**IEEE P802.11  
Wireless LANs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **802.11**  **Transmit Power Related CIDs** | | | | |
| **Date:** 2019-03-11 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Thomas Derham | Broadcom | 16340 W Bernardo Dr, San Diego CA |  | thomas.derham@broadcom.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document provides comment resolutions for REVmd letter ballot for some transmit power related CIDs – 2088, 2085, 2083, 2082, 2081, 2698.

R0: Initial draft

R1: Modified resolution to 2088 to also remove “maximum” from other sentences where it is describing a tolerance. Modified proposed resolution to 2698 taking into account some feedback received.

R2: Minor fixes

R3: Additional minor fixes

R4: Mods to proposed resolution to 2698 based on offline discussion

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2088 | 9.4.2.16 | 996 | 58 | "Maximum tolerance" is just "tolerance" | Change (I think 4) instances of "maximum tolerance" to "tolerance"; listing one example. |

**Discussion:** Tolerance (technical meaning) is defined as the allowed deviation from a standard. Therefore “maximum” is redundant. There are indeed 4 such examples of “maximum tolerance”, however two of them are deleted per the resolution to CIDs 2081/2082/2083 (see below) so only 2 remain. Thankfully, there are no examples of “minimum tolerance” in the standard, however there are instances of “tolerance” where the adjective “maximum” is elsewhere in the sentence with the same meaning, e.g. “the XXX tolerance shall be YYY maximum”, for which “maximum” should also be removed.

**Proposed Resolution:** Revise. Delete “maximum” in each of the following locations: 9.4.2.16 p996 line 58, 11.10.12 p2285 line 24, 15.4.5.6 p2853 line 37, 15.4.5.7 p2853 line 42, 16.3.7.5 p2883 line 31, 16.3.7.6 p2883 line 36, 17.3.9.5 p2921 line 38 and line 39, 17.3.9.6 p2921 line 45 and line 46, 18.4.7.4 p2944 line 12, 18.4.7.5 p2944 line 17, 19.3.18.4 p3025 lines 32 and 33, 19.3.18.6 p3026 line 18, 20.3.3.2.1 p3060 line 59, 20.3.3.3 p3061 line 9, 21.3.17.3 p3200 line 44, 22.3.17.3 p3277 line 58, 23.3.16.3 p3381 line 35, 24.3.3.2.1 p3424 line 36, 24.3.3.3 p3424 line 46, 25.3.2.3.1 p3453 line 60, 25.3.2.3.3 p3454 line 9. Replace “maximum allowable deviation” with “tolerance” in 22.3.17.3 p3277 line 53.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2085 | 9.6.6.5 | 1497 | 43 | Are there any other places in the spec where an element (TPC Report) is present in a frame before non-element fields?  This seems to be at odds with format of management frames in 9.3.3.2, with this sentence at P847L24: "The frame body consists of the fields followed by the elements defined for each management frame subtype." | If TPC Report element in the middle of non-element fields  is something unique, it would be worth highlighting (as an exception for example), both in this section and in 9.3.3.2 P847L24.  If element in the middle of non-element fields is not special, please revise teh sentence in P847L24. |

**Discussion:** The answer to the original commenter’s question is “Yes”. There is at least one other example of an element appearing in a frame before non-element fields. In 9.6.13.25 Channel Usage Response frame format, the Channel Usage element field contains zero or more Channel Usage elements, and this appears immediately prior to the Country String field which is fixed length. There are probably more examples, however your correspondent’s index finger is already sore from finding this one.

The sentence (actually in 9.3.3.1) that the commenter refers to is curious in that it uses the definite article “the” without clearly identifying which “fields” (or, indeed, “elements”) it is referring to. The sentence refers to the definition for each “management frame subtype” however it is unclear if the sentence is intended to apply to the hierarchy of frames/subframes/elements defined for certain types of frames within a certain subtype (e.g. fields/elements defined for each type of Action frame within the Action field). There are several variations in the way specific mgmt frame body definitions specify the inclusion of elements, e.g. in some cases the text states the “XXX element is present”, in other cases it states “the XXX field contains a YYY element”, etc. As such, the attempt in the sentence in 9.3.3.1 to specify a definitive order for fields and elements does not seem accurate and may be confusing.

**Proposed Resolution:** Revise. In 9.3.3.1, modify the sentence as follows: “The frame body consists of ~~the~~ fields ~~followed by the~~ and elements as defined for each management frame subtype.”

