IEEE P802.11
Wireless LANs

|  |
| --- |
| Security Comment Resolution |
| Date: 16 Feburary 2012 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Yong Liu | Marvell |  | 1-408-222-8412 | yongliu@marvell.com |
|  |  |  |  |  |

Abstract

This document provides resolutions to CIDs 6444, 6325, 6336, 6335, 6294, 6143, 6256, 6259, 6258 in relation to the Draft P802.11ad\_D5.0 and the data base 11-12-0020-09-00ad-sb001-comment-database

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6444 | 11.4.5.3.2 | 466 | A new primitive - MLME-PN-Exhaustion.indication - is referenced, but is not defined | Add definition for MLME-PN-Exhaustion.indication (and other introduced related primitives) in Clause 6.3 | REVISEAdd definitions for both MLME-PN-Exhaustion.indication and MLME-PN-Warning.indication in Clause 6.3 Please see text changes in 12/0214r0 |
| 6325 | 11.4.5.3.2 | 466 | A new primitive - MLME-PN-Exhaustion.indication - is referenced here. This (and other related primitives) needs to be defined in Clause 6.3. | Define the missing primitives. | REVISESee CID 6444 resolution |
| 6294 |   | 470 | (CID 5517, Jouni Malinen) The base standard defines limitations on how many PTKSAs can exist for the same Supplicant/Authenticator MAC addresses (just one) in 11.5.1.1.6. P802.11ad seems to be changing the PTKSA derivation behavior for non-transparent multi-band RSNA (11.5.16.2) in a way that could allow two different PTKSAs for different bands to be derived even if the STAs use the same addresses (e.g., when different pairwise cipher is used). It looks like the restriction in 11.5.1.1.6 would need to be modified to allow this. | Replace "For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA with the same Supplicant and Authenticator addresses." with "For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA per band with the same Supplicant and Authenticator addresses." (page 1280 line 24 of P802.11-REVmb/D12) | REVISEChange to “… there shall be only one PTKSA per band/channel …”Please see text changes in 12/0214r0 |
| 6335 | 11.5.1.1.2 | 470 | The PMKSA does include the Authenticator MAC address. Otherwise RSNA security assumptions are broken. This would make legacy STA implementations non-compliant. | Either restore this bullet or add a qualifier for 11ad. | REVISE1. Restore the bullet2. Clarify that for multi-band RSNA case, the MAC address is associated with the operating band when the PMKSA is establishedPlease see text changes in 12/0214r0  |
| 6143 | 11.5.1.1.6 | 470 | The base standard defines limitations on how many PTKSAs can exist for the same Supplicant/Authenticator MAC addresses (just one) in 11.5.1.1.6. P802.11ad seems to be changing the PTKSA derivation behavior for non-transparent multi-band RSNA (11.5.16.2) in a way that could allow two different PTKSAs for different bands to be derived even if the STAs use the same addresses (e.g., when different pairwise cipher is used). It looks like the restriction in 11.5.1.1.6 would need to be modified to allow this. | Replace "For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA with the same Supplicant and Authenticator addresses." with "For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA per band with the same Supplicant and Authenticator addresses." (page 1280 line 24 of P802.11-REVmb/D12) | REVISESee CID 6294 resolution |
| 6336 | 11.5.1.1.6 | 470 | The PTKSA does not included the key ID . Including the keyID would make legacy STA implementations non-compliant. | Either remove this bullet or add a qualifier for 11ad. | DISAGREEIn REVmb D12, PTKSA already includes Key ID. |
| 6256 | 11.5.1.1.2 | 470 | Please check the security association lists against REVmb D12. The following errors exist (and there may be others):1. The struckout text at 470.08 doesn't match REVmb D12 1278.65,2. The Key ID inserted in 11.5.1.1.6 already exists at 1280.453. Likewise for 11.5.1.1.8 and 11.5.1.1.12. |   | REVISE1. Restore the struckout text in 11.5.1.1.2See CID 6335 resolution2. Remove change to PTKSA elements in 11.5.1.1.6 since the change was already included in REVmb D123. Remove 11.5.1.1.8 and 11.5.1.1.12 since the changes to these subclauses were already included in REVmb D12 |
| 6258 | 11.6.2 | 478 | The extension of the Key ID KDE makes existing devices non-compliant and probably creates an interoperability problem in the OBand. | Describe the Band ID field as present only in Key ID KDEs transmitted by Multi-band capable STAs. | REVISE1. Remove changes to GTK KDE and Key ID KDE2. Define a new Multiband GTK KDE and a new Multiband Key ID KDE Please see text changes in 12/0214r0 |
| 6259 | 11.6.2 | 478 | Inserting an additional octet field into the middle of an existing structure will have an interesting effect on interoperability. | Find an alternative that will not break interoperability and make existing devices non-compliant. Consider adding a new Band ID KDE instead. Or signal the presence of the additional field with one of the reserved bits and state that it shall only be transmitted by a multi-band capable STA to another such STA. | REVISESee CID 6258 resolution |

*Editor: Please add the following two new subclauses in 6.3*

**6.3.xx PN event report**

**6.3.xx.1 General**

This subclause describes the management procedures associated with PN event report.

**6.3.xx.2 MLME-PN-Exhaustion.indication**

**6.3.xx.2.1 Function**

This primitive indicates that the PN associated with a temporal key exceeds dot11PNExhaustionThreshold.

**6.3.xx.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-PN-Exhaustion.indication(

 Key ID,

 Key Type,

 Address

 )



**6.3.xx.2.3 When generated**

This primitive is generated by the MLME when the PN associated with a temporal key exceeds dot11PNExhaustionThreshold.

