IEEE P802.11
Wireless LANs

|  |
| --- |
| 11mc comment resolutions 5167-5170 |
| Date: 2015-08-20 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | HP (Aruba Networks) | 1322 Crossman Ave Sunnyvale, CA 94089 | +1 630-363-1389 | dstanley@arubanetworks.com  |

Abstract

This document contains the proposed resolutions to CIDs 5167, 5168, 5169, 5170, 5165.

Also CIDs 5997 and 5998.

R1: Includes results of 2015-08-07 teleconference, resolutions agreed to 5167, 5169, 5170, 5165, 5997 and 5998. CID 5168 is still open.

R2: Includes updated proposed resolutions to CIDs 5167, 5168.

Includes proposed resolutions to CIDs 6398, 6349, 6184 (from MAC-AP Pulled in 11-15-0565r12). Includes proposed resolutions to CIDs 6511, 6183 and 6275 (from MAC-AR pulled in 11-15-0565r12).

Includes proposed resolutions (or discussion) for CIDs 6509, 6510, 6365, 6364, 6367, 6023, 6295, 5062.

R3: Includes changes per the Cambridge 2015-08-19 meeting.

**CID 5167, 5169 - MAC**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5169 | 1076.50 | 8.4.5.16 |  |  | "The Emergency Alert URI field is formatted in accordance with IETF RFC 3986." is not correctly formulated. It should say: "The Emergency Alert URI field is encoded using the guidance from IETF RFC 3986" | per comment. |
| 5167 | 1066.53 | 8.4.5.4 |  |  | change "The Venue Name is a variable-length UTF-8 formatted" to "The Venue Name is a variable-length UTF-8 encoded"and replace "formatted" with "encoded" throughout the doc, where applicable (eg, instances where it says that the field is formatted in accordance with RFC3986, instances of UTF-8 formatted, etc). | as suggested |

**The cited text is seen in context below:**

****

**The commenter’s proposed change applies to the cited and similar text:**

At 1066.53, and additional locations 1067.29, 1071.47replace “formatted” with “encoded” as shown below:

The Venue Name is a variable-length UTF-8 encoded field containing the venue’s name. The

maximum length of this field is 252 octets.

And at

1076.62: The Emergency NAI Information field is a variable-length field encoded using UTF-8 and formatted in accordance with IETF RFC 4282.

**Proposed resolution: Revised**

At 1066.53, and additional locations 1067.29, 1071.47replace “formatted” with “encoded”

And change at

1076.62: The Emergency NAI Information field is a variable-length field encoded using UTF-8 and formatted in accordance with IETF RFC 4282.

Note to commenter: RFC 3986 does not define an encoding, rather it defines a format.

**CID 5168 - MAC**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5168 | 1075.53 | 8.4.5.14 |  |  | The text does not say how the Public Identifier URI/FQDN is encoded. | Submission will be provided.The text has to say that the field is encoded using the guidelines from RFC3986. |

**The Cited text is below:**

****

**Discussion:** Propose the following change:

The Public Identifier URI/FQDN field is a variable-length field containing zero or more Public Identifier

URI/FQDN subelements, as defined in 8.4.2.21.14 (Location Identifier report). Each URL/FQDN field is a variable-length fieldencoded in accordance with IETF RFC 3986.

2015-08-07 telecon discussion: Definition of the format is in 8.4.2.21.14, Table 8-122, so no additional edits needed.

**Action:** Dorothy to confirm with commenter.

**2014-08-11: Update from commenter:**

I also disagree with the conclusion that there is no need to specify the encoding of the URI/FQDN ANQP element. Table 8-122 defines the values of the URI/FQDN Descriptor field (perhaps the title of Table 8-122 should be changed from “URI/FQDN Descriptor Field encoding” to “URI/FQDN Descriptor Field values”), it does not talk about how the next field in figure 8-240 is encoded (ie, the Public Identifier URI/FQDN, variable length field). A URI can be of a format like this:

Hűhahó@áéőú.üű/~?úü , which cannot be ASCII-encoded, as these characters are not part of the ASCII set of characters, it has to be encoded using UTF-8.

**Proposed resolution: Revised**

At 809.6, change the title table 8-122 from “URI/FQDN Descriptor field encoding” to “URI/FQDN Descriptor field values” and change the heading of the first column in the table from “**URI/FQDN Descriptor” to “Value”**

And

At809.1, change as shown:

The URI/FQDN Descriptor field is defined in Table 8-122 (URI/FQDN Descriptor field encoding).