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2083 | 9.4.1.19 | 909 | 32 | Is the tolerance of the Max Transmit Power field value 5 dB or +/-5 dB? | Tolerance indicated in 11.10.13 is 5 dB. Tolerance in 9.6.6.4 is +/-5 dB. Similar power tolerance values are +/-5dB. Almost certainly this is just a syntax inconsistency (all other tolerance values are defined as +-dB value instead of just a dB value), but there is a remote possibility that intention has been to disallow reporting a maximum power that is less than the actual value (one-sided tolerance, e.g., to disallow a device transmitting at 30 dBm to report a value of 25 dBm).  Suggested resolution is to remove both tolerance statments, include a single statement in 9.4.1.9 (as suggested by a separate comment), and set the tolerance value to +/-5dB, unless someone clarifies the  one-sided tolerance has been deliberate. |
| 2082 | 9.4.1.19 | 909 | 32 | Max Transmit Power field value tolerance is specified in 9.6.6.4 and then again 11.10.13, both wrong places, and with different values in each section, instead of this section. All other related power level fields (e.g., "Transmit Power Used", 9.4.1.20) have their respective tolerance values specified in the same section where the field is defined. | Remove tolerance statements from 9.6.6.4 and 11.10.13, and modify the paragraph as following. Wording is the same as 9.4.1.20. Also note there is another comment on the +/-5 dB vs. 5 dB.  ---  "The Max Transmit Power field is a 2s complement signed integer and is 1 octet in length. It provides an upper limit, in units of dBm, on the transmit power as measured at the output of the antenna connector to be used by that AP on the current channel. The Max Transmit Power value has a tolerance of +/-5 dB. See 11.10.13 (Operation of the Max Transmit Power field). The Max Transmit Power field is shown in Figure 9-103 (Max Transmit Power field)." |
| 2081 | 9.4.1.19 | 909 | 37 | Max Transmit Power is transmitted by both APs and non-APs (e.g., as part of the Link Measurement Request frame). | Change "by that AP" to "by the transmitting STA" |

**Discussion:** Agree with commenter that it is very unlikely “5 dB” is supposed to indicate “+5 dB”, and much more likely that the “+/-“ convention was inadvertently omitted. Agree with the commenter that a single (correct) definition in 9.4.1.19 (where Max Transmit Power field is defined) is preferred, and we don’t need to duplicate in 11.10.13 or 9.6.6.4. Agree with commenter that Max Transmit Power field can be transmitted by both APs and non-AP STAs

**Proposed Resolution (for all 3 CIDs):** Revise (basically accept, but with some typo fixes and explicit instructions for clarity). Delete sentence in 11.10.13 “The maximum tolerance for the value reported in Max Transmit Power field shall be 5 dB.”. Delete sentence in 9.6.6.4 “The maximum tolerance for the value reported in Max Transmit Power field is ±5 dB. Modify 9.4.1.19 as follows:

"The Max Transmit Power field is a 2s complement signed integer and is 1 octet in length~~,~~. It provid~~ing~~es an upper limit, in units of dBm, on the transmit power as measured at the output of the antenna connector to be used by ~~that AP~~ the transmitting STA on the current channel. The Max Transmit Power value has a tolerance of +/-5 dB. See 11.10.13 (Operation of the Max Transmit Power field). The Max Transmit Power field is shown in Figure 9-103 (Max Transmit Power field)." Note to Editor: use typeset “+/-“ symbol.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2698 | 11.7.5 | 2242 | 36 | In several places in this clause, a STA that supports TPC is required to determine a regulatory and/or local power limit based on elements sent by its associated AP (Country, Power Constraint, Transmit Power Envelope, ..). In some/many cases, the most recently received element is obtained in a Beacon frame, the contents of which might not be authenticated despite a SA existing with the AP. This can effectively expose a DoS vector on an authenticated RSN link if beacons are spoofed with very low TPC power constraint. | Revise so that (at least if the STA has an SA with the AP), the STA it is not mandated to take into account elements for TPC that have been received from an unauthenticated frame. A "should" might be appropriate for this case. The STA would still be mandated to take into account these elements when received in an authentication frame (e.g. in a mgmt frame with MFP, with beacon protection capability, etc) |

**Discussion:** It is true that, in general, an adversary could inject fake (unprotected) Beacon or Probe Response frames purporting to be from an AP (or block and manipulate the genuine frames transmitted by that AP) and, per current rules, could force associated STAs to arbitrarily reduce their transmit power on the channel to unusable levels. For example, if Local Power Constraint field in Power Constraint element is set by the adversary to its largest value representing 255 dB, the STA would derive the local maximum transmit power level as {Reg Limit} – 255 which would essentially prevent the STA from transmitting at all.

