IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11me/D1.0 (LB258) | | | | |
| Date: 2022-06-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Mark RISON | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |

Abstract

This submission proposes resolutions for various CIDs on 11me/D1.0. Green indicates material agreed to in the group, yellow material to be discussed, red material rejected by the group and cyan material not to be overlooked. The “Final” view should be selected in Word (this means Word comments can be disregarded by the Editor).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1780  9.4.1.9  1078.27 | "REFUSED,  REFUSED\_REASON\_UNSPECIFIED" is not clear as to whether these are synonyms or a single enumeration tag | Delete "REFUSED," and change all other "REFUSED"s to "REFUSED\_REASON\_UNSPECIFIED"s |
| CID 1781  9.4.1.9  1078.27 | "REFUSED,  REFUSED\_REASON\_UNSPECIFIED" is not clear as to whether these are synonyms or a single enumeration tag | Change to "REFUSED or REFUSED\_REASON\_UNSPECIFIED" |

Discussion:

The TG expressed a preference for a single tag, and since in some contexts the reason can be specified, the tag needs to be the explicit one.

It turns out there is some confusion in the spec about result v reason v status codes.

The Reason Result Code field is not affected by these changes.

Proposed resolution:

REVISED

Delete “REFUSED,” at the referenced location and at 2262.21.

Change “REFUSED” to “REFUSED\_REASON\_UNSPECIFIED” at 404.3, 407.7, 516.16, 519.26/29/32, 537.39, 545.4, 546.37, 548.39, 550.33, 678.9, 679.29, 727.25, 729.62, 753.62, 755.55, 764.10, 766.3, 2782.52.

Change “result code” to “status code” at 2745.48/59 (assoc rsp), 2782.45/52/56 (addba rsp), 5689.19 (addts rsp).

Change “result code” to “reason code” at 2776.65, 2777.2/8/10 (delts).

At 3100.2 change “status field” to “Status Code field”; at 3100.7 change “the result code shall not take the value

“successful.”” to “the Status Code field shall not be SUCCESS.”; at 1051.11 change “Status code” to “Status Code” (auth).

Delete the full stop in the Valid Range cell at 764.11, 766.4.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1637  Mark RISON  9.6.15.1 | It's not immediately clear which frames can/do have a MIC element. I find:  The MIC element provides message integrity to mesh peering Management frames. The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering Open frame. The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering Confirm frame. The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering Close frame. Table 9-439--Mesh Group Key Inform frame Action field format shows both a MIC element and an AMPE (element) Table 9-440--Mesh Group Key Acknowledge frame Action field format ditto  The FTE shall have a MIC element count of zero (2x)  If dot11MeshSecurityActivated is true and the mesh STA shares a PMK with the candidate peer mesh STA but either the Mesh Peering element or the MIC element are not present in the frame, the frame shall be silently discarded. If dot11MeshSecurityActivated is false but either the Mesh Peering element or the MIC element is present in the frame, the frame shall be silently discarded.  When the mesh STA constructs a mesh peering Management frame [...] -- The input AAD shall be three distinct components consisting of  -- The localMAC -- The peerMAC -- The contents of the mesh peering Management frame from the category (inclusive) to the MIC element (exclusive) -- The output synthetic initialization vector shall be copied into the MIC field of the MIC element in the mesh peering Management frame -- The output cipher text shall become the remainder of the mesh peering Management frame after the MIC element  When the mesh STA verifies a mesh peering Management frame [...] -- The input synthetic initialization vector shall be the MIC field of the MIC element in the mesh peering Management frame -- The input cipher text shall be the part of the mesh peering Management frame following the MIC element -- The input AAD shall be three distinct components consisting of -- The peerMAC -- The localMAC -- The contents of the mesh peering Management frame from the category (inclusive) to the MIC element (exclusive)  When constructing protection on mesh group handshake frames [...] -- AAD shall be three distinct components as follows: -- The localMAC -- The peerMAC -- The contents of the mesh group key handshake frame from the category (inclusive) to the MIC element (exclusive) -- The synthetic initialization vector produced by AES-SIV shall be copied into the MIC field of the MIC element in the frame. -- The produced cipher text shall become the remainder of the mesh group key handshake frame after the MIC element.  When verifying the protection on the mesh group handshake frames [...] -- AAD shall be three distinct components as follows: -- The peerMAC -- The localMAC -- The contents of the mesh group key handshake frame from the category (inclusive) to the MIC element (exclusive) -- The synthetic initialization vector shall be the MIC field of the MIC element in the frame. -- The cipher text shall be the content after the MIC element in the frame. -- If AES-SIV validation function takes above input. -- If the function returns the special symbol "FAIL," the frame shall be discarded. -- If the plaintext is returned successfully, the produced plaintext shall be treated as the contents after the MIC element in the frame.  Mesh Group Key Inform frame shall be constructed as follows: [...] -- The MIC element shall be set according to the protection mechanism in 14.6.2 (Protection on mesh group key handshake frames).  Mesh Group Key Acknowledge frame shall be constructed as follows: [...] -- The MIC element shall be set according to the protection mechanism in 14.6.2 (Protection on mesh group key handshake frames).  Based on this, it's not immediately clear that you can have a Self-protected Action frame without a PMK. This suggests that Self-protected Action frame that is not protected is allowed! | After the first para of 9.6.15.1 add "NOTE---A Self-protected Action frame might not be protected." |

Discussion:

So yes, it turns out that you can have a Self-protected Action frame that is not protected (see first para of 9.6.15.1). This is somewhat counterintuitive!

Proposed resolution:

REVISED

At 238.62 change “The protection on each Self-protected Action frame is provided by the protocol that uses the

frame.” to “The protection on each Self-protected Action frame is optionally provided by the protocol that uses the frame.”

At 1965.50 change “NOTE—In Self-protected Action frames, the MIC element and the Authenticated Mesh Peering Exchange element are present after the Action field when the frame is protected (see 9.3.3.13 (Action frame format)).” to “NOTE—A Self-protected Action frame is not necessarily protected. When it is, the MIC element and the Authenticated Mesh Peering Exchange element are present after the Action field (see 9.3.3.13 (Action frame format)).”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1881  Mark RISON  12.4.8.6.3  3124.32 | One-mega-para stream-of-consciousness descriptions of procedures, mixing "if"s and "otherwise"s and "if so"s and "if not"s are not clear. Also, mixing shalls with the present tense casts doubt on the strength of the requirements given using the present tense | Change the referenced para to the following, where \* indicates indentation/bulleting:  Upon receipt of a Com event, the protocol instance shall check the status code in the Authentication frame:  \* If the status code is not SUCCESS, the protocol instance shall silently discard the frame and shall send a Del event to the parent process.  \* Otherwise, the password identifier, if any, shall be checked:  \*\* If a password identifier is present and no password is associated with that identifier, BadID shall be set and the protocol instance shall construct and transmit an Authentication frame with status code UNKNOWN\_PASSWORD\_IDENTIFIER.  \*\* If no password identifier is present or if a password is associated with that identifier, the finite cyclic group shall be checked:  \*\*\* If the group is not supported, BadGrp shall be set and the protocol instance shall construct and transmit an Authentication frame with status code UNSUPPORTED\_FINITE\_CYCLIC\_GROUP with the finite cyclic group set to the rejected group, and shall send a Del event to the parent process.  \*\*\* If the group is supported, the protocol instance shall zero the Sc and Rc counters and generate the PWE and the secret values according to 12.4.5.2 (PWE and secret generation). It shall then process the received SAE Commit message (see 12.4.5.4 (Processing of a peer's SAE Commit message)):  \*\*\*\* If validation of the received SAE Commit message fails, the protocol instance shall send a Del event to the parent process.  \*\*\*\* Otherwise, it shall construct and transmit an SAE Commit message (see 12.4.5.3 (Construction of an SAE Commit message)), (#595)increment Sc, and construct and transmit an SAE Confirm message (see 12.4.5.5 (Construction of an SAE Confirm message)). The Sync counter shall be set to 0 and the t0 (retransmission) timer shall be set. The protocol instance shall transition to the Confirmed state. |

Discussion:

As it says in the comment.

Proposed changes:

Change the referenced para as follows:

Upon receipt of a *Com* event, the protocol instance shall check the ~~Status of~~status code in the Authentication frame~~.~~:

* If the ~~S~~status code is not SUCCESS, the protocol instance~~frame~~ shall ~~be~~ silently discard~~ed~~ the frame and send a *Del* event ~~shall be sent~~ to the parent process.
* Otherwise, the ~~frame shall be processed by first checking whether a~~ password identifier ~~is present.~~, if any, shall be checked:
  + If ~~so~~a password identifier is present and ~~there is~~ no password is associated with that identifier, the protocol instance shall set *BadID* ~~shall be set~~ and ~~the protocol instance shall~~ construct and transmit an Authentication frame with ~~S~~status ~~C~~code ~~set to~~ UNKNOWN\_PASSWORD\_IDENTIFIER.
  + ~~If there is no password identifier present or if a password is associated with that identifier~~Otherwise, ~~the frame shall be processed by next checking~~ the ~~f~~Finite ~~c~~Cyclic ~~g~~Group field shall be checked:
    - ~~to see if the requested group is supported.~~ If the group is not supported, the protocol instance shall set *BadGrp* ~~shall be set and the protocol instance shall~~, construct and transmit an Authentication frame with ~~S~~status code UNSUPPORTED\_FINITE\_CYCLIC\_GROUP ~~indicating rejection with~~ and the ~~f~~Finite ~~c~~Cyclic ~~g~~Group field set to the rejected group, and ~~shall~~ send ~~the parent process~~ a *Del* event to the parent process.
    - ~~If the group is supported~~Otherwise, the protocol instance shall zero ~~the~~ *Sc* and *Rc* ~~counters~~ and ~~it shall~~ generate the ***PWE*** and the secret values according to 12.4.5.2 (PWE and secret generation). It shall then process the received SAE Commit message (see 12.4.5.4 (Processing of a peer’s SAE Commit message))~~.~~:
      * If validation of the received SAE Commit message fails, the protocol instance shall send a *Del* event to the parent process~~;~~.
      * ~~o~~Otherwise, ~~it~~the protocol instance shall construct and transmit an SAE Commit message (see 12.4.5.3 (Construction of an SAE Commit message)), (#595)increment *Sc* ***<note to Editor: this needs to be italicised>***, ~~and~~ construct and transmit an SAE Confirm message (see 12.4.5.5 (Construction of an SAE Confirm message))~~. The~~, set *Sync* ~~counter shall be set~~ to 0 ~~and~~, set the t0 (retransmission) timer ~~shall be set. The protocol instance~~, and transition~~s~~ to *Confirmed* state.

At 3125.7 change “check the finite cyclic group field being rejected” to “check the finite cyclic group being rejected”.

At 3125.20 change “the finite cyclic group field is checked” to “the Finite Cyclic Group field is checked”.

At 3124.22 change “*Sync* variable, *Rc*, and *Sc* variables” to “*Sync*, *Rc*, and *Sc* variables”.

At 3125.25 change “the *Sc* counter” to “*Sc*”.

At 3126.36/61 change “the *Rc* variable” to “*Rc*”.

At 3126.1/3/40/43/55 change “the *Sync* counter” to “*Sync*”.

At 3126.62 change “the *Sync*” to “*Sync*”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1881 in <this document>, which make the changes proposed by the commenter, with minor editorial tweaks.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1592  Mark RISON  12.4.7.4 | There are editorial issues with the description of encoding and decoding of SAE Commit messages | Make the changes indicated in 21/1130 |
| CID 1810  Mark RISON  12.4.7.4  3118.51 | The wording could be made more straightforward and consistent | Change the second para to "An SAE Commit message shall include a Finite Cyclic Group field (see 9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (see 9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (see 9.4.1.40 (FFE field)). If the SAE Commit message is in response to an Anti-Clogging Token field request (see 12.4.7.6 (Status codes)), an Anti-Clogging Token field shall be included (see 9.4.1.38 (Anti-Clogging Token field)). When the PWE is derived using the hash-to-element method, the Anti-Clogging Token field is encapsulated in an Anti-Clogging Token Container element; otherwise, the Anti-Clogging Token field is included in the frame outside of an element as described in Table 9-41 (Presence of fields and elements in Authentication frames). If a password identifier is used in generation of the password element (PWE) a Password identifier element shall be included and the identifier shall be encoded as a UTF-8 string in the Identifier portion of the element (see 9.4.2.216 (Password Identifier element)). If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if any, to the Rejected Groups field of the Rejected Groups element (see 9.4.2.246 (Rejected Groups element)). Each rejected group shall be represented using the ordering conventions of 9.2.2 (Conventions). If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent and any groups have been rejected during the current SAE session, the Rejected Groups element shall be present, otherwise it shall not be present. " |
| CID 1798  Mark RISON  12.4.7.4  3118.62 | "If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if any, to the Rejected Groups field of the Rejected Groups element." -- behaviour is unclear if a group is offered (and hence rejected) twice | Change to "If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if any, to the Rejected Groups field of the Rejected Groups element, if not already present there." |
| CID 1811  Mark RISON  12.4.7.4  3118.54 | "If the SAE Commit message is in response to an Anti-Clogging Token field request (see 12.4.7.6 (Status codes)), an Anti-Clogging Token field shall be included (see 9.4.1.38 (Anti-Clogging Token field))" -- missing the otherwise case | Append "; otherwise it shall not be included" |

Discussion:

As it says in the comments. Note re CID 1811 that “otherwise it shall not be included” is missing for the Password Identifier element too.

Proposed changes:

Change 9.4.2.246 Rejected Groups element at 1680.82 as follows:

The Rejected Groups field contains ~~a list of~~one or more Finite Cyclic Group fields indicating all of the finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

Change 12.4.7.4 Encoding and decoding of SAE Commit messages as follows:

An SAE Commit message shall be encoded as an Authentication frame with an Authentication Algorithm Number field set to 3, a Transaction Sequence Number of 1 and a Status Code of SUCCESS or SAE\_HASH\_TO\_ELEMENT. Status codes not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT indicate a rejection of a peer’s SAE Commit message and are described in 12.4.7.6 (Status codes).

