IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB234 CID 3053, 3171, 3184, 3186, 3187, 3188, 3190, 3290, 3365, 3369, 3388, 3597, 3723 EDMG OFDM PHY, Spoofing and ShortSSW | | | | |
| Date: 2019-1-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Hiroyuki Motozuka | Panasonic | 600 Saedo-cho, Tsuzuki-ku, Yokohama, Kanagawa, Japan |  | motozuka.hiroyuki@jp.panasonic.com |
| Takenori Sakamoto |  |  | sakamoto.takenori@jp.panasonic.com |
| Yutaka Murakami |  |  | murakami.ytk@jp.panasonic.com |
| Lei Huang |  |  | lei.huang@sg.panasonic.com |
| Gaius Wee |  |  | yaohuang.wee@sg.panasonic.com |
| Kazu Takahashi |  |  | takahashi.kazu@jp.panasonic.com |

Abstract

This submission proposes resolution of comments on 30.6 EDMG OFDM mode and related subclauses received from LB# 234 (TGay Draft 2.0).

13 CIDs: 3053, 3171, 3184, 3186, 3187, 3188, 3190, 3290, 3365, 3369, 3388, 3597, 3723

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3171 | 29.6.2.6 | 481 | It is not clear what "frequency chanel dependent" means? | Replace "frequency channel dependent" with "frequency, channel and bandwidth dependent" | **Revised** |

**Discussion**

**According to Table 97 (Pilot tones definition), the different sequence of the pilot tone indexes are defined for each channel number. We propose to replace “frequency channel dependent” with “dependent on the channel number,” that we think straightforward.**

**Proposed changes to D2.2**

29.6.2.6 Pilot sequences

***Editor: Change the 1st paragraph in 29.6.2.6 as follows (P513L3-5 of D2.2):***

The pilot sequence P(*iSTS*, *n*, *k*) is created by inserting a sequence of zeros corresponding to tones –*NSR* to *NSR*. The pilots are then inserted at the tone indexes *Mp*(*k*) defined in 29.6.2.4, which are dependent on the channel number, but independent of the space-time stream or OFDM symbol number as follows:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3053 | 9.4.2.146 | 103.24 | Please delete Clause 9.4.2.146 per Editor Note | Delete Clause 9.4.2.146 | **Accepted** |
| 3365 | 9.4.2.146 | 103.24 | This clause (in fact, DTP) has been removed in 11md D1.0 given deletion of the 11ad OFDM PHY. Compared with STP, DTP has much higher implementation complexity. Furthermore, performance gain of DTP is doubtful. It is suggested to remove the DTP for EDMG OFDM mode. | delete whole clause | **Accepted** |
| 3369 | 29.2.2 | 343 | DTP has been removed in 11md D1.0 given deletion of the 11ad OFDM PHY. Compared with STP, DTP has much higher implementation complexity. Furthermore, performance gain of DTP is doubtful. | delete the row corresponding to parameter "EDMG\_TONE\_PAIRING" | **Accepted** |
| 3290 | 29.6.9.3.9 | 506.11 | "The array of group indexes, GroupPairIndex, can represent any permutation of indexes 0, 1, ..., NG - 1.  However, for NG = 92, 142, and 192, GroupPairIndex(NG - 1) shall be equal to NG - 1."  Implementing any permutation for N\_G cause a complexity problem. | separate contiribution will be provided | **Revised** |

**Discussion**

**Agree in principle on the comments. The DTP has been removed in REVmd as DMG OFDM has removed. Note that the MAC sublayer functional description and definition of frame format relate to DMG DTP have been removed as well, and current draft EDMG spec (REVmd D2.0+11ay D2.2) doesn’t have them for EDMG DTP.**

