IEEE P802.11
Wireless LANs

|  |
| --- |
| Suggested resolutions to CID219 and CID357 |
| Date: 2017-09-11 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Kazuyuki Sakoda | Sony |  |  | Kazuyuki.Sakoda (at) sony (dot) com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document provides suggested resolutions to CID 219 and CID357, which are related to mesh operation.

# CID 219:

## Comment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PP.LL** | **Clause** | **Comment** | **Proposed Change** | **Suggested Resolution** |
|  | 14.5.4 | 14.5.4 needs to cover IGTKdata not just GTKdata | At the end of the last paragraph of the referenced subclause, add "The IGTKData subfieldin the Authenticated Mesh Peering Exchange element shall contain the Key ID concatenated by the IPN and the IGTK (as specified in 9.4.2.118 (Authenticated Mesh Peering Exchange element))."At 2144.24 (802.11mc/D7.0 reference) change 9.4.2.118 to 14.5.4 | REVISED: Adopt changes proposed in doc11-17/xxxr0. |

## Discussion:

The commenter pointed out that there is no description in 14.5.4 how the IGTKData subfield in the Authenticated Mesh Peering Exchange element is filled.

Looking at sublcauses 14.5.4 (Distribution of group transient keys in an MBSS), 9.4.2.118 (Authenticated Mesh Peering Exchange element), and 12.7.2 (EAPOL-Key frames), it should be reasonable suggestion.

The commenter also suggested to replace a reference in subclause 14.6.3.









## Suggested resolution:

REVISED:

***To REVmd Editor: Change 1st and 2nd paragraphs in 14.5.6 as follows:***

* Distribution of group transient keys in an MBSS

The MGTK shall be a random or pseudorandom number. The mesh STA shall distribute the MGTK to the peer mesh STA using the Mesh Peering Open frame during the AMPE. Upon successful completion of AMPE, each mesh STA shall establish states for the peer mesh STA’s mesh GTKSA. The GTKdata subfield in the Authenticated Mesh Peering Exchange element shall contain the MGTK concatenated with the Key RSC and the GTKExpirationTime (as specified in 9.4.2.118 (Authenticated Mesh Peering Exchange element)).

When dot11RSNAProtectedManagementFramesActivated is true, a mesh STA shall distribute the IGTK to the peer mesh STA using the Mesh Peering Open frame during the AMPE. Upon successful completion of AMPE, each mesh STA shall establish an IGTKSA (see 12.6.1.1.9 (IGTKSA)) with the mesh peer. The IGTKdata subfield in the Authenticated Mesh Peering Exchange element shall contain the Key ID concatenated with the IPN and the IGTK (as specified in 9.4.2.118 (Authenticated Mesh Peering Exchange element)).

***To REVmd Editor: a bullet under the 1stparagraphs in 14.6.3 as follows:***

* Mesh Group Key Inform frame construction and processing

Mesh Group Key Inform frame shall be constructed as follows:

* The Authenticated Mesh Peering Exchange element shall be set as the following:
* The Selected Pairwise Cipher Suite field shall be set to four octets of zero.
* The Local Nonce field shall be set to the same value as sent in the Mesh Peering Open frame that established the mesh peering instance.
* The Peer Nonce field shall be set to the same value as received in the Local Nonce field of the Authenticated Mesh Peering Exchange element of the incoming Mesh Peering Open frame that established the peering instance.
* The Key Replay Counter field shall be set to the mesh STA’s local replay counter value, incremented by 1, for the mesh peering. After setting this field, the local replay counter shall also be incremented by 1.
* The GTKdata field shall be present and shall contain the data for the MGTK from MGTK source. The components of the GTKdata are specified in 14.5.4 (Distribution of group transient keys in an MBSS).
* If management frame protection is used, the IGTKdata field shall be present and shall contain the data for the IGTK from IGTK source. The components of the IGTKdata are specified in 14.5.4 (Distribution of group transient keys in an MBSS).
* The MIC element shall be set according to the protection mechanism in 14.6.2 (Protection on mesh group key handshake frames).

# CID 357:

## Comment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PP.LL** | **Clause** | **Comment** | **Proposed Change** | **Suggested Resolution** |
| 1968.25 | 11.25.6 | The note is incomplete. For a Mesh STA, the ASRA bit is the "dynamic" flag to request an emergency session, but the value of the ESR bit (the "static" flag indicating the emergency handling capability of the mesh) should also be considered. It's no use trying to prioritse a path though the mesh for an emergency session (e.g. when the ASRA bit is set to 1), if the mesh is not capable of handling that emergency session (e.g. when the ESR bit is set to 0). | Change the start of the sentence to read "NOTE--The ESR bit set to 1 and the ASRA bit set to 1, informs the mesh STA ...." | REVISED: Adopt changes proposed in doc11-17/xxxr0. |

## Discussion:

Commenter is requesting to make the note more complete sentence, as ASRA field is valid only when ESR field is set to 1. (Accept the request only when the STA is capable of handling it).

Here, 2 STAs are involved. A requesting STA and a requested STA. We should make it clear if requesting STA needs to set ESR field to 1, when the requesting STA sets ASRA field to 1.





## Suggested resolution:

***To REVmc Editor: Change NOTE following the 5th paragraph in 11.25.6 as follows:***

* Interworking procedures: emergency services support

…

When dot11ESNetwork is true in a mesh STA, the ESR shall be set to 1. When that mesh STA receives a Mesh Peering Open frame that includes the Interworking element with the ASRA field equal to 1, it allows access to emergency services and forwards MSDUs to an emergency server.

NOTE—The ESR bit set to 1 and the ASRA bit set to 1, informs the mesh STA to prioritize resources for the emergency call, to proactively find a better path before the link conditions deteriorate below a certain threshold, and/or to change some of the mesh STA’s behavior (for example, to disable any power save features).

# Reference:

[1] Draft P802.11REVmd\_D0.2.

[2] 11-17/927 “REVmd Working Group Comments for MAC ad-hoc”