An SAE Commit message shall ~~consist of~~include a Finite Cyclic Group field (9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (9.4.1.40 (FFE field)). ***<insert para break>***

If the SAE Commit message is ~~in response to~~a request for an Anti-Clogging Token field or in response to such a request (see 12.4.7.6 (Status codes)), ~~the~~an Anti-Clogging Token field ~~is present~~shall be included (see 9.4.1.38 (Anti-Clogging Token field)); otherwise it shall not be included. When the PWE is derived using the hash-to-element method, the Anti-Clogging Token field is encapsulated in an Anti-Clogging Token Container element; otherwise, the Anti-Clogging Token field is included in the frame outside of an element as described in Table 9-69 (Presence of fields and elements in Authentication frames). ***<insert para break>***

If a password identifier is used in generation of the ~~password element (~~PWE~~) the~~ a Password ~~i~~Identifier element shall be ~~present~~included and the identifier shall be encoded as a UTF-8 string in the Identifier ~~portion of the element~~field (see 9.4.2.216 (Password Identifier element)); otherwise it shall not be included.

If the status code of the SAE Commit message is SAE\_HASH\_TO\_ELEMENT and if any groups have been rejected during the current SAE session, a Rejected Groups element shall be included (see (9.4.2.246 Rejected Groups element)); otherwise it shall not be included.

If an SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of an ~~previous~~ SAE Commit message with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if ~~applicable~~any, to the Rejected Groups field of the Rejected Groups element, if not already present there.

NOTE—Each rejected group ~~shall be~~is represented as an unsigned 16-bit integer using the bit ordering conventions of 9.2.2 (Conventions).

When transmitting an SAE Commit message, the scalar and element shall be converted to octet strings and placed in the Scalar field and FFE field, respectively. The scalar shall be treated as an integer and converted into an octet string of length *m* such that 2*8m* > *r*, where *r* is the order of the group, according to 12.4.7.2.2 (Integer to octet string conversion), and the element shall be converted into (an) octet string(s) according to 12.4.7.2.4 (Element to octet string conversion). When receiving an SAE Commit message the component octet strings in the Scalar field and FFE field shall be converted into a scalar and element, respectively, according to 12.4.7.2.3 (Octet string to integer conversion) and 12.4.7.2.5 (Octet string to element conversion), respectively.

Proposed resolution:

Make the changes shown under “Proposed changes” for CID 1592, 1798, 1810, 1811 in <this document>, which make the changes suggested by the commenter, with minor editorial tweaks.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1980  Mark RISON | There are technical and editorial issues with the description of "group addressed privacy" | Make the changes shown under "Proposed resolution" under CID 453 in 21/0829 (latest revision) |

Discussion:

“Group addressed privacy” (without the quotes) is a column heading and “group addressed privacy” (without the quotes) is a concept.

Note that by definition an Action frame that supports group addressed privacy is a robust Action frame. Also note that this concept only applies to Action frames, not to other Management frames. And Action frames are not specified with a Yes or No in T9-51, their category is.

Proposed resolution:

REVISED

In 4.5.4.9 change:

Management frame protection protocols in an MBSS apply to the following frames:

— Individually addressed robust Management frames after establishment of the RSNA MTK,

— Group addressed robust Management frames that are specified with Yes in the “Group Addressed Privacy” column of Table 9-79 (Category values) after establishment of the RSNA MGTK, and

— Group addressed robust Management frames that are specified with No in the “Group Addressed Privacy” column of Table 9-79 (Category values) after establishment of the RSNA IGTK.

to:

Management frame protection protocols in an MBSS apply to the following frames:

— Individually addressed robust Management frames, after establishment of the MTK,

— Group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), after establishment of the MGTK, and

— Group addressed robust Management frames that are not Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), after establishment of the IGTK.

Change “RSNA PTK” to “PTK” in 4.5.4.9, “RSNA GTK” to “GTK” in C.3 (3x).

In Table 9-71 change:

The MME is present when management frame protection is enabled at the AP, the frame is a group addressed robust Action frame, and the category of the Action frame does not support group addressed privacy as indicated by Table 9-79 (Category values).

to:

The MME is present when management frame protection is enabled at the AP and the frame is a group addressed robust Action frame not of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values).

In 11.12 change:

In an MBSS, for group addressed Management frames that are specified with Yes in the Group Addressed Privacy column of Table 9-79 (Category values)

to:

In an MBSS, for group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values)

In 12.5.3.1 and 12.5.5.1 change:

individually addressed robust Management frames and (MBSS only) the group addressed Management frames that receive “Group Addressed Privacy” as indicated in Table 9-79 (Category values) shall be protected

to:

individually addressed robust Management frames, and (MBSS only) group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), shall be protected

In 14.7 change:

all individually addressed mesh Data frames and individually addressed robust Management frames (see 12.2.7 (Requirements for management frame protection)) shall be protected by the mesh PTKSA, and all group addressed Data frames and group addressed Action frames that are indicated as “Group Addressed Privacy” in Table 9-79 (Category values) shall be protected by the mesh GTKSA.

to:

individually addressed mesh Data frames and individually addressed robust Management frames (see 12.2.7 (Requirements for management frame protection)) shall be protected by the mesh PTKSA, and group addressed Data frames, and group addressed Action frames of a category specified with Yes in the Group addressed privacy column of Table 9-79 (Category values), shall be protected by the mesh GTKSA.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 2297  Stephen McCANN  3.2  214.49 | The term "high throughput (HT)" does not use a hyphen. | Change "high throughput (HT)" to "high-throughput (HT)". |

Discussion:

It is not clear whether “high-throughput” should have a hyphen. Grammatically, as an adjective, it should, but IEEE 802.11 hates hyphens, and “high-throughput” is not on the list of exceptional permissions to use hyphens. Note also that “very high throughput” doesn’t have hyphens either.

Proposed resolution #1:

REVISED

Change “high throughput” to “high-throughput” at 2.18, 214.49, 229.40.

Change “High Throughput SIGNAL field” to “high-throughput SIGNAL field” at 239.59.

Change “High Throughput” to “High-Throughput” at 1338.37 (leftmost instance), 1339.55, 1339.59, 5389.46.

Proposed resolution #2:

REVISED

Change “high-throughput” to “high throughput” at 207.27/41, 208.23/38/44, 209.30/42/47/51/54/59/63, 210.10, 211.10, 224.22/26/31/34/38/44/48/54/58, 225.1/3, 227.34, 228.25, 240.6, 255.35/37/38/40/41, 3532.9, 4922.13/14.

Change “High-throughput” to “High throughput” at 279.37, 3532.1, 4928.52, 5047.27.

Change “High Throughput SIGNAL field” to “high throughput SIGNAL field” at 239.59.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1948  Mark RISON  3.2 | "non-HE PPDU" is not defined. Does it include S1G PPDUs, for example? | Add a definition based on the non-HT definition, but adding HT and VHT PHYs to the list |

Discussion:

We have a definition of non-HT PPDUs:

**non-high-throughput (non-HT) physical layer (PHY) protocol data unit (PPDU):** A PPDU that is transmitted by a Clause 15 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), Clause 17 (Orthogonal frequency division multiplexing (OFDM) PHY specification), or Clause 18 (Extended Rate PHY (ERP) specification) PHY, or not using a TXVECTOR FORMAT parameter equal to HT\_MF, HT\_GF or VHT.

However, we don’t have a definition of non-HE PPDUs.

Note that HT and VHT PHYs’ TXVECTOR includes a FORMAT parameter, so the clauses don’t need to be explicitly listed.

Proposed resolution:

REVISED

Add the following definition in Clause 3.2:

**non-high-efficiency (non-HE) physical layer (PHY) protocol data unit (PPDU):** A PPDU that is transmitted by a Clause 15 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), Clause 17 (Orthogonal frequency division multiplexing (OFDM) PHY specification), or Clause 18 (Extended Rate PHY (ERP) specification) PHY, or not using a TXVECTOR FORMAT parameter equal to HT\_MF, HT\_GF, VHT or HE.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1273  Jouni MALINEN  12.7.2  3206.27 | The current shall requirement for the Authenticator to change the GTK based on any authenticated EAPOL-Key Request frame with key type Group might be problematic in cases where the associated stations/Supplicants cannot be fully trusted. This requirement would allow any Supplicant to force a GTK change at any point in time and arbitrarily frequently. That could result in reduced performance for group-addressed frame delivery and undesired resource consumption for other associated STAs. The Authenticator should be in control on when the GTK is changed and while the Supplicants could be allowed to request changes, they should not be allowed to force this to happen. The current text is as follows: "If the EAPOL-Key frame in which the Request bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way handshake with the Supplicant, and then execute the group key handshake to all Supplicants." | Replace "the Authenticator shall change the GTK" with "the Authenticator may change the GTK".  Replace "execute the group key handshake to all Supplicants" with "execute the group key handshake to all Supplicants, if the GTK was changed" |
| CID 1476  Mark RISON  12.7.2  3206.25 | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." has many issues | Change to "If the EAPOL-Key frame in which the Request bit is 1 has a key type of Group, the Authenticator is not currently performing GTK rekeying and the requesting Supplicant has not recently made such a request, the Authenticator shall generate a new GTK with a new key ID (see 12.7.10 (RSNA Authenticator key management state machine)) and then execute the group key handshake with all Supplicants that are not in WNM sleep mode to deliver them, except a Supplicant for which it is currently performing PTK rekeying, in which case if it has not yet transmitted message 3 it shall deliver them in that message instead, and if it has already transmitted message 3 it shall perform the group key handshake after the end of the 4-way handshake." |
| CID 1848  Mark RISON  12.7.7.1  3226.45 | "The Supplicant may trigger a group key handshake by sending an EAPOL-Key frame with the Request bit set  to 1 and the type of the Group Key bit." -- doesn't say this causes a new GTK (cf. 12.7.2), and an equivalent statement for the 4WH is missing from 12.7.6 | Change to "The Supplicant may trigger a group key handshake and obtain a new GTK by sending an EAPOL-Key request frame with a key type of Group (see 12.7.2)." At 3216.41 add "The Authenticator may trigger a 4-way handshake and obtain a new PTK by sending an EAPOL-Key request frame with a key type of Pairwise (see 12.7.2)." |
| CID 1449  Mark RISON  12.7.2  3206.25 | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." -- there's no need to execute a GKH if a 4WH has just been executed | Change to "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the requesting Supplicant, and then execute the group key handshake to all other Supplicants." |
| CID 1450  Mark RISON  12.7.2  3206.25 | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." is open to abuse | Change to "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator is not currently in the process of handling such a request and the requesting Supplicant has not recently made such a request, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." |
| CID 1451  Mark RISON  12.7.2  3206.25 | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." -- there's no need to execute a 4WH | Change to "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK and then execute the group key handshake to all Supplicants." |
| CID 1452  Mark RISON  12.7.2  3206.25 | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall change the GTK, initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to all Supplicants." -- the GTK isn't changed per se, it's updated | "If the EAPOL-Key frame in which the Request  bit is 1 has a key type of Group, the Authenticator shall generate a new GTK with a new key ID (see 12.7.10 (RSNA Authenticator key management state machine)), initiate a 4-way  handshake with the Supplicant, and then execute the group key handshake to deliver this new GTK to all Supplicants." |
| CID 1846  Mark RISON  12  3206.24 | It is not clear whether an EAPOL-Key request (pairwise) necessarily causes the GTK to be changed | At 3206.28 add "NOTE---The GTK is not necessarily changed in response to an EAPOL-Key request frame that has a key type of Pairwise." |
| CID 1942  Mark RISON  12 | EAPOL-Key request frames are defined but have no behaviour apart from having a separate replay counter (but not clear separate to what); all the behaviour is instead described in terms of frames with the Request bit set | Recast the material about frames with the Request bit set to be about EAPOL-Key request frames |

Discussion:

As these comments indicate, there are various issues with the current specification of EAPOL-Key request frames:

* A requirement to rekey is open to abuse/misuse
* There is no point doing a 4WH in response to a GTK rekeying request (see CID 1272, accepted in principle on 2022-03-09)
* It’s not always clear whether the GTK is actually changed following a GTK rekeying request
* It’s not made clear that GTK rekeying involves a changed key ID
* The behaviour for a GTK rekeying request if PTK or GTK rekeying is currently in progress isn’t clear
* The behaviour w.r.t. STAs in WNM sleep mode isn’t clear
* The effect of PTK rekeying on the GTK could be spelt out (viz. that the GTK isn’t changed)

Jouni MALINEN has also raised concerns about the

NOTE—While the MIC calculation is the same in each direction, the Key Ack bit is different in each direction. It is set in EAPOL-Key frames from the Authenticator and 0 in EAPOL-Key frames from the Supplicant. 4-way handshake requests from the Supplicant have the Request bit equal to 1. The Authenticator and Supplicant need to check these bits to stop reflection attacks. It is important that message 1 contents not be used to update state, in particular the keys in use, until the data are validated with message 3.

in 12.7.6.1:

Most of this note is talking about protection against reflection attacks and for that, it is critical for EAPOL-Key frames from each party always be clearly distinct from any frame sent by the other party. That note about requesting a 4-way handshake is not really something that should be interpreted to talk only about rekeying requests, i.e., it is about any EAPOL-Key request frame. For this context, that sentence would be worded with something like "EAPOL-Key request frames from the Supplicant have the Request bit equal to 1 while all the EAPOL-Key frames from the Authenticator have the Request bit equal to 0." In other words, the key point here is that the EAPOL-Key request frames differ from any EAPOL-Key frame that the Authenticator could send. Furthermore every EAPOL-Key frame from the Authenticator has Key Ack = 1. This bit alone should actually be sufficient to stop reflection attacks, i.e., the part about the Request bit should not really be needed since the EAPOL-Key request frames are supposed to use Key Ack = 0 even though they sometimes expect a response. Maybe someone in TGi 20 or so years ago thought that Key Ack = 1 might be used EAPOL-Key request frames.

The last sentence of the note is not related to reflection attacks.