At 809.23, change as shown:

“The Public Identifier URI/FQDN field contains a ~~value in~~ URI ~~or FQDN~~ encoded using UTF-8 and formatted in accordance with RFC 3986 that points to a location object or an FQDN that identifies a location server.”

**CIDs 5170 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5170 | 788.19 | 8.4.2.21.10 |  |  | Location Configuration Information Report can also be included into an ANQP response (8.4.5.12). Thus, the figure heading is misleading, as it suggests that the report can only be included into a MR.Change the title from "Measurement Report field format for Location Configuration InformationReport" to "Location Configuration Information Report field format". | as suggested. |

**The cited text is below**

****

**The commenter’s proposed change is:**

Figure 8-209 - Location Configuration Information Report field format

**Proposed resolution: Revised**

Change the title to

Figure 8-209 - Format of Location Configuration Information report

**CID 5165 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5165 | 1776.43 | 10.25.3.2.1 |  |  | change Response to Request and the reference in parenthesis to 10.25.3.1.2 STA procedures to transmit a GAS Query. | as suggested |

**The cited text is below:**

****

 **The commenter’s proposed change is:**

The ANQP query request is transported in the Query Request field of

GAS Request frames as described in 10.25.3.1.2 (STA procedures to transmit a GAS Query

).

Not sure what “change response to request” refers to.

MAH proposed resolution: Propose: Revised. Change the referenced subclause to, "10.25.3.1.2 (STA procedures to transmit a GAS Query)"

**Proposed resolution: Revised**

Change the referenced subclause to, "10.25.3.1.2 (STA procedures to transmit a GAS Query)"

**CIDs 5997 (MAC) and 5998 (GEN)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5997 | 912.56 | 8.4.2.67.5 |  |  | RFC 3164 has been obsoleted by RFC 5424 | replace reference to RFC 3164 with RC 5424 |
| 5998 | 5.11 | 2 |  |  | RFC 3164 has been obsoleted by RFC 5424 | replace reference to RFC 3164 with RC 5424 |

**The cited text is below, see 3087.57 and 5.11**

****

****

**Changes will be:**

At 5.11 change as shown:IETF RFC 5424, TheSyslog Protocol, March. 2009.

At 912.56: portion of a WNM Log message as described in IETF RFC 5424

At 2947.22: as described in IETF RFC 5424

At 3087.57: as described in IETF RFC 5424.

**Proposed resolution: Accepted**

**CID 6349 (From 11-15-0565r12 “Motion MAC-AP pulled” tab)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6349 | 103.13 | 4.5.4.3 | It says "When the deauthentication service is terminating SAE authentication any PTKSA, GTKSA, mesh TKSA, or mesh GTKSA related to this SAE authentication is destroyed. If PMK caching is not enabled, deauthentication also destroys any PMKSA created as a result of this successful SAE authentication." 1) What about deleting any IGTKSA? 2) Is this not duplicated at "In an RSNA, deauthentication also destroys any related..." a few lines below? | Delete the cited paragraph | REVISED (MAC: 2015-06-25 18:39:54Z): Delete lines 13-16 on page 103. At 103.36 insert “Mesh GTKSA, Mesh TKSA, and Mesh PMKSA” after "(IGTKSA)" At 103.38 change the sentence to: If pairwise master key security association (PMKSA) caching is not enabled, deauthentication also deletes the PMKSA or Mesh PMKSA. |

**Proposed resolution –** no technical change from prior resolution – fixed editorial nits (proposed change left an “and” in the middle of the list).

**Proposed resolution: Revised**

Delete lines 13-16 on page 103
and
Change the paragraph at 103.32 as 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 or Mesh PMKSA.

Editor: Please check to see if the acronyms need to be expanded or not and adjust accordingly.

**CID 6398 (MAC) (From 11-15-0565r12 “Motion MAC-AP pulled” tab)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6398 | 1870.07 | 11.2.2.2 | Figure 11-1 refers to a Note but it is not clear what note is intended (the one in the next subclause?) | Identify the note in question | REJECTED (MAC: 2015-06-25 19:10:26Z): WEP has been deprecated and we are not making any changes to it. |

**Discussion:**

CID pulled from Motion, request to delete “Note”

Cited text is in WEP definition section. Text was present in 802.11-2012 and IEEE 802.11-2007. “Note” might refer to “NOTE” at 1871.1 (next page). WEP is deprecated.

