IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11me/D1.0 (LB258) | | | | |
| Date: 2022-03-21 | | | | |
| 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 an Anti-Clogging Token field 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." |

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)

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, 1942, 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.

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, 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).

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.

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 (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~~ an SA expired and could not be renewed (by rekeying; see 12.6.21).

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, a 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 a key associated with an existing SA is changed or a new key is associated with an existing SA.

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

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).

At 850.22 and 851.31 change "RSN SA" to "SA".

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

Proposed resolution:

REVISED

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

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? |

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? |

|  |  |  |
| --- | --- | --- |
| 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

TBD: 1989

**References:**

802.11me/D1.0 except where otherwise specified