I'd assume this note was added as an attempt to make implementors aware of a critical requirement for the 4-way handshake to be secure. It does not look like this location for the note is really ideal. 12.7.6.6 (4-way handshake implementation considerations) would seem to be a more appropriate location for the last two sentences (with the "these bits" needing to be expanded if the prior sentence are not included there) and the rest of this note would seem to be more appropriate for 12.7.6.8 (4-way handshake analysis) which already covers this very topic in the penultimate paragraph.

Open questions for group discussion:

* Another possible response to a Supplicant that is making excessive PTK or GTK rekeying requests would be to deauth/disassoc it. Should this be mentioned?
* Should it be allowed to “sneak in” the new GTK if a 4WH happens to be in progress and M3 has not yet been sent?
* Does it need to be specified that the GKH needs to be deferred until the end of the 4WH otherwise, or should it be expected that Supplicants will be able to cope with a 4WH and GKH in parallel (possibly with different GTKs and key IDs)?
* Should the process by which GTK rekeying is performed be moved from 12.7.2 (format) to 12.6.21 (behaviour)?

Note that under CID 1571 "EAPOL-Key frame in which the Request bit is 1" becomes just "EAPOL-Key request frame". Ditto CID 1440 and “EAPOL request message”

Related comments not addressed here: CIDs 1844/1845, 1944.

Proposed changes:

Change the para at 3206.24 (in 12.7.2 EAPOL-Key frames) as follows, (re)numbering NOTEs as appropriate:

Alternative 1a:

If the Authenticator receives an EAPOL-Key frame in which the Request bit is 1 ~~has~~with a key type of Pairwise and the Authenticator is not currently performing a 4-way handshake with the Supplicant, the Authenticator ~~shall~~ should perform PTK rekeying by initiating~~e~~ a 4-way handshake with the Supplicant.

NOTE 1—The Authenticator might ignore the request if, for example, it has recently performed a 4-way handshake with the Supplicant.

NOTE 2—The GTK is not changed in response to an EAPOL-Key request frame with a key type of Pairwise. ***<insert para break>***

Alternative 1b:

If the Authenticator receives an EAPOL-Key frame in which the Request bit is 1 ~~has~~with a key type of Pairwise and the Authenticator is not currently performing a 4-way handshake with the Supplicant, the Authenticator shall perform PTK rekeying by initiating~~e~~ a 4-way handshake with the Supplicant.

NOTE 1—The GTK is not changed in response to an EAPOL-Key request frame with a key type of Pairwise. ***<insert para break>***

Alternative 2a:

If the Authenticator receives ~~the~~an EAPOL-Key frame in which the Request bit is 1 ~~has~~with a key type of Group and the Authenticator is not currently performing GTK rekeying, the Authenticator ~~shall~~ should perform GTK rekeying as follows:

* ~~change the~~ generate a new GTK with a new key ID (see 12.7.10 (RSNA Authenticator key management state machine))~~, initiate a 4-way handshake with the Supplicant, and then~~
* ~~execute~~initiate ~~the~~a group key handshake ~~to~~with ~~all~~each Supplicant~~s~~ that is not in WNM sleep mode, except a Supplicant with which it is currently performing a 4-way handshake, in which case if it has not yet transmitted message 3 it may deliver the GTK in that message instead, or otherwise it shall initiate the group key handshake after the end of the 4-way handshake~~.~~

NOTE 3—The Authenticator might ignore the request if, for example, it has recently performed GTK rekeying (whether on request from the same Supplicant or otherwise).

Alternative 2b:

If the Authenticator receives ~~the~~an EAPOL-Key frame in which the Request bit is 1 ~~has~~with a key type of Group and the Authenticator is not currently performing GTK rekeying, the Authenticator ~~shall~~ should perform GTK rekeying as follows:

* ~~change the~~ generate a new GTK with a new key ID (see 12.7.10 (RSNA Authenticator key management state machine))~~, initiate a 4-way handshake with the Supplicant, and then~~
* ~~execute~~initiate ~~the~~a group key handshake ~~to~~with ~~all~~each Supplicant~~s~~ that is not in WNM sleep mode, except a Supplicant with which it is currently performing a 4-way handshake, in which case it shall initiate the group key handshake after the end of the 4-way handshake~~.~~

NOTE 3—The Authenticator might ignore the request if, for example, it has recently performed GTK rekeying (whether on request from the same Supplicant or otherwise).

Alternative 2c:

If the Authenticator receives ~~the~~an EAPOL-Key frame in which the Request bit is 1 ~~has~~with a key type of Group and the Authenticator is not currently performing GTK rekeying, the Authenticator ~~shall~~ should perform GTK rekeying as follows:

* ~~change the~~ generate a new GTK with a new key ID (see 12.7.10 (RSNA Authenticator key management state machine))~~, initiate a 4-way handshake with the Supplicant, and then~~
* ~~execute~~initiate ~~the~~a group key handshake ~~to~~with ~~all~~each Supplicant~~s~~ that is not in WNM sleep mode~~.~~

NOTE 3—The Authenticator might ignore the request if, for example, it has recently performed GTK rekeying (whether on request from the same Supplicant or otherwise).

Change the para at 3226.45 (in 12.7.7 Group key handshake; 12.7.7.1 General) as follows, (re)numbering NOTEs as appropriate:

The Supplicant may ~~trigger~~ request a group key handshake to obtain a new GTK by sending an EAPOL-Key request frame with ~~the Request bit set to 1 and the type of the Group Key bit~~ a key type of Group (see 12.7.2).

NOTE—The Authenticator might ignore this request.

Delete the NOTE at 3216.42 (in 12.7.6 4-way handshake; 12.7.6.1 General):

~~NOTE—While the MIC calculation is the same in each direction, the Key Ack bit is different in each direction. It is set to 1 in EAPOL-Key frames from the Authenticator (if an EAPOL-Key frame is required in response) and 0 in EAPOL-Key frames from the Supplicant. 4-way and group handshake requests from the Supplicant have the Request bit equal to 1 and the Error bit equal to 0. The Authenticator and Supplicant need to check these bits to stop reflection attacks. It is important that message 1 contents not be used to update state, in particular the keys in use, until the data are validated with message 3.~~

Add the following paras at the end of 12.7.6.6 4-way handshake implementation considerations:

The Authenticator and Supplicant shall check the Key Ack and Request bits in EAPOL-Key frames to stop reflection attacks.

The Supplicant shall not use message 1 contents to update state, in particular the keys in use, until validated with message 3.

At 3216.47 (in 12.7.6 4-way handshake; 12.7.6.1 General) add a para, (re)numbering NOTEs as appropriate:

The Supplicant may request a 4-way handshake to obtain a new PTK by sending an EAPOL-Key request frame with a key type of Pairwise (see 12.7.2).

NOTE—The Authenticator might ignore this request. ***[not if we pick Alternative 1b above]***

Change 3186.43 (in 12.6.21 RSNA rekeying) as follows:

A ~~s~~Supplicant may send an EAPOL request message to the ~~a~~Authenticator to request rekeying (see 12.7.2).

NOTE—The Authenticator might ignore this request. ***[only for GTK rekeying, if we pick Alternative 1b above]***

At 1956.53 change “a group rekeying” to “GTK rekeying”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1273 et al. in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1382  Mark RISON | "An Authenticator may initiate a 4-way handshake for the purpose of renewing the key associated with a  PTKSA" -- renewing should be tied to rekeying, perhaps by defining rekeying as the act of renewing a key on a link that already has that type of key (e.g. pairwise). But note that with EKID you're not necessarily renewing that key, potentially just adding another key | At 847.33 change "renewal of an expiring RSN SA" to "rekeying to renew an expiring SA". At 847.46 change "RSN keys expired and could not be renewed" to "RSN keys expired and could not be renewed by rekeying". At 850.22 and 851.31 change "RSN SA" to "SA". Change the cited text to "An Authenticator may initiate a 4-way handshake for the purpose of renewing a key associated with a SA, or, when extended key IDs for individually addressed frames are supported, to provide an additional PTK for a PTKSA" |

Discussion:

At the moment, the spec sometimes talks of renewing keys, sometimes of refreshing, and sometimes of rekeying, and it is not immediately obvious that these are the same thing. In addition, using different terms makes it harder to search the 6000-page spec for the corresponding requirements. “rekey” should be the key word.

In a TG discussion in early 2022, it was noted that a key is rekeyed while an SA is renewed (and that the only way to renew an SA is to rekey). In a TG discussion on 11 April 2022 it was agreed that a given PTKSA only has one PTK (so for EKID you have two PTKSAs).

Arguably, in the initial stages of EKID, you are not really rekeying (you set the PTK for key ID 0, then you set the PTK for key ID 1, and only then do you start rekeying). Ditto for the GTK. However, per CID 1381, it probably simplest to include this under the term “rekeying”.

Also, an “RSN SA” is not a defined term. It’s just an SA, or actually a security association, since an SA is a source address.

Proposed changes:

Change 6.4.4.1.2 From ESS\_DISENGAGING as follows:

To make this transition, the SME cancels a previous event that predicted an ESS link failure. This might be due to network parameters indicating renewed link strength or a successful renewal of an expiring ~~RSN SA~~ security association (by rekeying; see 12.6.21).

Change 6.4.4.2.1 From ESS\_CONNECTED as follows:

This transition indicates that administrative action was taken to shut down the link, a sudden loss of signal strength or that ~~RSN keys~~ a security association expired and could not be renewed (by rekeying; see 12.6.21).

Change 6.4.7.2.2 Semantics of the service primitive (in 6.4.7.2 MSGCF-ESS-LINK-DOWN.indication) and 6.4.7.3.2 Semantics of the service primitive (in 6.4.7.3 MSGCF-ESS-LINK-GOING-DOWN.indication) as follows:

~~Keys used by an RSN SA have~~ A security association has expired due to time or traffic limitations, or  
TKIP countermeasures have invalidated the key hierarchy.

Change 12.6.21 RSNA rekeying as follows:

When a PTKSA is deleted, a non-AP and non-PCP STA may reassociate with the same AP or PCP and/or establish a new ~~RSNA~~PTKSA with the AP or PCP. If the non-AP and non-PCP STA has cached one or more PMKSAs, it may skip the PMKSA establishment and proceed with the creation of a new PTKSA ~~by using~~via a 4-way handshake, an FT 4-way handshake, or FILS authentication using the procedures defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a GTKSA is deleted, a~~n originating~~ non-AP and non-PCP STA may create a new GTKSA ~~by using~~via a 4-way handshake or a group key handshake.

Rekeying is the process by which an existing security association is renewed or a new instance of an existing type of security association (e.g. PTKSA, GTKSA) is created.

NOTE—This includes adding a second PTKSA when extended key IDs for individually addressed frames are supported and changing the GTK when GTK rekeying. In both these cases the key ID differs from the key ID currently in use for that type of security association.

An Authenticator may initiate a 4-way handshake for the purpose of PTK rekeying (~~renewing the key associated~~ with a PTKSA).

An Authenticator may initiate a group key handshake for the purpose of GTK rekeying (with a GTKSA), IGTK rekeying (with an IGTKSA), BIGTK rekeying (with a BIGTKSA) or WIGTK rekeying (with a WIGTKSA).

At 3242.41 and 3243.29 change “GTKReKey” to “GTKRekey”.

At 3120.27, 3152.50, 3157.22/32, 3162.54, 5256.17/32/46, 5261.29 change “refreshed” to “refreshed (by rekeying)”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1382 in <this document>, which make changes in the direction suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1398  Mark RISON | "This standard assumes" -- it shouldn't assume, it should mandate | Change the ~9 instances of "standard assumes" to "standard relies on the fact that" (I can provide locations) |
| CID 1397  Mark RISON  12.6.9  3177.16 | "This standard assumes that IEEE Std 802.1X-2010 does not block the Controlled Port when authentication is  triggered through reauthentication." is odd. It's a matter of fact: does IEEE Std 802.X-2010 do so or does it not? | Change to "This standard relies on the fact that IEEE ..." |

Discussion:

As it says in the comment. However, at least one location is believed to refer to assumptions on entities outside the scope of the 802.11 standard.

Proposed changes:

Make the changes indicated at the following locations:

353.25: ~~In order for~~To ensure the MAC ~~to~~ operates properly, ~~this standard assumes that~~ the DS shall meet~~s~~ the MSDU (“object”) reordering requirements of IEEE Std 802.1AC-2012 [B17].

2927.51: In an infrastructure BSS, the Interworking element contains signaling for HeSSs(M12). The HESSID is a 6-octet MAC address that identifies the HeSS(M12). The HESSID value shall be identical to one of the BSSIDs in the HeSS(M12) and all BSSs in the HeSS shall use the same value. Thus, it is a globally unique identifier that, in conjunction with the SSID, may be used to provide network identification for an SSPN.

~~NOTE 1—This standard assumes that the HESSID field in the Interworking element is administered consistently across all BSSs in an HeSS(M12).~~

NOTE ~~2~~—The concept of an HeSS is orthogonal to an ESS, and any SSIDs can be used by the BSSs that provide access to the HeSS. For more information on HeSS, refer to Wi-Fi Alliance documents [B59] and [B60].(M12)

2960.50: ~~NOTE—This standard assumes that all APs in an ESS are configured consistently for QMF service~~ All APs in an ESS shall have the same QMF settings when GQMF has been enabled for use by associated non-AP STAs.

3168.25: NOTE—The IEEE 802.1X Uncontrolled Port allows IEEE 802.1X frames to pass between the Supplicant and Authenticator. […] ***<para break, move out of NOTE>***

Supplicants without a Controlled Port compromise RSN security and shall not be used.

NOTE—Although IEEE Std 802.1X-2010 does not require a Supplicant Controlled Port, this standard ~~assumes~~relies on the fact that the Supplicant has a Controlled Port in order to provide the needed level of security. ~~Supplicants without a Controlled Port compromise RSN security and are not used.~~

3176.40: When the policy selection process chooses IEEE 802.1X authentication, this standard ~~assumes~~relies on the fact that IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled ~~p~~Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between the STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port. The security of an RSNA depends on this ~~assumption~~ being true. *[note the security is in the blocking of the CP, not on the exchanging of 1X stuff via the UP]*

3177.5: ~~This standard assumes~~ NOTE—IEEE Std 802.1X maintains each Controlled Port ~~remains~~in a blocked state until the IEEE 802.1X state variables portValid and keyDone both become true. This ~~assumption~~ means that the IEEE 802.1X Controlled Port discards MSDUs sent across the IEEE 802.11 channel prior to the installation of cryptographic keys into the MAC.

