IEEE P802.11
Wireless LANs

|  |
| --- |
| 11mc assigned CIDs  |
| Date: 2016-05-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | Hewlett Packard Enterprise | 1322 Crossman Ave Sunnyvale, CA 94089 | +1 630-363-1389 | dorothy.stanley@hpe.com  |

Abstract

This document contains the proposed resolutions to CIDs:

MAC: 7346, 7105, 7511, 7062, 7553

GEN: 7649, 7530, 7510, 7350, 7739, 7552

R0: Initial resolutions proposed

R1: Includes updates from Cambridge

R2: Additional proposed resolutions to CIDs 7062 and 7553

R3: Add 7552 (Editor Rework)

R4: Includes updates from 2016-05-13 teleconference

**CID 7553 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7553 | 104.50 | 4.5.4.3 |  | A | Does "PMKSA caching" include "mesh PMKSA caching", given that a "mesh PMKSA" is not a type of "PMKSA"? Is mesh PMKSA caching even defined? | Delete "or mesh PMKSA" at the end of the sentence |

**Discussion:**

From Ad-hoc notes in 11-15-565r41:

**MAC: 2016-05-01 21:01:53Z -**

12.11.3.1 Dan objects to deleting “or mesh PMKSA” because mesh does use PMKSA.12.11.3.2 From the minutes there are two sentences and we are deleting the “or mesh PMKSA” from only one sentence.12.11.3.2.1 ACTION ITEM #15: Dorothy will check with Dan H, as he wrote most of the mesh security sections. Proceed with ACCEPTED, as the plan, unless we hear otherwise.

The cited text is below:



**The proposed “Accepted resolution would make the change shown below:**

In an RSNA, deauthentication also deletes any related pairwise transient key security association (PTKSA),

group temporal key security association (GTKSA), station-to-station link (STSL) master key security

association (SMKSA), STSL transient key security association (STKSA), integrity group temporal key

security association (IGTKSA), mesh GTKSA, mesh TKSA, and mesh PMKSA that exist in the STA and

closes the associated IEEE Std 802.1X Controlled Port. If pairwise master key security association

(PMKSA) caching is not enabled, deauthentication also deletes the PMKSA.

However, mesh PMKSA caching is defined, see 1960.35:

“— Mesh PMKSA: A result of successful completion of the active authentication protocol.”

 and 1962.23:
“The mesh PMKSA is used to create

the mesh TKSA. Mesh PMKSAs are cached for up to their lifetimes. Mesh PMKSAs contain the following

elements, and are identified by their PMKID.”

So the prior sentence near the cited text is incorrect in indicating that the Mesh PMKSA is deleted upon deauthentication.

**Proposed resolution: Revised**

At 104.48, change “mesh TKSA, and mesh PMKSA that exist in the STA” to “and mesh TKSA that exist in the STA”

This change corrects the text to indicate that mesh PMKSA caching is defined (see 1960.35 and 1962.23).

***Modify section 12.6.12 as indicated:***

**12.6.12 RSNA authentication in an MBSS**

When establishing an RSNA in an MBSS, a mesh STA shall use IEEE Std(#130) 802.11 SAE authentication (see 12.4 (Authentication using a password)), or optionally IEEE Std(#130) 802.1X authentication, prior to establishment of an authenticated peering. An RSNA security association, called a mesh PMKSA(#6228) , is created upon successful completion of authentication. The mesh PMKSA is used with the AMPE to create a mesh TKSA.

A mesh PMKSA may be cached and used with the AMPE to establish a fresh mesh TKSA. A STA includes the PMKID for the PMKSA in the Mesh Peering Open frame. If the PMKID in a received Mesh Peering Open frame is unknown, the AMPE handshake fails. If both sides assert possession of a cached mesh PMKSA but the AMPE handshake fails, a STA may delete the cached mesh PMKSA for the selected PMKID. A mesh PMKSA may not be changed while cached.

Authentication using IEEE Std(#130) 802.11 SAE authentication is based on a password. A password is required to be shared between two mesh STAs in order to successfully complete authentication. This password can be pairwise – each pair of mesh STAs in an MBSS has a unique password – or it can be shared-all mesh STAs in the MBSS share the same password.

Due to the security properties of IEEE Std(#130) 802.11 SAE authentication, an adversary has no greater possibility in determining a shared password than in determining a pairwise password. The potential for misuse, though, is greater if a shared password becomes known to an adversary because an unlimited number of mesh STAs under the control of the adversary can be added to the MBSS.

