that includes the ChannelList parameter, and the BSSID field is the wildcard BSSID, an MLME (either TR-MLME or NT-MLME) shall use neither the BSSID field nor the Channel Number field in selecting the MLME to deliver a message and shall, instead, invoke the corresponding primitive for all MLMEs that match the Band ID field.

To transmit a tunneled MMPDU, the SME of a multi-band capable device generates an OCT MLME request primitive that includes the peer Multi-band element and the local Multi-band element. If the OCT MLME request primitive is the MLME-SCAN.request primitive with ScanType parameter set to ACTIVE, the BSSID field within the peer Multi-band element shall be set to the value of the BSSID parameter in the MLME-SCAN.request primitive and the BSSID field within the local Multi-band element shall be set to an individual MAC address.

 A NT-MLME receiving an OCT MLME request primitive shall

— As defined in this standard, process the request and construct an OCT MMPDU corresponding to the primitive in question. The NT-MLME shall not transmit any frame as a result of this primitive.

— Generate an MLME-OCTunnel.request primitive with parameters including the OCT MMPDU, the Multi-band peer parameter set to the peer Multi-band element and the Multi-band Source parameter set to the Multi-band element identifying the NT-MLME.

An NT-MLME does not issue an MLME-OCTunnel.request primitive if a selected TR-MLME does not exist. A TR-MLME does not issue an MLME-OCTunnel.indication primitive if a selected NT-MLME does not exist.

A single OCT MLME request primitive received by an NT-MLME may result in the invocation of one or more MLME-OCTunnel.request primitives at TR-MLME(s). Each invocation shall be towards a different TR-MLME.

A TR-MLME receiving an MLME-OCTunnel.request primitive shall transmit an On-channel Tunnel Request frame addressed to the peer TR-MLME and which includes the tunneled MMPDU. The peer TR-MLME(s) is identified by the PeerSTAAddress parameter of the MLME-OCTunnel.request primitive. The On-channel Tunnel Request frame shall not be group-addressed. Once the On-channel Tunnel Request frame is transmitted and acknowledged or attempts to transmit the frame are abandoned, the TR-MLME shall issue an MLME-OCTunnel.confirm primitive, with the appropriate result code, to inform the NT-MLME of the outcome of the frame transmission.

An On-channel Tunnel Request frame shall not be transmitted as a Public Action frame unless the tunneled MMPDU does not require management frame protection. An On-channel Tunnel Request frame transmitted as a Public Action frame shall target an NT-MLME known to be collocated with the specified TR-MLME. The receiving TR-MLME shall silently ignore the receive On-channel Tunnel Request frame if it is not targeting a collocated NT-MLME.

A TR-MLME receiving an On-channel Tunnel Request frame shall generate an MLME-OCTunnel.indication primitive with the Multi-band local parameter set to the Multi-band element identifying the TR-MLME, the Multi-band Source parameter set to the value of the Multi-band Source field contained in the On-channel Tunnel Request frame and the Tunneled RXVECTOR parameter set to the RXVECTOR of the On-channel Tunnel Request frame. The MLME-OCTunnel.indication primitive shall be generated to the NT-MLME identified by the peer Multi-band element contained within the received On-channel Tunnel Request frame.

An NT-MLME receiving an MLME-OCTunnel.indication primitive shall

— As defined in this standard, process the OCT MMPDU parameter of the primitive as if the MMPDU had been received over the air, with the exception that an Ack frame, if any, shall not be sent as a response to the reception of the MMPDU.

— Generate an OCT MLME indication primitive, if one is defined, corresponding to the frame type of tunneled MMPDU. This primitive is generated to the SME of the STA, which processes the MMPDU as defined in this standard. The Multi-band local parameter of the OCT MLME indication primitive shall be set to the value of the Multi-band local parameter of the MLME-OCTunnel.indication primitive and the Multi-band peer parameter shall be set to the value of the Multi-band Source parameter of the MLME-OCTunnel.indication primitive.

In the case of a .request/.indication primitive, the process stops here. Otherwise, the process continues as described below.