**6.3.xx.2.4 Effect of receipt**

On receipt of this primitive, the SME deletes the temporal key associated with the PN.

**6.3.xx.3 MLME-PN-Warning.indication**

**6.3.xx.3.1 Function**

This primitive indicates that the PN associated with a temporal key exceeds dot11PNWarningThreshold.

**6.3.xx.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-PN-Warning.indication(

 Key ID,

 Key Type,

 Address

 )



**6.3.xx.3.3 When generated**

This primitive is generated by the MLME when the PN associated with a temporal key exceeds dot11PNWarningThreshold.

**6.3.xx.3.4 Effect of receipt**

On receipt of this primitive, the SME can create a new temporal key before the PN space is exhausted.

*Editor: Please make the following changes*

**11.5.1.1.2 PMKSA**

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. When the PMKSA is the result of a successful SAE authentication, it is generated as a result of the successful completion of the SAE exchange. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is created by the Supplicant’s SME when the EAP authentication completes successfully or the PSK is configured. The PMKSA is created by the Authenticator’s SME when the PMK is created from the keying information transferred from the AS, when IEEE 802.1X authentication is utilized, or when the SAE exchange successfully completes or the PSK is configured. The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes. The PMKSA consists of the following elements:

* PMKID, as defined in 11.6.1.3. The PMKID identifies the security association.
* Authenticator’s or peer’s MAC address. For multi-band RSNA, the MAC address is associated with the operating band when the PMKSA is established.
* PMK.
* Lifetime, as defined in 11.6.1.3.
* AKMP.
* All authorization parameters specified by the AS or local configuration. This might include parameters such as the STA’s authorized SSID.

**11.5.1.1.6 PTKSA**

The PTKSA is a result of the 4-Way Handshake, FT 4-Way Handshake, FT Protocol, or FT Resource Request Protocol. This security association is also bidirectional. PTKSAs are cached for the life of the PMKSA or PMK-R1 security association. Because the PTKSA is tied to the PMKSA or to a PMK-R1 security association, it only has the additional information from the 4-Way Handshake. For the PTKSA derived as a result of the 4-Way Handshake, there shall be only one PTKSA per band/channel with the same Supplicant and Authenticator MAC addresses. For the PTKSA derived as a result of an initial mobility domain association or fast BSS transition, there shall be only one PTKSA with the same STA’s MAC address and BSSID.

*Editor: Please delete changes to GTK KDE and Key ID KDE*

*Editor: Please add two new KDEs in* ***Table 11-6—KDE***

Multiband GTK KDE

Multiband Key ID KDE

*Editor: Please add following text to 11.6.2*

The format of the Multiband GTK KDE is shown in Figure 11-xx.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key ID (0, 1, 2, or 3) | Tx | Reserved (0) | Band ID | GTK |
| bits 0-1 | bit 2 | bits 3-7 | 1 octet | (Length - 6) octets |

Figure 11-xx Multiband GTK KDE

The Band ID field contains the identification of the frequency band (see 8.4.1.45 Band ID field).

The format of the Multiband Key ID KDE is shown in Figure 11-xx.

|  |  |  |
| --- | --- | --- |
| Key ID | Reserved | Band ID |
| bits 0-1 | bits 2-7 | bits 8-15 |

Figure 11-xx Multiband Key ID KDE

The Band ID field contains the identification of the frequency band (see 8.4.1.45 Band ID field).

*Editor: Please make the following changes*

**11.6.6.4 4-Way Handshake Message 3**

**…**

* For PTK generation for a supported band other than the current operating band, the Authenticator’s Beacon/mmWave Beacon/Announce/Probe Response/Information Response frame’s Multi-band element associated with the supported band, and optionally, a second Multi-band element that indicates the Authenticator’s pairwise cipher suite assignment for the supported band, and, if group cipher for the supported band is negotiated, the ~~encapsulated GTK and the GTK’s key identifier~~ Multiband GTK KDE for the supported band, if dot11MultibandSupportEnabled is true, or;
* for generating a single PTK for all involved bands, the Authenticator’s Beacon/mmWave Beacon/Announce/Probe Response/Information Response frame’s RSN element and Multi-band element(s), and optionally, additional RSN element and Multi-band element(s) that indicate the Authenticator’s assignment of one pairwise cipher suite for all involved bands; if a group cipher for all involved bands is negotiated, the ~~encapsulated GTK and the GTK’s key identifier~~ Multiband GTK KDEs for all involved bands, if dot11MultibandSupportEnabled is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s), or;
* for generating different PTKs for the current operating band and other supported band(s), the Authenticator’s Beacon/mmWave Beacon/Announce/Probe Response/Information Response frame’s RSN element and Multi-band element(s), and optionally, additional RSN element and Multi-band elements that indicate the Authenticator’s pairwise cipher suite assignments for one or more involved bands; if group ciphers for the involved bands are negotiated, the ~~encapsulated GTKs and the GTK’s key identifiers~~ Multiband GTK KDEs for the involved bands, if dot11MultibandSupportEnabled is true and the Joint Multi-band RSNA subfield is set to 1 for both the Authenticator and Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.
* For STK generation Initiator RSNIE, Lifetime of SMK is used.
* If the Extended KeyID for Unicast subfield of the RSN Capabilities field is set to 1 for both the Authenticator/STA\_I and Supplicant/STA\_P, then the Authenticator/STA includes the Key ID KDE with the assigned key identifier for the current operating band; or the Authenticator includes the Multiband Key ID KDE(s) with the assigned key identifier(s) for one or more supported bands, if dot11MultibandSupportEnabled is true.