3177.16: ~~This standard assumes that~~ NOTE—IEEE Std 802.1X-2010 does not block the Controlled Port when authentication is triggered through IEEE 802.1X reauthentication. During ~~IEEE 802.1X~~ reauthentication, an existing RSNA can protect all MSDUs exchanged between the STAs. Blocking MSDUs is not required during reauthentication over an RSNA.

3182.3: When the IEEE 802.1X authentication completes successfully, ~~this standard assumes that~~ the STA’s IEEE 802.1X Supplicant and the IEEE 802.1X AS share a secret, called a PMK.

3197.46: The PMK-R1s are generated by the R0KH and ~~are assumed to~~shall be delivered from the R0KH to the R1KHs within the same mobility domain.

3197.52: ~~It is assumed by this standard that t~~The PSK ~~is~~shall be specific to a single S0KH and a single R0KH.

3198.39: The distribution of keys from the R0KH to the R1KHs is outside the scope of this standard. ~~It is assumed that t~~The PMK-R1s ~~are~~shall be distributed from the R0KH to the R1KHs following the requirements specified in 13.2.2 (Authenticator key holders).

3269.48: Each R0KH-ID and R1KH-ID ~~is assumed to~~shall be expressed as a unique identifier within the mobility domain.

3270.24: The R0KH and the R1KH ~~are assumed to~~shall have a secure channel between them that can be used to exchange cryptographic keys without exposure to any intermediate parties. The cryptographic strength of the secure channel between the R0KH and R1KH ~~is assumed to~~shall be greater than or equal to the cryptographic strength of the channels for which the keys are used. T~~his standard assumes that t~~he key transfer includes the PMK-R1, the PMK-R1 PMKSA, the PMK-R1 context, and the associated key authorizations.

3270.33: The PMK-R1 distribution from the R0KH to the R1KHs within the same mobility domain shall satisfy the following ~~assumptions~~:

3270.46: The S0KH and S1KH are entities that ~~are assumed to~~ ~~physically~~ reside in the Supplicant.

3271.23: ~~NOTE—It is assumed by this standard that t~~The Fast BSS Transition Policy bits in the MDE ~~are administered consistently~~shall be the same across the mobility domain.

3335.63: The authenticated mesh peering exchange (AMPE) establishes an authenticated mesh peering between ~~the~~ mesh STAs~~, under the assumption~~ that have established a mesh PMKSA ~~has already been established~~

3336.4: The AMPE is also used to establish an authenticated peering between two APs that support the AP PeerKey protocol (as defined in 12.10 (AP PeerKey support)) and that have established ~~under the assumption that~~ a PMK and PMKID ~~have already been established~~

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1398 and 1397 in <this document>, which convert assumption into either requirements or informational material.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1823  Mark RISON  ~~17.6.7.2~~ 12.7.6.2  3217.21 | "Key MIC = 0" is confusing when it's not referring to the bit but to the field, which is empty in that case | Change "Key MIC = 0" to "Key MIC = Not present" at 3217.21 |

Discussion:

Actually the field is present, but all-zeroes, except when an AEAD cipher is used. However, the definition of the Key MIC field fails to cover this case. The definition of the other Key MIC field (the one in the Key Information field) already encompasses the “no MIC if AEAD” aspect:

6) Key MIC (bit 8) is set to 1 if not using an AEAD cipher and a MIC is in this EAPOL-Key frame and is set to 0 otherwise.

Note that the so-called “EAPOL-Key frame” is actually not a frame (see CIDs 1399, 1836, 1837), it’s an EAPOL PDU, where the first part is defined by 802.1X and the second part by 802.11.

Proposed changes:

Change at 3217.21 “Key MIC = 0” to "Key MIC = Not present when using an AEAD cipher; otherwise 0"

Change at 3208.1 as follows:

**h) Key MIC.** When the ~~negotiated AKM is not 00-0F-AC:14, 00-0F-AC:15, 00-0F-AC:16, or 00-0F-AC:17~~ Key MIC subfield (of the Key Information field) is 1, the ~~EAPOL~~ Key MIC field is a MIC of the EAPOL-Key frame~~s~~ (see Figure 12-33), i.e., from and including the ~~EAPOL p~~Protocol ~~v~~Version field of the EAPOL PDU to and including the Key Data field, calculated with the Key MIC field set to 0. If the Encrypted Key Data subfield (of the Key Information field) is 1, the Key Data field is encrypted prior to computing the MIC. When using an AEAD cipher, the ~~EAPOL~~ Key MIC field is not present. When not using an AEAD cipher, when the Key MIC subfield (of the Key Information field) is 0, the Key MIC field is 0. The length of this field depends on the negotiated AKM as defined in 12.7.3 (EAPOL-Key frame construction and processing) (see Table 12-11 (Integrity and key wrap algorithms)).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1823 in <this document>, which clarify that the Key MIC field is not present when using an AEAD cipher, and is otherwise present but 0 if the Key MIC subfield of the Key Information field is 0.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1406  Mark RISON | "RSC(s)", "RSC values" -- I think these are actually replay counters, not RSCs | Change to "replay counters" (I can provide locations) |
| CID 1394  Mark RISON  9.4.2.185  1585.28 | It is not clear which KDEs can be included. Also missing a description of the RSC encoding | At the end of the penultimate para add "If the RSC is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the RSC field. The RSC for TKIP is the TKIP sequence counter (TSC); for CCMP and GCMP it is the packet number (PN);  see Table 12-8 (Key RSC field)." |
| CID 1814  Mark RISON  6 | "The Key Delivery element contains the current Key RSC" wrong case, and anyway what is a "current Key RSC"? | In Clause 6 change "KDE(s) and the current Key RSC" to "KDE(s) and the current RSC for the GTK" (3x). In 9.4.2.185 change "the current Key RSC" to "the current RSC for the GTK" |
| CID 2136  Mark RISON | All but the first "contains the current receive sequence counter (RSC)" should be just "contains the current RSC" | I can provide locations |
| CID 2149  Mark RISON | Sometimes the Key RSC field is called RSC | Pick one and change the others to that. I can provide locations |
| CID 2151  Mark RISON  490.23 | "Value to which the RSC(s) is initialized." should be "is/are", or reword as "Initialization value of the RSC(s)" | As it says in the comment |

Discussion:

The RSC is the value of the PN(/IPN/BIPN/WIPN/TSC) at the transmitter. At the receiver, this is put into a replay counter, which is then compared with subsequent PNs(/etc.).

Also, the term “Key RSC” is not defined (though there is a Key RSC field). A given RSC applies to a particular type of key (PTK, GTK, IGTK, BIGTK, WIGTK, etc.).

Also, it’s “receive sequence counter” not “receive sequence count” (but it should be abbreviated to RSC after the first use anyway).

Related CIDs: 1507 (below), 1518 (Submission Required), 1661 (Discuss), 1679 (Discuss), 1736 (Submission Required), 1908 (Discuss).

Proposed changes:

Make the changes indicated at the following locations:

418.60: ~~The~~ KDE(s) and the ~~Key~~current GTK RSC.

432.8, 445.16, 459.45 (also delete initial space): KDE(s) and the current ~~Key~~GTK RSC.

490.23: ~~Value to which~~ Initialization value of the ~~RSC~~replay counter(s) ~~is initialized~~.

1360.58: For WEP, the RSC ~~value~~field is reserved.

1585.30: The Key Delivery element contains the current ~~Key~~GTK RSC and one or more KDEs. ~~This is used to communicate the Key RSC and one or more KDEs in a FILS authentication exchange.~~

1585.46: […] for the GTK being installed. If the RSC is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the RSC field. The RSC for TKIP is the TKIP sequence counter (TSC); for CCMP and GCMP it is the packet number (PN); see Table 12-9 (Key RSC field).

1956.20: The PN field contains the current RSC ~~number~~ for the IGTK being installed

3214.32, 3215.62: ~~Key~~RSC

3214.53: ~~Key~~RSC is the ~~key~~ RSC

3226.18/24: ~~Key~~ RSC

3264.30: The AP constructs a Key Delivery element indicating the current GTK and ~~Key RSC~~GTK PN, and the current IGTK and IPN if management frame protection is enabled, and the current BIGTK and BIPN if beacon protection is enabled(11ba), and the current WIGTK and WIPN if WUR frame protection is enabled.

3266.46: The STA installs the GTK and ~~key~~GTK RSC, and IGTK and ~~IPN~~IGTK RSC if management frame protection is enabled, and BIGTK and ~~BIPN~~BIGTK RSC if present in the key delivery element and dot11BeaconProtectionEnabled is true(11ba), and WIGTK and ~~WIPN~~WIGTK RSC if present in the key delivery element and dot11RSNAWURFrameProtectionActivated is true.

1480.4: contains the bit string of {GTK || ~~Key~~ RSC || GTKExpirationTime} as the GTK data material. When present, the GTKdata field is protected by the exchange in which it is contained (see 14.5 (Authenticated mesh peering exchange (AMPE))). The ~~Key~~ RSC denotes the last TSC or PN sent using the GTK

1585.37: ~~Key~~ RSC

1585.46: The ~~Key~~ RSC field contains

3204.53: ~~Key~~ RSC

3207.38/45/48/51 (8x)/58: ~~Key~~ RSC

3214.53: this is the ~~Key~~ RSC field

3217.20, 3218.12, 3219.62, 3222.26, 3227.24, 3228.35: ~~Key~~ RSC

3338.31: 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 9.4.2.117 (Authenticated Mesh Peering Exchange element)).

490.23: Receive Sequence Counter

490.48: Receive Sequence Counter parameter

1360.51: The RSC field contains the current receive sequence counter (RSC) for the GTK being installed, to allow a STA to identify replayed MPDUs.

1362.29: The WIPN field ~~indicates~~contains the current ~~receive sequence counter~~RSC for the WIGTK being installed

1585.46: […] contains the current ~~receive sequence counter (~~RSC~~)~~ for the GTK being installed.

1955.58: The RSC field contains the current ~~receive sequence counter (~~RSC~~)~~ for the GTK being installed

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1406 in <this document>, which make the suggested changes.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1521  Mark RISON | I've already forgotten why PTKs are transient keys while GTKs are temporal keys, but in any case this distinction seems dubious because (a) often the spec just talks of "temporal key", which would miss out PTKs (e.g. 6.3.19.1.2 for MLME-SETKEYS.req only talks of temporal keys) and (b) the spec sometimes talks of group transient keys anyway (e.g. "14.5.4 Distribution of group transient keys in an MBSS") | Change "transient key" to "temporal key" throughout (I can provide locations) |

Discussion:

We have the following definitions for pairwise **transient** key, group **temporal** key (in fact we have two of these!), transient key and temporal key:

**group temporal key (GTK):** A random value, assigned by the group source, which is used to protect group addressed medium access control (MAC) protocol data units (MPDUs) from that source. The GTK might be derived from a group master key (GMK).

**group temporal key (GTK):** A temporal key that is used to protect information exchanged in group addressed Data frames.

**pairwise transient key (PTK):** A concatenation of session keys derived from the pairwise master key (PMK) or from the PMK R1 (PMK-R1).

**temporal key (TK):** Temporal key integrity protocol (TKIP) only: The combination of temporal encryption key and a message integrity code (MIC) key. Non-TKIP only: A temporal encryption key.

NOTE—A temporal key is a session key.

where

**temporal encryption key:** The portion of a pairwise transient key (PTK) or group temporal key (GTK) used directly or indirectly to encrypt data in medium access control (MAC) protocol data units (MPDUs).

We also have a reference to “group transient keys”, which is apparently wider than GTKs:

**14.5.4 Distribution of group transient keys in an MBSS**

A PTK is not a temporal (encryption) key because it’s not only used to encrypt stuff (see Figure 12-30—Pairwise key hierarchy). On the other hand, a GTK is only used to encrypt stuff (see Figure 12-31—Group key hierarchy), so it’s a temporal (encryption) key (the temporal key isn’t a “portion of” the GTK except in a mathematical sense).

The issue with Clause 6 is that it is not sufficiently clear that in the case of Key Type Pairwise or PeerKey it’s not the PTK or TPK that’s passed, it’s the TK or TPK-TK.

Proposed changes:

Move the definitions of BIGTK, GMK, IGTK from 3.1 to 3.2.

Delete the definition of GTK in 3.1.

Change/add the definitions in 3.2 as follows:

**group ~~temporal~~ key (GTK):** A temporal key that is used to protect information exchanged in group addressed ~~Data~~ frames.

**group temporal key (GTK):** The group key that is used to protect information exchanged in group addressed Data frames.

**pairwise transient key (PTK):** A concatenation of session keys derived from the pairwise master key (PMK) or from the PMK R1 (PMK-R1), including a temporal key that is used to protect information exchanged in individually addressed frames.

**temporal encryption key:** A group temporal key (GTK) or t~~T~~he portion of a pairwise transient key (PTK) ~~or group temporal key (GTK)~~ used directly or indirectly to encrypt data in medium access control (MAC) protocol data units (MPDUs).

**temporal key (TK):** Temporal key integrity protocol (TKIP) only: The combination of temporal encryption key and a message integrity code (MIC) key. Non-TKIP only: A temporal encryption key. When abbreviated this is, unless explicitly shown otherwise, specifically the key used to protect individually addressed frames, as distinct from e.g. the TK that is the group temporal key (GTK).

Change 490.14, 491.42, 494.36, 751.30, 752.17 as follows:

Defines whether this key is a ~~group key~~GTK,

~~pairwise key~~TK, ~~PeerKey~~TPK-TK, ~~integrity group key~~IGTK,

~~beacon protection key~~BIGTK, or ~~wake-up radio~~

~~integrity group temporal key~~WIGTK respectively.