The peer SME responds to the reception of an OCT MLME indication primitive by generating the corresponding OCT MLME response primitive. This response includes the peer Multi-band element and the local Multi-band element.

An NT-MLME receiving an OCT MLME response primitive, if one is defined, or generating a response by itself, if no OCT MLME response primitive is defined (e.g., MLME-SCAN.response is not defined), shall

— As defined in this standard, process the response and construct an OCT MMPDU corresponding to the primitive in question. The NT-MLME shall not transmit any frame as a result of this primitive.

— Generate an MLME-OCTunnel.request primitive with parameters including the OCT MMPDU, the Multi-band peer parameter set to the the peer Multi-band element and the Multi-band Source parameter set to the Multi-band element identifying the NT-MLME. If no OCT MLME response primitive is defined, the Multi-band peer parameter shall be set to the value of the Multi-band Source parameter received in the corresponding MLME-OCTunnel.indication primitive. The MLME-OCTunnel.request primitive shall be generated to the TR-MLME identified by the local Multi-band element specified in the OCT MLME response primitive, if one is defined, or to the TR-MLME identified by the Multi-band local parameter of the MLME-OCTunnel.indication primitive that triggered this response, if no OCT MLME response primitive is defined.

A TR-MLME receiving an MLME-OCTunnel.request primitive transmits an On-channel Tunnel Request frame addressed to the peer TR-MLME that includes the tunneled MMPDU. The peer TR-MLME(s) is identified by the PeerSTAAddress parameter of the MLME-OCTunnel.request primitive. Once the Onchannel Tunnel Request frame is transmitted and acknowledged or attempts to transmit the frame are abandoned, the TR-MLME issues an MLME-OCTunnel.confirm primitive, with the appropriate result code, to inform the NT-MLME of the outcome of the frame transmission.

A TR-MLME receiving an On-channel Tunnel Request frame generates an MLME-OCTunnel.indication primitive with the Multi-band local parameter set to the Multi-band element identifying the TR-MLME, the Multi-band Source parameter set to the value of the Multi-band Source field contained in the On-channel Tunnel Request frame and the Tunneled RXVECTOR parameter set to the RXVECTOR of the On-channel Tunnel Request frame. The MLME-OCTunnel.indication primitive is generated to the NT-MLME identified by the peer Multi-band element contained within the received On-channel Tunnel Request frame.

An NT-MLME receiving an MLME-OCTunnel.indication primitive

— Processes the OCT MMPDU parameter of the primitive as if the MMPDU had been received over the air.

— Generates an OCT MLME confirm primitive, if one is defined, corresponding to the frame type of the tunneled MMPDU. This primitive is directed at the SME and has the Multi-band local parameter set to the value of the Multi-band local parameter of the MLME-OCTunnel.indication primitive and the Multi-band peer parameter set to the value of the Multi-band Source parameter of the MLME-OCTunnel. indication primitive. If the OCT MLME confirm primitive is the MLME-SCAN.confirm primitive and the NT-MLME did not scan all the channels specified in the corresponding MLME-SCAN.request primitive, the ResultCode parameter in the MLME-SCAN.confirm primitive shall be set to PARTIAL\_SCAN and the ScannedChannelList parameter shall list all channels that have been scanned.

An NT-MLME receiving an MLME-OCTunnel.confirm primitive shall:

— As defined in this standard, take action, if there is one, based on the success or otherwise of the OCT MMPDU transmission by the TR-MLME.

Figure 11-53 (Forward path of OCT messages based on OCT parameters) and Figure 11-54 (Return path of OCT messages based on OCT parameters) illustrate the complete forwarding of OCT messages based on the procedure described above in this subclause. Figure 11-53 (Forward path of OCT messages based on OCT parameters) depicts the forward path, i.e., from a requesting multi-band device (MBD) that initiates the OCT procedure with a responding MBD. Figure 11-54 (Return path of OCT messages based on OCT parameters) depicts the return path, i.e., from a responding MBD that generates an OCT MMPDU in response to the reception of an OCT MMPDU from a requesting MBD.