**Also, for EDMG OFDM PHY, the DTP algorithm defined in D2.2 requires implementation of any permutation of sequence with lengths 42, 92, 142 and 192 for NCB=1, 2, 3 and 4 respectively at transmitter. This requires much higher implementation complexity compared to STP, (or the symbol interleaver for 16-QAM and 64-QAM that employs regular block interleaver; see “29.6.9.3.10 interleaver”). Additional study should be needed to see if the performance gain justifies the complexity, or consider less complex algorithm.**

**We propose to remove DTP from EDMG OFDM PHY as well since the specification for it in D2.0 is incomplete, and no strong evidence encouraging further study and completion has been seen.**

**When the DTP is removed, the Static Tone Pairing (STP) doesn’t need to be a separate “mode”, so we propose to remove whole tone pairing related subclause and include the equation for tone pairing in each subclause for the definition of the modulation.**

**Proposed changes to D2.2**

***Editor: Remove whole Subclause 9.4.2.146 (P115L3-L15 of D2.2):***

***Editor: Remove “EDMG\_TONE\_PAIRING” from Table 43 (P347 of D2.1):***

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

29.3.3.3.2.3 Definition for EDMG SC mode and EDMG OFDM mode PPDUs

***Editor: Remove the 11th Bullet in the sixth paragraph in 29.3.3.3.2.3 (P401L36 of D2.2):***

In case of an EDMG A-PPDU, the following apply:

*(11th Bullet)*

***Editor: Remove the Tone Pairing Type field from Table 56(EDMG-Header-A field structure and definition for an SU PPDU) in 29.3.3.3.2.3 (P405 of D2.2):***

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Reserved | 10 | 102 | Set to 0 by the transmitter and ignored by the receiver. |
| CRC | 16 | 112 | Header Check sequence. Calculation of the header check sequence is defined  in 20.3.7. |

29.6.6 Encoding of EDMG-Header-B

*Editor: Change the last paragraph in 29.6.6 as follows (P521L29,L30 of D2.2):*

The data blocks shall be modulated using DCM QPSK modulation. The EDMG-Header-B shall use the OFDM modulation as defined for the Data field of the PPDU (see 29.6.9.3).

29.6.7 Encoding of EDMG-Header-A for EDMG A-PPDU transmission

*Editor: Change the last paragraph in 29.6.6 as follows (P523L3-L5 of D2.2):*

The data blocks shall be modulated using DCM QPSK modulation. The EDMG-Header-A field shall use an OFDM modulation as defined for the Data field of the PPDU in 29.6.9.3.

29.6.9.3 Modulation mapping

29.6.9.3.1 General

*Editor: Change the third paragraph in 29.6.9.3.1 as follows (P531L15-L17 of D2.2):*

The DCM BPSK, Dual Stream DCM BPSK, and DCM QPSK modulations use the tone pairing mechanism to extract channel frequency diversity as defined in 29.6.9.3.3, 29.6.9.3.4 and 29.6.9.3.5, erspectively. The 16-QAM and 64-QAM modulations use the interleaver defined in 29.6.9.3.10.

29.6.9.3.3 DCM BPSK modulation

*Editor: Change the last paragraph in 29.6.9.3.3 as follows (P532L19-L21 of D2.2):*

where the tone pairing index *P*(*k*) is defined as *P(k)* = *k* + *NSD*/2 in the range *NSD*/2 to *NSD* – 1. The *qth* modulated data block of the *iSSth* spatial stream is mapped to *NSD* data subcarriers of the *qth* OFDM symbol of the *iSSth* spatial stream.

29.6.9.3.4 Dual Stream DCM BPSK modulation

*Editor: Change the fourth paragraph in 29.6.9.3.4 as follows (P533L4,L5 of D2.2):*

where the tone pairing index *P*(*k*) is defined as *P(k)* = *k* + *NSD*/2 in the range *NSD*/2 to *NSD* – 1. The *qth* modulated data block of the *iSSth* spatial stream is mapped to *NSD* data subcarriers of the *qth* OFDM symbol of the *iSSth* spatial stream.