The only potential way for the STA to mitigate such attack is to roam to a different AP on a different channel (if such AP exists) where hopefully the same attack is not being carried out.

It is noted that the only current way for the STA to receive Country, Power Constraint and Transmit Power Envelope elements directly from its associated AP is in Beacon and Probe Response frames (except for Channel Usage element, which is a special case applying to non-infra / TDLS operation by the associated STA).

However, the introduction of Beacon Protection into REVmd means that the integrity and data origin of these frames can now (when supported by both AP and STA) be verified by the associated STA.

Any changes made to address this comment should ensure STA remains compliant with its own knowledge of regulatory maximum transmit power limits.

The Country String field of the Country element is used by a non-AP STA to as hint to determine the regulatory domain in which it is operating, and therefore should not be ignored.

Proposed resolution is along the following lines:

* Change requirement on STA to “should” for using maximum transmit power values in Country, Power Constraint and Transmit Power Envelope elements if those elements are not integrity protected. Add a note with reference to integrity protection.
* (Note that, even if STA ignores certain of these elements when determining regulatory maximum transmit power, the text still requires the STA to select the minimum value from a list including the STA’s own knowledge of the regulatory limit, which is in practice how STAs ensure regulatory compliance)
* Add “regulatory maximum transmit power” into the list of items used to determine the local maximum transmit power (the minimum is selected), to ensure that even if the STA were to ignore certain unprotected elements or for some reason the elements have not been received at all, its determination of local maximum transmit power would never exceed its determination of the regulatory maximum transmit power.

**Proposed Resolution:** Revise by modifying text in 11.7.5 as follows:

A STA shall determine a regulatory maximum transmit power for the current channel by selecting the minimum of the following:

* Any regulatory maximum transmit power received in an integrity protected Country element from the AP in its BSS, PCP in its PBSS, another STA in its IBSS, or a neighbor peer mesh STA in its MBSS. If the STA has not received an integrity protected Country element but has received an unprotected Country element from the same AP, PCP, IBSS STA or mesh STA, it should use the regulatory maximum transmit power received in the unprotected element instead.
* Any regulatory maximum transmit power for the channel in the current regulatory domain known by the STA from other sources

A STA shall determine a local maximum transmit power for the current channel by selecting the minimum of the following:

* Unless the STA is extended spectrum management capable and has received a Transmit Power Envelope element for a channel width of 20 MHz and 40 MHz, any local maximum transmit power received in the combination of an integrity protected Country element and an integrity protected Power Constraint element from the AP in its BSS, PCP in its PBSS, another STA in its IBSS, or a neighbor peer mesh STA in its MBSS. If the STA has not received integrity protected Country and Power Constraint elements but has received unprotected Country and Power Constraint elements from the same AP, PCP, IBSS STA or mesh STA, it should use the local maximum transmit power received in the unprotected elements instead.
* If the STA is extended spectrum management capable, any local maximum transmit power received in an integrity protected Transmit Power Envelope element from the AP in its BSS, another STA in its IBSS, or a neighbor peer mesh STA in its MBSS. If the STA has not received an integrity protected Transmit Power Envelope element but has received an unprotected Transmit Power Envelope element from the same AP, PCP, IBSS STA or mesh STA, it should use the local maximum transmit power received in the unprotected element instead.
* The regulatory maximum transmit power for the current channel as determined by the STA (see above)
* Any local maximum transmit power for the channel in the current regulatory domain known by the STA from other sources

The Local Power Constraint field of any transmitted Power Constraint element and each Local Maximum Transmit Power For *X* MHz field (where *X* = 20, 40, 80, or 160/80+80) in the Transmit Power Envelope element shall each be set to its respective value that allows the mitigation requirements to be satisfied in the current channel.

NOTE—The local maximum transmit power for the channel needs to meet the mitigation requirements for the channel in the current regulatory domain. The conservative approach is to set the local maximum transmit power level equal to the regulatory maximum transmit power level minus the mitigation requirement. However, it might be possible to satisfy the mitigation requirement using a higher local maximum transmit power level. A lower local maximum transmit power level might be used for other purposes (e.g., range control, reduction of interference).

NOTE—Integrity protection is provided by certain mechanisms defined in Clause 12 (Security), e.g. see 11.53 (Beacon frame protection procedures).