Can consider a straw poll, proposed resolution written as keeping the proposed reject.

Straw poll:

We should:

1. Delete “note” 2
2. Reject the comment as initially proposed 4
3. Improve the reference to the existing NOTE

**Proposed resolution: Rejected**

WEP has been deprecated and the BRC has decided to not make any changes to it.

**CIDs 6511 (MAC) and 6183 (MAC) (From 11-15-0565r12 “Motion MAC-AR pulled” tab)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6511 | 2103.16 | 13.5.7 | It says "KDF-X"; X is undefined | Change to "KDF-Length" | REVISED (MAC: 2015-07-17 04:10:47Z): Make the changes as indicated in 11-15/764r3 (https://mentor.ieee.org/802.11/dcn/15/11-15-0764-03-000m-resolution-of-some-security-comments.docx) for clause 13. |
| 6183 | 2077.00 | 13 | In "AEK <- KDF-256(PMK, "AEK Derivation", Selected AKM Suite ||" (2103.1) and "MTK <- KDF-Length(PMK, "Temporal Key Derivation", min(localNonce, peerNonce) ||" (2103.10) what is the hash used? | Clarify (was PRF intended instead of KDF, perhaps?) | REVISED (MAC: 2015-07-17 04:10:14Z): Make the changes as indicated in 11-15/764r3 (https://mentor.ieee.org/802.11/dcn/15/11-15-0764-03-000m-resolution-of-some-security-comments.docx) for clause 13. |

**Disccussion:**

These 2 CIDs were discussed previously by the BRC and were pulled from motion on MAC-AR.

Requestor: not a technical change, don’t need to duplicate length specification. Change from

using the hash algorithm defined by the AKM in Table 8-130 to generate an AEK of length of 256 bits.

to

using the hash algorithm defined by the AKM in Table 8-130 to generate an AEK ~~of length of 256 bits~~.

**Propose to proceed with the text as in the cited document, sentence statement is accurate.**

**CID 6511: Proposed Resolution: Revised**

**Change the cited location as shown:** KDF-Hash-Length

Note to editor: This change is also made in <https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx>

**CID 6183: Proposed Resolution: Revised**

Incorporate the text changes in 11-15-0764r5 (<https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx> ) for section 13.5.7.

**CID 6184 (From 11-15-0565r12 “Motion MAC-AP pulled” tab) and**

**CID 6275 (From 11-15-0565r12 “Motion MAC-AR pulled” tab)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6184 | 1865.00 | 11 | In "KCK || PMK = KDF-512(keyseed, "SAE KCK and PMK"," (1884.56) and "TPK = KDF-Length(TPK-Key-Input, "TDLS PMK", min (MAC\_I, MAC\_R)" (1997.21) and "PMK = KDF-256(keyseed, "AP Peerkey Protocol"," (2030.54) and "KDF-Length(pwd-seed, "SAE Hunting and Pecking", p)" (1880.48 and 1883.9) what is the hash used? | Clarify (was PRF intended instead of KDF, perhaps?) | REVISED (MAC: 2015-06-25 18:43:06Z): Incorporate changes inserting "Hash" to KDF definition in document 11-15/076r2 (https://mentor.ieee.org/802.11/dcn/15/11-15-0764-02-000m-resolution-of-some-security-comments.docx) for section 11.6.9.2, 11.3.5.4, 11.3.4.3.2, 11.3.4.2.2. |
| 6275 | 1960.07 | 11.6.1.7.3 | It says "KDF-Hash-Length is the KDF as defined in 11.6.1.7.2 (Key derivation function (KDF)) used to generate a key of length 384 bits." but it's not being used to generate a key of length 384 bits, and it's not always 384 bits anwyay (see "Length" in the next para) | Delete "used to generate a key of length 384 bits" in the cited text | REVISED (MAC: 2015-07-17 00:16:33Z): Incorporate changes as shown in 11-15/764r3 (https://mentor.ieee.org/802.11/dcn/15/11-15-0764-03-000m-resolution-of-some-security-comments.docx) in section 11.6.1.7.3. |

**CID pulled from Motion MAC-AP: *“****For CID 6184 I would like to wait until we have the complete set of proposed changes (in 15/0764)”*

**Discussion:**

Sections identified in the prior CID 6184 resolution (noting the error in the resolution in document numbers: 11-15/076r2 (https://mentor.ieee.org/802.11/dcn/15/11-15-0764-02-000m-resolution-of-some-security-comments.docx) are:11.6.9.2, 11.3.5.4, 11.3.4.3.2, and 11.3.4.2.2.