***Instruct the editor to add new entry in the PICS as MP2.2.4 incrememting the last digit in all subsequent MP2.2.x entries:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  MP2.2.4 |  Mesh pairwise master key security association (PMKSA) caching | 12.6.12 (RSNA authentication in an MBSS) | MP2.2: M | Yes No N/A  |

**CID 7552**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7552 | 1960.06 | 12.6 |  | V | What is an "MTKSA"? The term appears in Subclause 12.6 twice, but not in Clause 3, nor is it defined/described in Subclause 12.5.1.1 | Change both instances to "mesh TKSA" or "mesh PTKSA" (depending on resolution to other comment), with the right case. Also delete "pairwise" before the second |

**Discussion:**

The following resolution was approved:

REVISED (GEN: 2016-02-25 06:32:05Z) incorporate the changes in 11-16/281r1 (https://mentor.ieee.org/802.11/dcn/16/11-16-0281-01-000m-resolution-of-cid-4859.docx) and remove "pairwise" in paragraphs 12.6.1.1.9 and 12.6.7

The editor identified issues implementing this portion: **“**remove "pairwise" in paragraphs 12.6.1.1.9 and 12.6.7”

History: This CID was discussed at the February Ft. Lauderdale meeting:

* + - 1. Discussion on the change of MGTKSA to mesh GTKSA or MTKSA to mesh TKSA. – Agreement on these three changes.
			2. Straw Poll on keeping or deleting pairwise
				1. Result – Keep =2; Delete =2; Abstain = 4;
				2. Remove “pairwise” in paragraphs 12.6.1.1.9 and 12.6.7
			3. Proposed resolution for CID 7552 and CID 7606; Revised; incorporate the changes in 11-16/281r1 (<https://mentor.ieee.org/802.11/dcn/16/11-16-0281-01-000m-resolution-of-cid-4859.docx>) and remove “pairwise” in paragraphs 12.6.1.1.9 and 12.6.7
			4. No Objection – Mark Ready for Motion

**Changes from 11-16-0281:**

***Instruct the editor to modify section 12.6.1.1.9 as indicated:***

**12.6.1.1.9 IGTKSA**

When management frame protection is enabled, a non-AP STA’s SME creates an IGTKSA when it receives a valid Message 3 of the 4-way handshake or FT 4-way handshake, the Reassociation Response message of the fast BSS transition protocol with a status code indicating success, a Mesh Peering Open Message of the Authenticated Mesh Peering Exchange (AMPE) protocol, or a valid Message 1 of the group key handshake. The Authenticator’s SME creates an IGTKSA when it establishes or changes the IGTK with all STAs to which it has a valid PTKSA or mesh TKSA.

***Instruct the editor to modify section 12.6.7 as indicated:***

**12.6.7 RSNA policy selection in an MBSS**

All mesh STAs in an MBSS use the same group cipher suite. Mesh STAs establish authenticated peerings with each other using the AMPE protocol (see 14.5 (Authenticated mesh peering exchange (AMPE))). In AMPE, mesh STAs negotiate a pairwise cipher suite, and establish a pairwise mesh TKSA, to protect individually addressed frames and state a group cipher suite and establish a mesh GTKSA to process incoming group addressed frames from a peer.

Observation: “Pairwise” is not present in 12.6.1.1.9, and is present in 2 locations in 12.6.7. Use of “pairwise” is accurate. Prior straw poll did not show strong support for removing “pairwise”.

**Proposed updated resolution: Revised**

Incorporate the changes in 11-16/281r1 (<https://mentor.ieee.org/802.11/dcn/16/11-16-0281-01-000m-resolution-of-cid-4859.docx>). These changes expand the acronyms uniformly as suggested by the commenter. Use of “pairwise” is accurate.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7062 | 832.37 | 9.4.2.25.3 |  |  | "a single AKM suite selector may be specified because IBSS STAs use the same AKM suite" - normative verb in clause 9.It is unclear as to whether this is granting permission. | If normative behaviour is present elsewhere, cite it here and change "may" to "can" and add reference to subclause defining the behaviour. Otherwise move this to a behavioural clause. |

The cited text is below:

“The AKM Suite List field contains a series of AKM suite selectors contained in the RSNE. In an IBSS only

a single AKM suite selector may be specified because IBSS STAs use the same AKM suite and because

there is no mechanism to negotiate the AKMP in an IBSS (see 12.6.5 (RSNA policy selection in an IBSS

and for DLS)).”