Change **14.5.4 Distribution of group transient keys in an MBSS**

to **14.5.4 Distribution of group keys in an MBSS**

Change “Group Key” to “group key” at 3097.13/16.

Change “the Group Key” to “a group key” at 3213.54/57.

Change “In an IBSS each STA defines its own group key, i.e., GTK” to “In an IBSS each STA defines its own GTK” at 3173.42.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1521 in <this document>, which address the issue raised by the commenter by clarifying the terminology for keys.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1989  Mark RISON | "CMMG NDP Announcement frame" -- no such frame | Make the changes shown under "Proposed changes" under CID 177 in 21/0829 (latest revision) |
| CID 1669  Mark RISON  10.32.4  2330.56 | "a CMMG NDP Announcement frame" -- no such frame | Change to "a CMMG NDP announcement" |

Discussion:

The resolution of CID 177 was missed from D1.0 (or did we agree it after D1.0 was out?).

Proposed changes:

In 9.2.4.6.4 CMMG variant HT Control field change “The CMMG NDP Announcement subfield of the CMMG variant HT Control field indicates that an NDP will be transmitted (according to the rules described in 10.33 (CMMG beamforming).” to “The CMMG NDP Announcement subfield of the CMMG variant HT Control field indicates that a CMMG NDP will be transmitted (according to the rules described in 10.33 (CMMG beamforming))” [at 934.52].

In 10.32.4 Link adaptation using the CMMG variant HT Control field change “a CMMG NDP Announcement frame” to “a CMMG NDP announcement” [at 2330.56].

In 10.37.1 NDP rules:

* In the first para [at 2362.21] change “CMMG NDP” to “a CMMG NDP” (2x); in the fifth [at 2362.36] change “carrying CMMG NDP” to “carrying a CMMG NDP”
* In the fourth para [at 2362.33] change “A STA that is a TXOP holder or an RD responder shall not set both the CMMG NDP Announcement and RDG/More PPDU subfields to 1 simultaneously.” to “A STA that is a TXOP holder or an RD responder shall not set both the CMMG NDP Announcement and RDG/More PPDU subfields to 1 in the same frame.”
* In the fifth para [at 2362.36] add as the second sentence “A *CMMG NDP announcement* is a PPDU containing a +HTC frame with the CMMG NDP Announcement subfield set to 1.” (with “*CMMG NDP announcement*” italicised)
* Change “a PPDU that is a CMMG NDP announcement” to “a CMMG NDP announcement” (2x) [at 2362.55/58]
* Change “A STA that has transmitted a CMMG NDP announcement in a frame that requires an immediate response” to “A STA that has transmitted a CMMG NDP announcement indication in a frame that requires an immediate response” [at 2363.1]
* Change “A CTS frame cannot be used for CMMG NDP announcement” to “A CTS frame cannot be used for CMMG NDP announcement indication” [at 2362.48]

In 10.37.3 Determination of CMMG NDP destination change “If Calibration Position subfield is equal to 1 in the CMMG NDP announcement at the NDP receiver” to “If the Calibration Position subfield is equal to 1 in the frame containing the CMMG NDP announcement indication” [at 2363.34].

Proposed resolution for CID 1989:

REVISED

Make the changes shown under “Proposed changes” for CID 1989 in <this document>, which reapply the changes agreed for CID 177 on D0.0.

Proposed resolution for CID 1669:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1985  Mark RISON  10.23.2 | "If a STA is permitted to begin a TXOP (as defined in 10.23.2.4 (Obtaining an EDCA TXOP)) and the STA has  at least one MSDU pending for transmission for the AC of the permitted TXOP, the STA shall perform exactly  one of the following actions" -- doesn't allow for pending MMPDUs, or for pending Control and similar frames (e.g. PS-Poll, QoS Null). Also "permitted to begin a TXOP" is vague, compared to 10.23.2.4's "-- Initiate the transmission of a frame exchange sequence." | Make the list in 10.23.2.4 be:  On these specific slot boundaries, each EDCAF shall make a determination to perform one and only one of the following functions:  -- Decrement the backoff counter.  -- Initiate a TXOP.  -- Invoke the backoff procedure due to an internal collision.  -- Do nothing.  and then in 10.23.2.5 make the intro read "If one of a STA's EDCAFs is to initiate a TXOP (as defined in 10.23.2.4 (Obtaining an EDCA TXOP)), the STA shall perform exactly one of the following actions:  ", delete "e) Restart the channel access attempt by invoking the backoff procedure as specified in 10.23.2 (HCF  contention based channel access (EDCA)) as though the medium is busy on the primary channel as  indicated by either physical or virtual CS and the backoff counter has a value of 0.", reletter the following bullets and then after the list add:  "NOTE--A EDCAF that initiates a TXOP has a frame available for transmission (see 10.23.2.4). There might be another EDCAF of lower priority that invokes the backoff procedure due to an internal collision (see 10.23.2.4)." |
| CID 1986  Mark RISON  10.23.2 | "If a STA is permitted to begin a TXOP (as defined in 10.23.2.4 (Obtaining an EDCA TXOP)) and the STA has  at least one MSDU pending for transmission for the AC of the permitted TXOP, the STA shall perform exactly  one of the following actions" -- doesn't allow for pending MMPDUs, or for pending Control and similar frames (e.g. PS-Poll, QoS Null). Also "permitted to begin a TXOP" is vague, compared to 10.23.2.4's "-- Initiate the transmission of a frame exchange sequence." | Make the list in 10.23.2.4 be:  On these specific slot boundaries, each EDCAF shall make a determination to perform one and only one of the following functions:  -- Decrement the backoff counter.  -- Initiate a TXOP.  -- Invoke the backoff procedure due to an internal collision.  -- Do nothing.  and then in 10.23.2.5 etc. say:  If one of a STA's EDCAFs is to initiate a TXOP (as defined in 10.23.2.4 (Obtaining an EDCA TXOP)), the STA shall perform exactly one of the following actions:  -- [list of things; delete doing a backoff if present in the list...]  NOTE--A EDCAF that initiates a TXOP has a frame available for transmission (see 10.23.2.4). There might be another EDCAF of lower priority that invokes the backoff procedure due to an internal collision (see 10.23.2.4). |
| CID 1535  Mark RISON  10.23.2.4  2208.28 | "At each of the above-described specific slot boundaries, each EDCAF shall initiate a transmission sequence if"  is incompatible with 10.23.2.5/6/13/14's permission to "Restart the channel access attempt by invoking the backoff procedure". | Delete "Restart the channel access attempt by invoking the backoff procedure as specified in 10.23.2 (HCF  contention based channel access (EDCA)) as though the medium is busy on the primary channel as  indicated by either physical or virtual CS and the backoff counter has a value of 0." at 2210.51 |
| CID 1419  Mark RISON  10.23.2.2  2206.18 | "g) If explicitly indicated, such as in 26.17.2.3.3 (Non-AP STA scanning behavior)" should also cover the permission to do a backoff even if you're permitted/required to start a TXOP ("Restart the channel access attempt by invoking the backoff procedure as specified in 10.23.2") | As it says in the comment |
| CID 2187  Michail KOUNDOURAKIS  10.23.2.5  2210.51 | It seems unfair that the STA has to do a new backoff if it chooses to not  reduce its intended transmission bandwidth, for any reason (action e).  For example the STA wants to transmit a 160MHz MSDU/PPDU which fits  in the TxOp if transmitted at 160MHz, but if CCA at that point says that only  primary 20MHz channel is idle the same MSDU/PPDU may require fragmentation  which the STA may be able to do at that last minute and it chooses to not  transmit and instead wait for the full bandwidth to become available. | Add an action to allow STAs to behave as if CS on the primary channel said "busy",  if the full bandwidth is not available and the STA chooses to not use the  reduced bandwidth. |
| CID 1536  Mark RISON  10.23.2.4  2208.22 | The "do nothing" case should be explicitly spelt out | At 2208.44 add a "NOTE---An EDCAF does nothing at each of the above-described specific slot boundaries if there is not a frame available for transmission at that EDCAF and the backoff counter for that EDCAF has a value of 0." and then number the NOTEs |

Discussion:

10.23.2.4 is extremely clear that exactly one thing happens on slot boundaries (which are also extremely precisely defined):

On these specific slot boundaries, each EDCAF shall make a determination to perform one and only one of the following functions:

— Decrement the backoff counter.

— Initiate the transmission of a frame exchange sequence.

— Invoke the backoff procedure due to an internal collision.

— Do nothing.

and the first three are spelt out too. In particular, for the second we have (note the “shall”):

At each of the above-described specific slot boundaries, each EDCAF shall initiate a transmission sequence if

— There is a frame available for transmission at that EDCAF, and

— The backoff counter for that EDCAF has a value of 0, and

— Initiation of a transmission sequence is not allowed to commence at this time for an EDCAF of higher UP.

Other locations talk about what a STA shall do when it is “permitted to begin a TXOP (as defined in 10.23.2.4)”, e.g. in 10.23.2.5:

If a STA is permitted to begin a TXOP (as defined in 10.23.2.4 (Obtaining an EDCA TXOP)) and the STA has at least one MSDU pending for transmission for the AC of the permitted TXOP, the STA shall perform exactly one of the following actions:

a) Transmit a 160 MHz or 80+80 MHz mask PPDU if the secondary channel, the secondary 40 MHz channel, and the secondary 80 MHz channel were idle during an interval of PIFS immediately preceding the start of the TXOP.

b) Transmit an 80 MHz mask PPDU on the primary 80 MHz channel if both the secondary channel and the secondary 40 MHz channel were idle during an interval of PIFS immediately preceding the start of the TXOP.

c) Transmit a 40 MHz mask PPDU on the primary 40 MHz channel if the secondary channel was idle during an interval of (11ax)duration 1) DIFS if the PPDU is transmitted in the 2.4 GHz band or 2) PIFS otherwise, immediately preceding the start of the TXOP.

d) Transmit a 20 MHz mask PPDU on the primary 20 MHz channel.

e) Restart the channel access attempt by invoking the backoff procedure as specified in 10.23.2 (HCF contention based channel access (EDCA)) as though the medium is busy on the primary channel as indicated by either physical or virtual CS and the backoff counter has a value of 0.

[more PPDU transmission options for TVHT and HE]

“permitted to begin a TXOP” must be cognate with “Initiate the transmission of a frame exchange sequence.” (sic)/“initiate a transmission sequence”. But then “e) Restart the channel access attempt by invoking the backoff procedure” is not within the scope of what is permitted by 10.23.2.4 when the backoff counter is 0, there is something to tx and there is no higher-priority EDCAF also in the same situation -- in this situation a STA “shall” initiate a TXOP. (And additionally it is not clear: on which EDCAF(s) is the backoff procedure invoked?)

In addition, while the rules on when a STA is “permitted to begin a TXOP” do not depend on the state of the secondary channel(s), only the primary channel, there may be situations in which a STA might prefer to do nothing rather than transmit at reduced bandwidth. In those situations the EDCAF in question should not be required to backoff, since it has not put anything on the WM.

Proposed changes:

Change 10.23.2.4 as follows:

On these specific slot boundaries, each EDCAF shall make a determination to perform one and only one of the following functions:

— Decrement the backoff counter.

— Initiate ~~the transmission of a frame exchange sequence~~ a TXOP.

— Invoke the backoff procedure due to an internal collision.

— Do nothing.

At each of the above-described specific slot boundaries, each EDCAF shall decrement the backoff counter if the backoff counter for that EDCAF has a nonzero value.

At each of the above-described specific slot boundaries, each EDCAF shall either initiate a ~~transmission sequence~~ TXOP or do nothing if

— There is a frame available for transmission at that EDCAF, and

— The backoff counter for that EDCAF has a value of 0, and

— Initiation of a transmission sequence is not allowed to commence at this time for an EDCAF of higher UP.

NOTE—An EDCAF might do nothing if the available bandwidth (based on the state of the secondary channel(s)) is insufficient for its purposes.

At each of the above-described specific slot boundaries, each EDCAF shall report an internal collision (which is handled as specified in 10.23.2.4 (Obtaining an EDCA TXOP)) if

— There is a frame available for transmission at that EDCAF, and

— The backoff counter for that EDCAF has a value of 0, and

— Initiation of a transmission sequence is allowed to commence at this time for an EDCAF of higher UP.

At each of the above-described specific slot boundaries, each EDCAF shall do nothing if

— There is no frame available for transmission at that EDCAF, and

— The backoff counter for that EDCAF has a value of 0.

Change 10.23.2.5 as follows:

If one of a STA’s EDCAFs is permitted to ~~begin~~initiate a TXOP (as ~~defined~~specified in 10.23.2.4 (Obtaining an EDCA TXOP)) ~~and the STA has at least one MSDU pending for transmission for the AC of the permitted TXOP~~, the STA shall perform exactly one of the following actions:

a) Transmit a 160 MHz or 80+80 MHz mask PPDU if the secondary channel, the secondary 40 MHz channel, and the secondary 80 MHz channel were idle during an interval of PIFS immediately preceding the start of the TXOP.

b) Transmit an 80 MHz mask PPDU on the primary 80 MHz channel if both the secondary channel and the secondary 40 MHz channel were idle during an interval of PIFS immediately preceding the start of the TXOP.

c) Transmit a 40 MHz mask PPDU on the primary 40 MHz channel if the secondary channel was idle during an interval of (11ax)duration 1) DIFS if the PPDU is transmitted in the 2.4 GHz band or 2) PIFS otherwise, immediately preceding the start of the TXOP.

d) Transmit a 20 MHz mask PPDU on the primary 20 MHz channel.

e) ~~Restart the channel access attempt by invoking the backoff procedure as specified in 10.23.2 (HCF contention based channel access (EDCA)) as though the medium is busy on the primary channel as indicated by either physical or virtual CS and the backoff counter has a value of 0.~~ Transmit nothing.

and after the bullets add:

NOTE—An EDCAF that initiates a TXOP has a frame available for transmission (see 10.23.2.4). There might be another EDCAF of lower priority that invokes the backoff procedure due to an internal collision (see 10.23.2.4).