This list is not complete.

11-15-0764 also includes changes in:

8.4.2.24.3

11.6.1.7.3 – called out in proposed resolution to CID 6275

11.6.1.7.4

11.6.1.7.5

11.6.1.7.5

11.10.2

13.5.7 – changes incorporated by CIDs 6511 and 6183

Introduction of “Hash” (CID 6275) and the corresponding changes for where it is referenced (KDF – CID 6184) affect all of the listed sections; changes are relevant to both comments.

**Proposed resolution to CIDs 6184 and 6275:**

**Revised**

Incorporate the text changes in 11-15-0764r5 (<https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx> ) for sections

11.6.9.2, 11.3.5.4, 11.3.4.3.2, 11.3.4.2.2,

8.4.2.24.3

11.6.1.7.3

11.6.1.7.4

11.6.1.7.5

11.10.2 and

13.5.7

Note to editor: this includes all changes in 11-15-0746r5 except for section 11.7.9 which is included by resolution to CID 6421.

**CIDs 6510 (MAC), 6509 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6510 | 1883.24 | 11.3.4.3.2 |  |  | It says "KDF-z"; z is undefined | Change to "KDF-Length" |
| 6509 | 1881.08 | 11.3.4.2.2 |  |  | It says "KDF-z"; z is undefined | Change to "KDF-Length" |

Discussion: Changes are also made in 11-15-0674r5.

Proposed resolution:

**CID 6509: Revised**

At 1881.08 change from”KDF-z” to “KDF-Hash-*Length”where “Length” is italic*

Note to editor: This change is also made in <https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx>

**CID 6510: Revised**

At 1883.24 change from”KDF-z” to “KDF-Hash-*Length”* *where “Length” is italic*

Note to editor: This change is also made in <https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx> .**CIDs 6365 (MAC) and 6364 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6365 | 1884.56 | 11.3.5.4 |  |  | "KCK || KEK" is not the way it's done anywhere else, and the inconsistency leads to unnecessary doubt | Change "KCK || PMK" to "kck\_and\_pmk" at 1884.56.Add "KCK = L(kck\_and\_pmk, 256, 256)" after the equation at 1884.56.Add "PMK = L(kck\_and\_pmk, 0, 256)" after the equation at 1884.56.In all cases, italicise "kck\_and\_pmk". |
| 6364 | 1884.56 | 11.3.5.4 |  |  | "KCK || KEK" is not the way it's done anywhere else, and the inconsistency leads to unnecessary doubt | Change "KCK || PMK" to "kck\_and\_pmk" at 1884.56.Add "KCK = L(kck\_and\_pmk, 0, 256)" after the equation at 1884.56.Add "PMK = L(kck\_and\_pmk, 256, 256)" after the equation at 1884.56.In all cases, italicise "kck\_and\_pmk". |

**Discussion:**

It is unclear that there is any need to make the change proposed by the commenter.

There is no technical error in the current text.

Proposed resolution:

**CID 6364: Rejected**

The text is clear as written; the comment does not identify an issue to be addressed.

**CID 6365: Rejected**

The text is clear as written; the comment does not identify an issue to be addressed.

Assign 6364, 6365, 6366 to Mark Rison as submission required.

**CID 6367 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6367 | 1880.57 | 11.3.4.2.2 |  |  | In "base = new-random-number" what is new-random-number and why is it not italic? | Define the term and make it italic |

**Discussion:**

Propose to remove dashes, and change text to a descriptive phrase

**Proposed resolution: Revised**

At 1880.57 change as shown:

*base* = a new random number

Note to editor: This change is also made in <https://mentor.ieee.org/802.11/dcn/15/11-15-0764-05-000m-resolution-of-some-security-comments.docx> .

**CID 6023 (GEN)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6023 | 31.63 | 3.2 | 3.2 defines "high throughput (HT) station (STA) 2G4" and "highthroughput (HT) station (STA) 5G" in terms of "an HT STA", but there isno definition of "HT STA" or "high throughput (HT) station (STA)". Whatis an "HT STA"? | Add definition for "HT STA". |

 **Discussion:**

The cited text is shown below:

** Discussion:** See clause 4.3.11, at 76.5. Is this good enough?

****

**Note that at 19.35, we define station:**

**station (STA):** A logical entity that is a singly addressable instance of a medium access control (MAC) and

physical layer (PHY) interface to the wireless medium (WM).