Discussion:

The normative IBSS behavior is specified in 12.6.5:



The text below is from 1971.38 in 12.6.5:



Proposed resolution: Revised

At 832.37, change “may be specified” to “is specified”.

This change eliminates the normative language from clause 9. The normative language is already referenced (12.6.5).

 **CID 7346- MAC**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7346 | 828.40 | 9.4.2.25.1 |  |  | It says "The RSNE contains authentication and pairwise cipher suite selectors, a single group data cipher suite selector, an RSN Capabilities field, the PMK identifier (PMKID) count, a PMKID list, and a single group management cipher suite selector." but it doesn't necessarily contain all of these, and the PMKID count is not of particular significance compared to the other counts. And "authentication" is vague | Change to "The RSNE potentially contains AKM and pairwise cipher suite selector lists, single group data and management cipher suite selectors, an RSN Capabilities field, and a PMKID list." Or replace the first para with "The RSNE contains the information necessary to establisn an RSNA. The format of the RSNE is shown in Figure 9-254." |

**Discussion:**

The cited text is below:



The comment is on the first paragraph of the cited section; the commenter’s two proposed resolutions are shown below. The proposed change (revised) generalizes the description and updates reference language.

The RSNE potentially contains AKM and pairwise cipher suite selectors, single group data and management cipher suite selectors, an RSN Capabilities field and a PMKID list.The format of the RSNE is shown in Figure 9-254 (RSNE format).

Alternatively, the commenter suggests:

The RSNE contains the information necessary to establish an RSNA. The format of the RSNE is shown in Figure 9-254 (RSNE format).

**Proposed resolution: Revised**

Change the cited text as indicated below. This change generalizes the description and updates reference language.

“The RSNE contains theinformation required to establish an RSNA. . The format of the RSNE is defined in Figure 9-254 (RSNE format).”

**CID 7105 – MAC**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7105 | 1972.65 | 12.6.7 |  |  | "Because a VHT STA is also an HT STA ... elimination of TKIP ..."- this note is stunningly irrelevant because this subclause has nothing to be with TKIP. | Remove cited note. |

**Discussion:**

The cited text is in 12.6.7, “RSNA Policy Selection in an MBSS”

1972.65:



Similar text is in other Policy section sections:

1971.19 in 12.6.5, “**RSNA policy selection in an IBSS and for DLS”**

****

Also at 1969.45**, “12.6.3 RSNA policy selection in an infrastructure BSS**

****

At 129. 49-52 and 1899.22-26, WEP and TKIP are deprecated.

At 1903. 13, in 12.2.6 “RSNA assumptions and constraints” there is a “shall” for non-use of TKIP by HT:

 “An HT STA shall not use either of the pairwise cipher suite selectors: “Use group cipher suite” or TKIP to

communicate with another HT STA.”

Suggest moving/adding the note here.

**Proposed resolution: Revised**

At 1903.16, insert the following NOTE:

“NOTE—Because a VHT STA is also an HT STA, the elimination of TKIP also applies to VHT STAs.”

And

At 1972.65 (the cited location), delete the cited note.

At 1975.19, delete Note 2 “NOTE 2—Because a VHT STA is also an HT STA, the elimination of TKIP also applies to VHT STAs.”

At 1969.45, delete Note 1 “NOTE 1—Because a VHT STA is also an HT STA, the elimination of TKIP also applies to VHT STAs.”

These changes move the cited sentence (and 2 other instances) to one more general location.

**CID 7649 GEN**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7649 | 2925.61 | C.3 |  |  | The description of dot11RSNAActivated suggests it's only for APs | Delete "The entity advertises the RSNE in its Beacon and Probe Response frames." |

**Discussion:**

**The cited text is below:**



**The commenter suggests to delete the sentence highlighted below.**

"This is a control variable.

It is written by an external management entity.

Changes take effect for the next MLME-START.request primitive or MLMEJOIN.

request primitive.

When this object is true, this indicates that RSNA is enabled on this

entity. The entity advertises the RSNE in its Beacon and Probe Response

frames. Configuration variables for RSNA operation are found in the

dot11RSNAConfigTable.