TBD: make similar changes in 10.23.2.6 (3x), 10.23.2.13, 10.23.2.14.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID xxx in <this document>, which xxx

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1996  Mark RISON | "A-MSDU frame" is not clear | Change each of the ~12 instances to "MPDU that contains an A-MSDU" (I can provide locations) |
| CID 1997  Mark RISON  3.2 | "A-MSDU frame" is not clear | Add the following definition in 3.2: "aggregate medium access control (MAC) service data unit (A-MSDU) frame: A frame that contains an A-MSDU." |

Discussion:

An A-MSDU is an aggregation of MSDUs. It is not a frame, and referring to an “A-MSDU frame” just adds to the confusion that already permeates MPDUs, MMPDUs, MSDUs, etc.

Proposed resolution:

REVISED

Change “A-MSDU frame” to “frame that contains an A-MSDU” at 1009.21/25, 2924.4, 5561.41/42, 5562.54/55.

Change “A-MSDU frame” to “MPDU that contains an A-MSDU” at 2913.54.

Change “(A-MSDU) frame format” to “(A-MSDU) format” at 216.46.

Change “A-MSDU frame format” to “A-MSDU format” at 2179.20.

At 5562.30 and 5563.4 change “the number of octets in the frame body of an A-MSDU frame when an A-MSDU frame is” to “the number of octets in the frame body of a frame that contains an A-MSDU when it is”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1385  Mark RISON  12.5.5.2  3157.1 | The left-hand "Rsvd" field is not described as a reserved field | At the end of the last para add "The second octet is reserved." |
| CID 1386  Mark RISON  12.5.3.2  3142.53 | The "Rsvd" fields are not described as reserved fields. Also the figure is not searchable, unlike the GCMP figure | At the end of the last para add "The remaining bits of the Key ID octet are reserved. The second octet is reserved." Make the figure searchable |

Discussion:

Calling the field “Rsvd” (which is the third octet, not the second octet) in the figure suggests it’s reserved, but this is not actually stated anywhere. This also applies to CCMP, where additionally the reservedness of the lsbs of the key ID octet (i.e. the “Rsvd” subfield) isn’t specified either.

Proposed resolution for CID 1385:

REVISED

At 3156.62 add a new para:

The third octet of the GCMP Header field is reserved.

Proposed resolution for CID 1386:

REVISED

At 3142.49 change:

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header by a total of 8 octets, compared to the 4 octets added to the MPDU header when WEP is used. The ExtIV bit (bit 5) is always set to 1 for CCMP.

Bits 6–7 of the Key ID octet are for the Key ID subfield.

to:

The third octet of the CCMP Header field is reserved.

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header by a total of 8 octets, compared to the 4 octets added to the MPDU header when WEP is used. The ExtIV subfield is always set to 1 for CCMP.

Bits 6–7 of the Key ID octet are for the Key ID subfield. The remaining bits of the Key ID octet are reserved.

[Mark RISON to send the figure to the Editors.]

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1512  Mark RISON  6.3.19.1.4  490.50 | "-- When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter to 0. When the Key, Address, Key Type, and  Key ID parameters identify an existing key, the MAC shall not change the current transmitter TSC/  PN/IPN/BIPN counter or the receiver replay counter values associated with that key." has several issues:  \* the initialization of the RCs (for a new key) is not specified  \* (but this is duplication of Clause 12 anyway)  \* the IPN/BIPN are not required to be reset if they are changed (see 12.5.4.4)  \* it is not clear, comparing with the first para, what the behaviour should be for the same key, address and key type, but a different key ID. Using this, and resetting the counters, feels dangerous. Note the first para does not mention the address or the key ID | Change to "-- When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter and the receiver replay counter values as defined in Clause 12. When the Key, Address, Key Type, and  Key ID parameters identify an existing key, the MAC shall not change the current transmitter TSC/  PN/IPN/BIPN counter or the receiver replay counter values associated with that key." |
| CID 1513  Mark RISON  6.3.19.1.4  490.50 | "-- When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter to 0. When the Key, Address, Key Type, and  Key ID parameters identify an existing key, the MAC shall not change the current transmitter TSC/  PN/IPN/BIPN counter or the receiver replay counter values associated with that key." has several issues:  \* the initialization of the RCs (for a new key) is not specified  \* (but this is duplication of Clause 12 anyway)  \* the IPN/BIPN are not required to be reset if they are changed (see 12.5.4.4)  \* it is not clear, comparing with the first para, what the behaviour should be for the same key, address and key type, but a different key ID. Using this, and resetting the counters, feels dangerous. Note the first para does not mention the address or the key ID | Change to "-- When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter and the receiver replay counter values as defined in Clause 12. When the Key, Address, Key Type, and  Key ID parameters identify an existing key, the MAC shall not change the current transmitter TSC/  PN/IPN/BIPN counter or the receiver replay counter values associated with that key." and clarify the behaviour for the same key, address and key type, but a different key ID |
| CID 1505  Mark RISON  6.3.19.1.4  490.52 | "TSC/PN/IPN/BIPN counter" -- missing the WIPN counter | Change to "TSC/PN/IPN/BIPN/WIPN counter" |
| CID 1506  Mark RISON  6.3.19.1.4  490.52 | "TSC/PN/IPN/BIPN counter" -- missing the WIPN counter | Change to "TSC/PN/IPN/BIPN/WIPN counter" here and add WIPN where missing elsewhere |
| CID 1507  Mark RISON  12 | The value to which a PN is initialised is not clear | At 490.50 change “When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter to 0.” to “When the Key, Address, Key Type, and Key ID parameters identify a new pairwise key or PeerKey to be set, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter to 0. When the Key, Address, Key Type, and Key ID parameters identify a new key to be set that is not a pairwise key or PeerKey, the MAC  initializes the transmitter TSC/PN/IPN/BIPN counter to the value in the Receive Sequence Count parameter.”  At 3149.8 and 3159.6 change “The PN shall be implemented as a 48-bit strictly increasing integer, initialized  to 1 when the corresponding temporal key is initialized or refreshed.” to “The PN shall be implemented as a 48-bit strictly increasing integer, initialized  to 0 when the corresponding temporal key or transient key is initialized or refreshed.”  At 3151.30 and 3161.8 change “The receiver initializes  these replay counters to 0 when it resets the temporal key for a peer.” to “The receiver initializes  these replay counters to 0 when it sets the temporal key or transient key.”  At 3153.41 change “The IPN shall be implemented as a 48-bit strictly increasing integer, initialized to 1 when the  corresponding IGTK is initialized. The transmitter may reinitialize the sequence counter when the IGTK is  refreshed. “ to “The IPN shall be implemented as a 48-bit strictly increasing integer, initialized to 0 when the  corresponding IGTK is initialized. The transmitter may reinitialize the IPN to 0 when the IGTK is  refreshed. “  At 3153.51 change “The BIPN shall be implemented as a 48-bit strictly increasing integer, initialized  to 1 when the corresponding BIGTK is initialized. The transmitter may reinitialize the sequence counter when  the BIGTK is refreshed.” to “The BIPN shall be implemented as a 48-bit strictly increasing integer, initialized  to 1 when the corresponding BIGTK is initialized. The transmitter may reinitialize the BIPN to 0 when  the BIGTK is refreshed.”  At 3143.28 after “NOTE 1” insert “NOTE 2---The PN is incremented before the MPDU is constructed and therefore no MPDU is transmitted with a zero PN.” and renumber the other NOTEs in the subclause; ditto at 3157.36 after “NOTE” |
| CID 2166  Mark RISON  6.3.19.1.4  490.52 | "transmitter TSC/PN/IPN/BIPN counter" but there is no receive TSC/PN/IPN/BIPN counter, so delete "transmitter" (2x) | As it says in the comment |

Discussion:

As it says in the comments.

Note these changes require the IPN/BIPN to be restarted (from 1) when the IGTK/BIGTK is changed (in D1.0 this is optional).

Unfortunately it is not clear in BIP whether the IPN is incremented prior to or after transmission of the protected frame, so for now leave it vague and the initialisation value as 1.

Re CID 2166, it’s true that there is no receiver PN etc. but saying “transmitter” and “receiver” is helpful to distinguish the behaviour on each side.

Proposed resolution:

Change 490.50 as follows:

When the Key Type parameter is Pairwise or PeerKey, and the Key, ~~Address, Key Type, and~~ Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize~~s~~ the transmitter TSC/PN~~/IPN/BIPN~~ counter and the receiver replay counter(s) to 0 ***[or “to the values specified in Clause 12”?]***. When the Key Type parameter is not Pairwise or PeerKey, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter TSC/PN/IPN/BIPN/WIPN counter to 0 or 1 (see Clause 12 and Clause 29) or the receiver replay counter(s) to the value in the Receive Sequence Count parameter. When the Key Type, Key, ~~Address, Key Type, and~~ Key ID, and Address (where valid) parameters identify an existing key, the MAC shall not change the ~~current~~ transmitter TSC/PN/IPN/BIPN/WIPN counter or the receiver replay counter(s) ~~values~~ associated with that key.

Change 3149.8 and 3159.6 as follows:

The PN shall be implemented as a 48-bit strictly increasing integer, initialized to ~~1~~0 when the corresponding temporal key is initialized or refreshed.

At 3153.41 delete:

The transmitter may reinitialize the sequence counter when the IGTK is refreshed.

At 3153.51 delete:

The transmitter may reinitialize the sequence counter when the BIGTK is refreshed.

Change 3143.26 and 3157.33 as follows:

Increment the PN, to obtain a fresh nonzero PN for each MPDU

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1570  Mark RISON | aSlotTime takes account of the air propagation time, but not aSIFStime -- why not? If the coverage class makes the air propagation time significant, then a SIFS response might only arrive back at the transmitter (and any neighbours) after PIFS or more, potentially causing timeouts and/or collisions | At 3430.50 change "10 µs" to "If dot11OperatingClassesRequired is false, 10 µs If dot11OperatingClassesRequired is true, 10 µs plus any coverage-class- dependent aAirPropagationTime (see Table 9-131 (Coverage Class field parameters))" |
| CID 1714  Mark RISON | aSlotTime takes account of the air propagation time, but not aSIFStime -- why not? If the coverage class makes the air propagation time significant, then a SIFS response might only arrive back at the transmitter (and any neighbours) after PIFS or more, potentially causing timeouts and/or collisions. Having said that, you then have to allow for the SIFS to vary by that amount | Add a statement that the SIFS as measured by the receiver can vary from its nominal value to its nominal value plus the greatest allowed air propagation time |

Discussion:

When a STA responds after SIFS, devices away from that STA will see the IFS lengthened by the air propagation time (in both directions). However, this is not a problem because the slot time incorporates the air propagation time, so the energy will arrive within the first slot after SIFS (this assumes STAs sample the medium for CCA until close to the end of the slot -- perhaps something for D2.0!).

Similarly, it is not a problem for timeouts as long as the timeouts either explicitly include the air propagation time, or do so implicitly via a slot time (one for every SIFS in the timeout). For example:

AckTimeout interval, with a value of aSIFSTime + aSlotTime + aRxPHYStartDelay

CTSTimeout interval with a value of aSIFSTime + aSlotTime + aRxPHYStartDelay

NAVTimeout period is equal to (2 × aSIFSTime) + (CTS\_Time) + aRxPHYStartDelay + (2 × aSlotTime)

[EDCA backoff procedure] timeout interval of duration aSIFSTime + aSlotTime + aRxPHYStartDelay

[some DMG thing] not observing the subsequent sectorized beam transmission for aSIFSTime + aSlotTime + aRxPHYStartDelay

[some EDMG thing] space-time slot has a duration of aAirPropagationTime + TXTIME(SSW) + aSIFSTime

There are some SIFSes without an air propagation time in 10.3.2.5.2 RID update but Dave GOODALL has confirmed that they do not need one, since they are in the context of setting the RID (which is analogous to a NAV), not a “RIDTimeout”:

“The Response Indication field in the PHY layer signal field of an RTS will be NDP Response, assuming use of an NDP CTS. The RID counter value based on NDP Response will be the time to send either a 1 or 2 MHz NDP CTS + aSIFSTime, i.e. it only protects the NDP CTS and not the following data frame and Ack. Therefore the RID does not need a timeout like the NAVTimeout for the RTS/CTS case.”

TBD: There could be problems with the LongTxTime setting of the RID as used in Bidirectional TXOPs but I will need to research that separately.

TBD: Ditto BD1 defined in P2892L29 and P2892L48, and DTSF in P2898L11.

Proposed changes:

Change 10.3.2.3.3 SIFS as follows:

The SIFS is the time from the end of the previous PPDU[+SigExt] to the beginning of the preamble of the subsequent PPDU as seen on the WM at the STA transmitting the subsequent PPDU.

NOTE—The time between these PPDUs as seen on the WM at any other STA in the BSS, including the STA transmitting the previous PPDU, might be anything from SIFS to SIFS + aAirPropagationTime. Because aSlotTime includes aAirPropagationTime, even in the worst case the subsequent PPDU will start to arrive before PIFS at any STA in the BSS.

A non-DMG STA shall not allow the space between PPDU[+SigExt]s that are defined to be separated by a SIFS, as measured on the medium at the STA, to vary from the nominal SIFS by more than ± 10% × (aSlotTime – aAirPropagationTime) for the PHY in use. (#233)A DMG STA shall not allow the space between PPDUs that are defined to be separated by a SIFS, as measured on the medium at the STA, to vary from the nominal SIFS by more than –0% or +10% × (aSlotTime – aAirPropagationTime).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1570 and CID 1714 in <this document>, which clarify that the IFS is SIFS locally but up to SIFS+APT at any other STA.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 1663  Mark RISON  11.8.8.4.4  2803.63 | "When dot11OperatingClassesImplemented is true, a mesh STA may switch from the operating channel to a  channel in a different operating class." -- not possible because the CSA element/frame does not contain an OC, so you don't know how to interpret the channel number | Delete the cited text |

Discussion:

SAKODA Kazuyuki has commented as follows:

mesh STA needs to use the Extended Channel Switch Announcement when it is switching to a different operating class. We can find the description in 11.9.3.4 Selecting and advertising a new channel in an MBSS. In REVme D1.0, page 2809, line 34.