**Proposed resolution: Rejected**

An HT STA is described in Clause 4.3.11.

Altenate resolution:

**Proposed resolution: Revised**

At 31.61, insert the following definition:

**high throughput (HT) station (STA):** a station that supports high throughput (HT) medium access control (MAC) features described in Clause 9 and Clause 20 (High Throughput (HT) PHY specification) physical layer (PHY)

**CID 6295 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6295 |  |  |  |  | The things which are cached are the SAs, not just the Ks | Change "PMK cached" to "PMKSA cached" at 1926.5, "SMK cache" to "SMKSA cache" at 2903.32, "SMK caching" to "SMKSA caching" at 3287.31 |

**Discussion: The cited text is below.**

**1926.5:**

****

Discussion: changing “or PMK cached” to “or PMKSA cached” makes the definition circular.

**2903.32:**

****

Discussion: commenter proposed to change to “SMKSA cache”. “SMKSA cache” is not defined in the document. Submission required.

**3287.31**

****

Discussion: Line reference is wrong, line 21 applies. Commenter proposed to change to “SMKSA cache”. “SMKSA cache” is not defined in the document.

Submission required.

Assign to commenter

**CID 5062 (MAC)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5062 | 3489.06 | M.4.2 |  |  | The invocation of hmac\_sha1 at lines 4-5 includes a superfluous "digest," (the 2nd occurrence). | Change lines 4-5 to read: "hmac\_sha1(digest, ssidlength+4, (unsigned char\*) password, (int) strlen(password), digest1)" |

**Discussion:**



Propose to

1. Update the reference at 3488.7
2. Update the PSK definition at line 9 to have parameters that match the RFC 2898 Section 5.2
3. Delete clause M.4.2

**Proposed resolution: Revised**

At 3488.7 change as shown below:

The pass-phrase mapping defined in this subclause uses PBKDF2 as defined in IETF RFC 2898 section 5.2.[Bxx]

*PSK* = PBKDF2(*PassPhrase*, *ssid*, 4096, 256/8)

And add a reference to RFC 2898 in Annex A and delete the reference to B54.

At 3488.21, Delete: “— *ssidLength* is the number of octets of the *ssid*.”

Delete clause M.4.2.

In M.4.3, delete page 3490 lines 1, 7, and 14 (SSIDLength definitions)

Change

- the two instances of lowercase "passphrase" (both soft-hyphenated) in M.4.1 to "pass-phrase", at 3487.56, 3488.3

- "pass phrase" to "pass-phrase" at 3488.1

- "PassPhrase" to "passPhrase" at 3488.9

- "A pass-phrase is" to "passPhrase is" at 3488.13

- M.4.3 as follows:

Test case 1

~~Passphrase~~passPhrase = “password”

~~SSID~~ssid = { ‘I’, ‘E’, ‘E’, ‘E’ }

~~SSIDLength = 4~~

PSK = f42c6fc52df0ebef9ebb4b90b38a5f90 2e83fe1b135a70e23aed762e9710a12e

Test case 2

~~Passphrase~~passPhrase = “ThisIsAPassword”

~~SSID~~ssid = { ‘T’, ‘h’, ‘i’, ‘s’, ‘I’, ‘s’, ‘A’, ‘S’, ‘S’, ‘I’, ‘D’ }

~~SSIDLength = 11~~

PSK = 0dc0d6eb90555ed6419756b9a15ec3e3 209b63df707dd508d14581f8982721af

Test case 3

~~Password~~passPhrase = “aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa”

~~SSID~~ssid = {‘Z’,‘Z’,‘Z’,‘Z’, ‘Z’,‘Z’,‘Z’,‘Z’, ‘Z’,‘Z’,‘Z’,‘Z’, ‘Z’,‘Z’,‘Z’,‘Z’,

‘Z’,‘Z’,‘Z’,‘Z’, ‘Z’,‘Z’,‘Z’,‘Z’, ‘Z’,‘Z’,‘Z’,‘Z’,‘Z’,‘Z’,‘Z’,‘Z’}

~~SSIDLength = 32~~

PSK = becb93866bb8c3832cb777c2f559807c 8c59afcb6eae734885001300a981cc62

And insert the following sentence at the end of M.4.3:

Note that the passPhrase is not considered to have a terminating null.

**References:**

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