This object requires that dot11PrivacyInvoked also be equal to true."

**Proposed resolution: Accepted**

**CID 7530 (GEN)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7530 | 2130.04 | 14.5.1 |  |  | The term "mesh PMK" is used nowhere else | Change to "mesh PMKSA" |

**Discussion:**

**The cited text is below.**

****

At 1962.16, the MESH PMKSA is defined and includes a PMK:

****

**This is similar but not the same as CIDs** 7551, 7552 and 7606 which are resolved by incorporation of 11-16-0281r1, which changes to mesh TKSA, mesh GTKSA. The question here is whether to refer to a PMK (mesh PMK) or mesh PMKSA.

2130.04 refers to the “key confirmation” using the mesh PMK, which sounds correct, as key confirmation uses a key, not a security association (mesh PMKSA) as suggested by the commenter’s proposed resolution.

**Proposed resolution: Revised**

At 2130.04, change from “mesh PMK” to “PMK”.

Note to commenter:

2130.04 refers to the “key confirmation” using the mesh PMK, which is correct, as key confirmation uses a key, not a security association (mesh PMKSA) as suggested by the commenter’s proposed resolution.

In other mesh security descriptions, for example in the mesh PMKSA definition at 1962.16, “PMK” is used, rather than “mesh PMK”. Also see for example 2129.55, 2137.60-63. The change makes the cited location consistent with other usage in the mesh security section.

**CIDs 7510, 7350 (GEN)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7510 | 2875.55 | C.3 |  |  | dot11RSNAConfigNumberOfSTKSAReplayCountersImplemented is not used outside the MIB (unlike the PTKSA/GTKSA ones) | Mark this variable as deprecated |
| 7350 |  |  |  |  | Misuse of "sequence number" in the context of PNs/TSCs (rather than the MPDU SN) | At 1002.10 and 2018.45 change "[The] Key RSCdenotes the last frame sequence number sent using the GTK" to "[The] Key RSC denotes the last TSC or PN sent using the GTK"At 2011.52 change "Key RSC = For PTK generation, starting sequence number" to "Key RSC = For PTK generation, starting TSC or PN"At 2019.32 change "Key RSC = last transmit sequence number for the GTK" to "Key RSC = last TSC or PN for the GTK"Ar 2021.29 change " the last sequence number used with the GTK (RSC)" to " the last TSC or PN used with the GTK (RSC)"1930.42, 1931.47 are also suspect |

**CID 7510 Proposed resolution: Revised**

At 2938.58, change from **“**STATUS current” to “STATUS deprecated”

This change implements the commenter’s proposed resolution.

**CID7350 Proposed resolution: Revised**At 1002.10 and 2018.45 change "[The] Key RSC
denotes the last frame sequence number sent using the GTK" to "[The] Key RSC denotes the last TSC or PN sent using the GTK"
At 2011.52 change "Key RSC = For PTK generation, starting sequence number" to "Key RSC = For PTK generation, starting TSC or PN"
At 2019.32 change "Key RSC = last transmit sequence number for the GTK" to "Key RSC = last TSC or PN for the GTK"
At 2021.29 change " the last sequence number used with the GTK (RSC)" to " the last TSC or PN used with the GTK (RSC)"

These changes implement the commenter’s proposed changes. No change is made at 1930.42 and 1931.47 as these locations describe TKIP operation, and TKIP is deprecated.

**CID 7511(MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7511 | 836.10 | 9.4.2.25.4 |  |  | It says "A STA sets the GTKSA Replay Counter subfield of the RSN Capabilities field to the value contained in dot11RSNAConfigNumberOfPTKSAReplayCounters." | Change "PTKSA" to "GTKSA" |

**The cited text is below:**

****

**Proposed resolution: Accepted**

**CID 7739 (GEN)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7739 | 1994.34 | 12.7.1.7.3 |  |  | Q is unnecessary and confusing (not used elsewhere) | Define Length rather than Q in the para below (by adding 128 to each, obviously), delete the Length definition, and use Length <minus> 128 where you currently have Q in the two equations before the "where" |

**The cited text is below:**

****

**Discussion:**

**Proposed resolution: Rejected**

The current formulation is accurate and has been implemented by multiple independent implementations.

**References:**

<https://mentor.ieee.org/802.11/dcn/15/11-15-0532-38-000m-revmc-sponsor-ballot-comments.xls>