11.9.3.4 Selecting and advertising a new channel in an MBSS

is in 11.9.3 Selecting and advertising a new channel and/or operating class

which is in 11.9 Extended channel switching (ECS).

11.8.8.4.4 Channel switch across an operating class

is in 11.8.8.4 MBSS channel switching

which is in 11.8.8 Selecting and advertising a new channel

which is in 11.8 DFS procedures.

Proposed changes:

Change 11.8.8.4.4 as follows:

When dot11OperatingClassesImplemented is true, a mesh STA may switch from the operating channel to a channel in a different operating class using an Extended Channel Switch Announcement element or frame.

NOTE—A mesh STA can switch from the operating channel to a channel in the same operating class using a Channel Switch Announcement or Extended Channel Switch Announcement element or frame (see 11.9.3.4).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 1663 in <this document>, which clarify that switching to a channel in a different operating class requires use of ECSA.

Comments needing a direction:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Discussion** |
| 1312 | 3477.00 | 46 | 17.3.2.2 | Figure 17-4 is not an illustration of the transmitted PPDU, it is only showing the traninging fields. | We already said at the start of 17.3.2.1 that Figure 17-1 shows the format of the PPDU. Perhaps just delete the cited sentence? Or, if something is needed to reference Figure 17-4, then the wording needs to be aligned to the content of the figure. | Which direction is preferred? |
| 1372 | 3418.00 | 11 | 15.2.3.6 | Is there supposed to be an RCPI in the clause 15 RXVECTOR? If so, add it to the table, and fix the subclause header of 15.2.3.6. If not, delete 15.2.3.6. | Either: 1) Change the subclause header to "RXVECTOR RCPI" and add a row to Table 15-2 for the RCPI parameter; or 2) Delete subclause 15.2.3.6. | Which direction is preferred? |
| 1378 | 3417.00 | 63 | 15.2.3.3 | "RSSI is intended to be used in a relative manner" -- it's useless to know just that signal A is stronger than signal B, without knowing how strong signal A and signal B are, or even just the difference in power between signal A and signal B | Clarify how a unitless RSSI is to be used | Any ideas? Or just delete the RXVECTOR RSSI parameters? |
| 1550 |  |  |  | Where something is applicable to PCPs as well as APs, this should be stated | Review uses of AP and add "or PCP" where appropriate | Is there any solution other than to make a vague statement to the effect that unless stated otherwise statements made re APs generally apply to PCPs too? |
| 1714 |  |  |  | aSlotTime takes account of the air propagation time, but not aSIFStime -- why not? If the coverage class makes the air propagation time significant, then a SIFS response might only arrive back at the transmitter (and any neighbours) after PIFS or more, potentially causing timeouts and/or collisions. Having said that, you then have to allow for the SIFS to vary by that amount | Add a statement that the SIFS as measured by the receiver can vary from its nominal value to its nominal value plus the greatest allowed air propagation time | See CID 1570 |
| 1802 |  |  |  | "When the Multiple BSSID element is transmitted in a Beacon, DMG Beacon, or Probe Response frame, the reference BSSID is the BSSID field of the frame." -- what about in an S1G Beacon? Ditto "When a station receives a Beacon frame or DMG Beacon frame with a Multiple BSSID element that consists of a nontransmitted BSSID profile with only the mandatory elements" and probably other locations | Review the references to DMG beacons, and add references to S1G beacons where appropriate | Does the group agree that in general statements made about Beacon frames also apply to S1G/DMG Beacon frames? If so, what can be done apart from a generic statement that this is so? |
| 1803 |  |  |  | "A single Beacon frame may contain elements for the multiple BSSID set members; see 11.1.3.8 (Multiple BSSID procedure)." -- DMG Beacon and S1G Beacon frames may too. Ditto "multiple basic service set identifier (BSSID) capability: The capability to advertise information for multiple BSSIDs using a single Beacon or Probe Response frame" and "indicated in the Beacon and Probe Response frames by the Multiple BSSID subelement" and "If the multiple BSSID capability is supported, Beacon frames shall be transmitted using any basic rate valid for all of the BSSs supported." and probably other locations | Review the references to vanilla beacons, and add references to DMG and/or S1G beacons where appropriate | Does the group agree that in general statements made about Beacon frames also apply to S1G/DMG Beacon frames? If so, what can be done apart from a generic statement that this is so? |
| 2017 |  |  |  | In Clauses 16, 18, 23 there is a reference to a TXSTATUS and/or to TIME\_OF\_DEPARTURE but there is no TXSTATUS parameters subclause (unlike Clauses 15, 17, 19, 20, 21, 24) | Add a TXSTATUS parameters subclause to each PHY clause where it is missing (though arguably Table 16-5--Parameter vectors and Table 18-2--TXSTATUS parameters does it for those two clauses) | Which PHYs should have ToD information? |
| 2018 |  |  | 23 | In D3.0 23.3.19 PHY transmit procedure there was a reference to TXSTART(TXSTATUS) but no TXSTATUS is defined. Is timing info available for Clause 23 PHYs or not? | If S1G STAs want to be able to timing, then add the timing infrastructure to the S1G PHY specification | Does S1G need timing information? |
| 2119 |  |  |  | What an "operating class" does and does not specify seems to depend on the subclause the term is used in | Agree on what exactly an operating class does and does not specify, and capture this in the spec | We need to reach consensus on what an operating class does and doesn't define. I think that in practice all it defines is the starting factor, since we add/remove channels and behaviour limits over time. I don't think it even shows channel spacing or "phase", since e.g. global 128 is 42, 58, 106, 122, 138, 155, 171 |
| 2135 |  |  |  | Are there no uses of "direct link" in non-infrastructure BSSes (e.g. PBSS, IBSS, S1G/DMG relay)? Does Figure 4-12--DMG relay in a DMG BSS show a direct link not necessariily in an infrastructure BSS? Also "then the address is a BSSID for the Direct Link in an infrastructure BSS or for the IBSS." wrong case and allows for IBSS direct link | Address the issues identified | Any ideas? Do we agree that "direct link" only applies to an infrastructure BSS? |
| 1910 |  |  |  | "Info ID" needs to be "info ID" or have "field" or something appended. And is it InfoID or Info ID? | Either lowercase "Info ID" when not followed by "field", or add "field" when not present. Change "InfoID" to "Info ID" in Table 9-410--ANQP-element definitions | What is the preferred direction? |
| 2101 |  |  |  | "Std." is haphazardly present after "IEEE" and before "802" | I can provide locations if I'm told what the rule is for when it's needed | What is the rule for inclusion/non-inclusion of "Std."? |
| 2132 |  |  |  | "Tx" v "TX" inconsistency | Pick one and change the others to that. I can provide locations | Which is the preferred form? |
| 2156 |  |  |  | In 9.6.x, the first subsubsubclause is sometimes "General", sometimes "<blah> Action field" | Pick one and change the others to that. I can provide locations | What is the preferred form? |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1877 |  |  |  | The case of "transition event request" is inconsistent. It's not clear whether this is a Transition event request (per Table 9-230--Event Type field definitions for event requests and reports) or a Transition Event request (per Table 9-231--Transition Event Request subelement) | Decide whether the same convention is used as for Beacon requests, and then decide whether these are Transition {event requests} or {Transition Event} requests, and set the case accordingly | Needs group direction |
| 1897 | 2595.00 | 51 | 10.50.2 | "The total duration of the BDT Initiator PPDUs shall not exceed the TXOP limit as described in 10.23.2.3" -- that subclause does not discuss TXOP limits | Put in the correct xref | Needs S1G SME to provide the intended xref (unless this was a bug in merging 11ah into 11me) |
| 2021 |  |  | 9.6 | The way in which the subfields of Action fields are described is inconsistent as regards those that contain elements. It should either be "Blah element" in the table and then "The Blah element is defined in 9.xxx" in the text below, or it should be "Blah" in the table, and then "The Blah field contains a Blah element (see 9.xxx)" | I can try to do this if I have a direction from the group as to which option is preferred | What is the group direction? |
| 2028 |  |  | 9.4.2.30 | There is a lack of clarity on TCs and TCLASes: what a TC is for, whether User Priority in TCLAS element is input or output, whether it classifies MSDUs or MPDUs or MMPDUs or what (or "it depends"), whether UP > 7 is only for TFS, why the field called User Priority not UP | Rename the field to "UP" | Needs group direction (to include e.g. Thomas and Osama) |
| 2042 |  |  | 9.6 | In 9.6.3.2.2 DMG ADDTS Request frame variant and certainly others: the way the optional parts are described is inconsistent ("The optional X element", "The X element is optional and", "When present, the X element" etc.) | I can try to do this if I have a direction from the group as to which option is preferred | What is the group direction? |
| 2107 |  |  | 10.6 | The CMMG rules being separated (in 10.6.8) causes the exclusion rules structure of 10.6.5.x to be confusing or broken. DMG started it with 10.6.7. | Merge 10.6.7 and 10.6.8 into 10.6.5. I think perhaps the other Mark has some ideas about this | See if the other Mark has some ideas about this |
| 2175 | 2278.00 | 28 | 10.25.6.7.1 | "the S1G originator of an A-MPDU that is not an S- MPDU eliciting an NDP BlockAck frame" has about 13 different possible precedence interpretations | Clarify | Needs S1G SME direction |

Comments needing confirmation of the direction:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Discussion** |
| 1070 | 4309.00 | 6 | 27.2.3 | RXVECTOR and TRIGVECTOR are incomplete since they lacks a parameter for ppm offset or CFO (or similar). Timing information from the existing PHY-RXSTART, PHY-TXSTART and PLME-CHARACTERISTICS.confirm primitives probably suffice. | Add new RELATIVE\_TX\_RX\_FREQ\_OFFSET parameter to RXVECTOR and TRIGVECTOR | Any objections? |
| 1393 |  |  |  | A DMG SME has suggested that DMG relay should be deprecated. (And if it isn't the addressing rules need to be clarified) | Deprecate DMG relay operation | Any objections? |
| 1398 |  |  |  | "This standard assumes" -- it shouldn't assume, it should mandate | Change the ~9 instances of "standard assumes" to "standard relies on the fact that" (I can provide locations) | Any objections? E.g. "When the policy selection process chooses IEEE 802.1X authentication, this standard assumes that IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled port." |
| 1406 |  |  |  | "RSC(s)", "RSC values" -- I think these are actually replay counters, not RSCs | Change to "replay counters" (I can provide locations) | E.g. "Value to which the RSC(s) is initialized." at 490.23 (and other locations in C6); "the RSC value is reserved" at 1360.58. Also a number of locations where "Key RSC" should be just "RSC", e.g. "The KDE(s) and the Key RSC." at 418.60, "The Key Delivery element contains the current Key RSC and one or more KDEs" at 1585.30, "is the key RSC" at 3214.53, "The Key RSC denotes the last TSC or PN" at 1480.0, "The AP constructs a Key Delivery element indicating the current GTK and Key RSC" at 3264.30, "The STA installs the GTK and key RSC" at 3266.46, "concatenated with the Key RSC" at 3338.32. Spurious "number" in "RSC number" at 1956.20 |
| 1410 |  |  |  | Assaf KASHER reported that "A device can avoid beam tracking by setting the Beam tracking time limit to 0." (DMG). Is this desirable? | Specify that devices shall not set the beam tracking time limit to 0 | Any objections? |
| 1417 |  |  |  | "number of TBTTs" doesn't make sense since a TBTT is a time, not an object | Refer to a number of beacon intervals instead | Maybe reject based on "a series of TBTTs" in 11.1.3.2? |
| 1447 |  |  |  | There is no benefit, only possible doubt/confusion, in defining a standalone field that is only used in one element. Such fields should just be defined directly in the context of the element | Remove any "field" subclause that is only used in one element/frame, and move it to that element/frame's subclause | E.g. DELBA Parameter Set, Originator Preferred MCS, SM Power Control, Sync Control |
| 1521 |  |  |  | I've already forgotten why PTKs are transient keys while GTKs are temporal keys, but in any case this distinction seems dubious because (a) often the spec just talks of "temporal key", which would miss out PTKs (e.g. 6.3.19.1.2 for MLME-SETKEYS.req only talks of temporal keys) and (b) the spec sometimes talks of group transient keys anyway (e.g. "14.5.4 Distribution of group transient keys in an MBSS") | Change "transient key" to "temporal key" throughout (I can provide locations) | Any objections? ~20 instances |
| 1570 |  |  |  | aSlotTime takes account of the air propagation time, but not aSIFStime -- why not? If the coverage class makes the air propagation time significant, then a SIFS response might only arrive back at the transmitter (and any neighbours) after PIFS or more, potentially causing timeouts and/or collisions | At 3430.50 change "10 ┬╡s" to "If dot11OperatingClassesRequired is false, 10 ┬╡s If dot11OperatingClassesRequired is true, 10 ┬╡s plus any coverage-class- dependent aAirPropagationTime (see Table 9-131 (Coverage Class field parameters))" | Any objections? Or should coverage classes be deprecated? |
| 1673 |  |  |  | "entire frame exchange" -- it is not clear how this is distinguished from another (partial?) frame exchange | Delete "entire " throughout (5x -- I can provide locations) | Any objections? E.g. "the power management mode that the STA shall adopt upon successful completion of the entire frame exchange" |
| 1720 |  |  |  | A discussion with Solomon TRAININ indicates that in a PBSS the rules (for addressing, security, etc.) shall be infrastructure-like for transmissions a) to the PCP if associated (but you're not required to associate to the PCP), or b) to other STAs in the PBSS via the PCP if everyone involved is associated and if the PCP provides the forwarding service (which is not mandatory); and the rules shall be IBSS-like in all other cases. However, this is not clearly specified | State that in a PBSS the rules (for addressing, security, etc.) shall be infrastructure-like for transmissions a) to the PCP if associated (but you're not required to associate to the PCP), or b) to other STAs in the PBSS via the PCP if everyone involved is associated and if the PCP provides the forwarding service; and the rules shall be IBSS-like in all other cases | Any objections? Some reflector discussion |
| 1760 |  |  |  | A "may" in a "for example" is not really normative, and would be better as "might" | Change "may" to "might" in all of the following instances: If, for example, a STA has made and had accepted an explicit admission for a TS and the channel conditions subsequently worsen, possibly including a change in PHY data rate so that it requires more time to send the same data, the STA may make a request for more admitted\_time to the AP The non-AP and non-PCP STA can make this request if, for example, the device containing the non-AP and non-PCP STA intends to initialize another co-channel BSS or example, the precedence level may be used to convey to the AP that the requested TS is for the purposes of placing an emergency call. For example, it may choose to move to a different BSS. For example, it may choose to move to a different MBSS. For example, it may choose to move to a different BSS. For example, it may choose to move to a different BSS. These channel moving or BSS width switching operations might occur if, for example, another BSS starts to operate in either or both of the primary or secondary channels For example, URIs using the scheme names "data:" and "http:" may direct applications (e.g., a browser) on the STA to Internet pages that contain active scripts. For example, the Local Content ANQP-element may return two Local Content Duple fields An attempt to form a security association may also fail because, for example, the peer uses a different PSK or password from what the STA expects. the AP's Authenticator may have purged its PMKSA due to, for example, unavailability of resources, delay in the STA associating, etc. For example, the AS may communicate the MSK lifetime with the MSK. For example, when the resource being requested is QoS for downstream traffic, a TSPEC element may be followed by one or more TCLAS elements For example, when the resource being requested is QoS for upstream traffic, the TSPEC element may be followed by a Schedule element. The alternate destination may be an internet address on an Ethernet adapter, for example, to be used when the wireless link to the requesting entity is unavailable or unreliable." Also: the STA should send a new request for a TWT value by sending another frame that contains a TWT element, modifying the parameters of the request to indicate, for example, an acceptance of a proposed alternate TWT or dictated TWT value A mesh STA may use group addressed or individually addressed Mesh Data or QoS Null frames to change its mesh power management mode to a higher activity level, for example; | Any objections? First instance is at 2235.45 |
| 1893 |  |  |  | "IEEE MAC address" -- all MAC addresses are to be understood as being IEEE (802(.11)) MAC addresses in the context of this standard | Delete "IEEE" in the cited text and in "IEEE MAC individual or group address" and "IEEE MAC individual address" (I can provide locations) | Any objections? ~10 instances |
| 1902 |  |  |  | Consider 5 STAs A, B, C, D, E - and assume A is a PCP, and all want to be in the same PBSS. I think the following statements hold:\* B and C can associate to A, and then do security and data exchange using infra-like mechanisms (modulo the fact that A might not provide an intra-BSS forwarding service)\* D and E can choose not to associate with the PCP, and then do security and data exchange with any other STA in the PBSS (including A) using IBSS-like mechanisms (but not an actual IBSS)\* B and C can do security and data exchange with D and E using IBSS-like mechanisms too (and indeed have to, if A does not provide an intra-BSS forwarding service).[I'm not sure whether in the first bullet, if A does offer intra-BSS forwarding,this includes forwarding to unassociated STAs in the PBSS, or whether B and Cneed to do the last bullet to exchange data with D and E?] | Get a DMG SME to clarify | Any objections? See also 1720 |
| 1927 |  |  |  | The SCRAMBLER\_INITIAL\_VALUE is not the initial value of the scrambler, it's the value in the SERVICE field after scrambling | Change "SCRAMBLER\_INITIAL\_VALUE" to "SCRAMBLER\_SCRAMBLED\_SERVICE\_VALUE" throughout (I can provide locations) | Any objections? |
| 1995 |  |  |  | Vast swathes of CCMP and GCMP processing are the same. The duplication just causes spec rot (i.e. a fix in one gets forgotten in the other) | Extract the common parts, put them separately, and then have just the deltas specific to CCMP and GCMP separately | Any objections? |
| 1996 |  |  |  | "A-MSDU frame" is not clear | Change each of the ~12 instances to "MPDU that contains an A-MSDU" (I can provide locations) | Any objections? E.g. 2913.54 "A-MSDU subframes within an individually addressed A-MSDU frame", 5561.42 "an acknowledged A-MSDU frame" |
| 2004 |  |  |  | "individually addressed A-MSDU" -- (a) this is not defined; only addressing of MPDUs and MSDUs is defined and (b) assuming it means the MPDU the A-MSDU is in is unicast, it's the only permitted option anyway (except for GLK transmissions by an AP) per 10.11 fourth para | Change each instance to "individually addressed MPDU containing an A-MSDU" (I can provide locations) | Any objections? E.g. 913.30 "thesequence number of the corresponding individually addressed A-MSDUs" |
| 2048 |  |  |  | The claimed distinction between "collocated" and "co-located" is a fantasy, and it is guaranteed to lead to immediate spec rot. Alternatively, at least define the distinction in the spec. (See CID 4800 in REVmd) | Change "co-located" (case-insensitively) to "collocated" (case-preservingly). I can provide locations. Also change "Colocated" to "Collocated" in C.3 (5286.14/28) | Any objections? ~90 locations |
| 2060 |  |  |  | "The allowed values for the RCPI parameter are in the range 0 to 255, as defined in 9.4.2.37 (RCPI element)."; "The allowed values for the RCPI parameter are in the range 0 to 255, as defined in 17.3.10.7 (Received Channel Power Indicator Measurement)." and whatever 25.3.13 Received channel power indicator (RCPI) measurement ends up saying | The RCPI parameter in the PHY SAP should just be a power in dB with a resolution of 0.5 dB, without any particular encoding | Any objections? |
| 2073 |  |  |  | It is weird that the feature is "TIM broadcast" but the frames are just "TIM" frames | Rename TIM frames to TIM Broadcast frames (I can provide locations) | Any objections? ~80 instances |
| 2075 |  |  |  | The whole "field" v. "subfield" thing is just a big inconsistent mess (e.g. in the subclause for Reduced Neighbor Report element some things in the Neighbor AP Information field are fields and some are subfields, and the TBTT Information Set [sub!]field contains one or more TBTT Information fields). There is no value in trying to make the distinction, because (a) the distinction is not made reliably (b) it's not possible to make the distinction, because some things are subfields of X but are also the field that contains subfield Y (c) it doesn't tell you anything of particular significance | Change "subfield" to "field" throughout (I can provide locations) | Any objections? |
| 2079 |  |  |  | We have a ProbeDelay in the SCAN.req and a NAVSyncDelay in the START.req and JOIN.req. The former should only be used for scanning; the latter should be used not just when changing from doze to awake but also when changing to a new channel | In Clause 6 describe the NAVSyncDelay as also being used after switching channel. In 10.39.7.1 refer to the NAVSyncDelay not the ProbeDelay. In 11.2.3.2 say the NAVSyncDelay is also used after switching channel | Any objections? |
| 2129 |  |  |  | The rules on addressing (RA, TA, DA, SA) are not clear, especially in the context of A-MSDUs. There are also editorial issues | Make the changes shown in 21/0816 (latest revision) | The changes identified are probably not complete, but does the group agree with the direction? |
| 2141 |  |  |  | "Channel Center Frequency Segment 0" is confusing because it actually gives a channel number not a channel frequency (which requires the channel starting factor to be known) | Rename to "Channel Center Index Segment 0" | Any objections? Alternatively, have a NOTE somewhere to say it's an index not a frequency? |
| 2247 | 4334.00 | 12 | 27.3.4 | In the legend for the figure there is no distinction between Rus that require 40MHz pre-HE modulated transmission, and Rus that require 80MHz pre-HE modulated transmissions | Preferably use the dotted format used within the figure itself for the legend | Any objections? |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1430 |  |  | 20 | "header field[s]" in Clause 20 and children clauses should be "Header field" | I can provide locations | Any objections? |
| 1914 |  |  |  | "Vendor-Specific" should have a space, not a hyphen. Also case sometimes wrong ("Vendor-specific" or "vendor-specific" or "Vendor specific" or "vendor specific") | Use the term "Vendor Specific" throughout to refer to the Action frame | Any objections? |
| 1964 |  |  | 12.7.4 | AEAD ciphers should be tagged as an extra column in Table 12-11 and then just xreffed to that | Add an extra column to Table 12-11 that shows that only 00-0F-AC:14, 00-0F-AC:15, 00-0F-AC:16, or 00-0F-AC:17 are AEAD ciphers | Any objections? |
| 1994 |  |  |  | There is no difference between a "TDLS direct link" and a "TDLS link", and an IBSS or MBSS link is just as direct as a TDLS link (which appears ~20x) | Change "TDLS direct link" to "TDLS link" (I can provide locations) | Any objections? |
| 2010 |  |  |  | "individual MAC address" and "individually addressed MAC address" should be just "individual address" | I can provide locations | Any objections? |
| 2066 |  |  |  | We don't have a "broadcast destination address"; the term is "broadcast address" (and we don't have a broadcast source address either) | Change "broadcast destination address" to "broadcast address" throughout (I can provide locations) and in the instance at 2817.64 delete the " (DA)" too | Any objections? |
| 2095 |  |  |  | "BLAH format PPDU" should be just "BLAH PPDU" (also HT-greenfield format PPDU -> HT\_GF PPDU etc.) | I can provide locations | Any objections? |
| 2142 |  |  |  | Even within C.3 there is confusion as to whether MIB things are variables or attributes | Refer to them as MIB attributes throughout | Any objections? |
| 2144 |  |  |  | Since there are (except for regulatory matters) no legal requirements, say "conformant" not "compliant" | I can provide locations | Any objections? |
| 2148 |  |  |  | "entire" suggests that in places where not said it might be partial -- delete | I can provide locations | Any objections? |
| 2172 | 3206.00 | 38 |  | The row ordering in Table 12-7--Cipher suite key lengths seems haphazard | Sort alphabetically, or put the BIPs immediately after the corresponding non-BIP or something | Any objections? |
| 2179 |  |  |  | "Classifier Parameter" is sometimes spuriously capitalised. Also "the Classifier.". Also "Classifier Type" and words after it inconsistent too | I can provide locations | Any objections? |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1387 |  |  |  | "always" and "never" intensifiers imply that when they are not used an "is" or a "shall" is not definitive | Delete all "always"es and "never"s (I can provide locations) | Does the group agree with the direction? Examples: "The timestamp  indicated by SectorRevertTimestamp  is always later than the timestamp  indicated by  SectorSwitchTimestamp.", "the recipient shall always pass MSDUs or A-MSDUs up to the next MAC process" |
| 1390 |  |  | 3 | Clause 3 should refer to elements/fields/etc. by their name, not the expansion of (any part of) their names. E.g. HT Control, QoS Control field, Management MIC element, RDG/More PPDU subfield, EOF subfield, FILS Authentication frame, DMG Beacon frame, VHT Capabilities element, "transmitter address (TA)" | Refer to elements/fields/etc. in Subclauses 3.1 and 3.2 by their names, not the expansion of any terms within them | Does the group agree with the direction? Examples: "The MMPDU might include a Mesh Control field or management message integrity code element (Management MIC element)", "in which the reverse direction grant/ more physical layer protocol data unit (RDG/More PPDU) subfield is equal to 1." |
| 1414 |  |  |  | "STA[s] which" -> change to that. Maybe sometimes also when there is a comma, e.g. "geolocation database dependent (GDD) enabling STAs, which are required by regulation to provide their identification, geolocation"? | I can provide locations | Does the group agree with the direction? Examples: "estimates of throughput for MSDUs sent between the STA which corresponds to the PeerMACAddress indicated", "a frame from a peer STA which is not on the same primary channel" |
| 1421 |  |  |  | "counter value" should just be "counter" | I can provide locations | Does the group agree with the direction? Examples: "Initial backoff  counter value of 0.", "A replayed frame occurs when the PN from a received frame is less than or equal to the current replay counter value for the frame’s MSDU or A-MSDU priority and frame type." |
| 1459 |  |  |  | OCVC stands for "operating channel validation capable" so "OCVC capable" doesn't make sense | Change "OCVC capability" to "OCV capability" throughout (I can provide locations if necessary) | Does the group agree with the direction? |
| 1492 |  |  | 1.5 | L() is not very descriptive (cf. Truncate-n()) | Rename to Slice(). I can provide a list of locations | Does the group agree with the direction? |
| 1554 |  |  |  | There are references to channel "frequency index" but this is not defined | Change "frequency index" to "number" throughout. Change "ChannelCenterFrequencyIndex" to "ChannelCenterNumber" throughout, except in "dot11CurrentChannelCenterFrequencyIndex" | Does the group agree with the direction? |
| 1653 |  |  |  | Like "unicast" we should not use "groupcast" as a general term | Change to "group addressed" or "group addressing" when not in the context of GCR. I can provide locations | Does the group agree with the direction? |
| 1776 |  |  |  | Elements should have just one name (which may be just an abbreviation, e.g. RSNE), so remove parenthesis in: Multiple MAC Sublayers (MMS) element AP Configuration Sequence Number (AP-CSN) element Subchannel Selective Transmission (SST) element | As it says in the comment | Does the group agree with the direction? |
| 1777 |  |  |  | If the Management MIC element is to be referred to as MME, then put (MME) at the end of the Clause 9 subclause defining it and use MME everywhere else, as for RSNE | As it says in the comment | Does the group agree with the direction? |
| 1837 |  |  |  | Although the spec calls EAPOL-Key and EAPOL-Start "frames" it refers to "EAPOL PDU"s for the general term, and anyway they are not frames=MPDUs -- it would be better to be consistent | Change "EAPOL-Key frame" to "EAPOL-Key PDU" and "EAPOL-Start frame" to "EAPOL-Start PDU" throughout (I can provide locations) | Does the group agree with the direction? |
| 2002 |  |  | 9 | There is inconsistency as to whether the first address field in the PV0 MAC header is called Address 1 or RA (or maybe even A1). Ditto the next field (Address 2/TA) | Call the address fields for PV1 the same thing as they are for PV0 | Does the group agree with the direction? I think the comment should have been referring to PV1 not PV0 |

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID xxx  Mark RISON |  |  |

Discussion:

Proposed changes:

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID xxx in <this document>, which xxx

**References:**

802.11me/D1.0 except where otherwise specified