*Editor: Change the last paragraph in 29.6.9.3.4 as follows (P533L9,L10 of D2.2):*

where the tone pairing index *P*(*k*) is defined as *P(k)* = *k* + *NSD*/2 in the range *NSD*/2 to *NSD* – 1. The *qth* modulated data block of the *iSSth* spatial stream is mapped to *NSD* data subcarriers of the *qth* OFDM symbol of the *iSSth* spatial stream.

29.6.9.3.5 DCM QPSK modulation

*Editor: Change the fourth paragraph in 29.6.9.3.5 as follows (P534L4-L6 of D2.2):*

where the tone pairing index *P*(*k*) is defined as *P(k)* = *k* + *NSD*/2 in the range *NSD*/2 to *NSD* – 1. The *qth* modulated data block of the *iSSth* spatial stream is mapped to *NSD* data subcarriers of the *qth* OFDM symbol of the *iSSth* spatial stream.

***Editor: Remove whole Subclause 29.6.9.3.9 (P537L10-P538L19 of D2.2):***

29.6.9.3.10 Space-time block coding

***Editor: Remove the last paragraph of Subclause 29.6.9.3.11 (P540L37,L38 of D2.2):***

B.4.34.2 EDMG PHY features

***Editor: Remove Tone pairing related items: EDMG-P5.4.3, EDMG-P5.4.3.1 and EDMG-P5.4.3.2 from the table in B.4.34.2(EDMG PHY features) (P683-P684 of D2.2):***

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3187 | 29.3.3.2.4.2 | 372.9 | The formula in Line 9 is a wrong repetition of the formulat in line 7, | Remove this formula | **Accepted** |
| 3190 | 29.3.3.2.4.2 | 373.13 | shall is not appropriate in an informative clause. | Replace "shall" by "should" | **Accepted** |
| 3188 | 29.3.3.2.4.2 | 372.15 | "shall" is not appropriate in an informative clause. Also it will be nice to explain why this fairly obscure rule need to exist. Otherwise it sounds like a part of a recipe for an Amortentia potion. | At least replace "shall" with a "should" also provide an explanation to the rule. | **Revised** |
| 3597 | 29.3.3.2.4.2 | 372.25 | For spoofing algorithm, one possible case that base MCS<=5, N\_blks'<38 and (N\_blks' mod 3) not =1, is not considered for the corresponding values of N\_blks and N\_trn. It shall be included in the informative example for completeness. | Include the case of base MCS<=5, N\_blks'<38 and (N\_blks' mod 3) is not equal to 1, and give the corresponding values of N\_blks and N\_trn in the example | **Revised** |

**Discussion**

**(#3188) ...** *Also it will be nice to explain why this fairly obscure rule need to exist. Otherwise it sounds like a part of a recipe for an Amortentia potion. / ... also provide an explanation to the rule.*

**We propose changes as shown below to clarify the purposes of each step or condition described in step b) and c).**

**(#3597) Agreed on the comment. The condition the commenter mentioned (Base MCS<=5 && NBLKS’<38 && (NBLKS’ mod 3)!=1) should be covered in step c) since the text in step b) (see the following) doesn’t say the condition should not be used:**

* If and , the Base MCS field ~~shall~~should(#3188,#3190) be set to the value that is greater than 5

The equation ( and ) can be applied regardless of or not, so we propose the change to the algorithm as shown below.

**Proposed changes to D2.2**

29.3.3.2.4.2 Example of spoofing algorithm for EDMG SC PPDUs

***Editor: Change the text in subclause 29.3.3.2.4.2 as follows (P397L2 of D2.2):***

The following is an informative algorithm for calculating the value of the Length field (reffered to below as *Length*), the Training Length field (refferred to below as *Training\_Length*), and the MCS field (reffered to below as *Base MCS*) in the L-Header of an EDMG SC mode PPDU.

1. The tentative number of SC symbol blocks, , is calculated as   
   , where *TXTIME* is defined in 29.12.3 and , and are defined in 29.5.10.4.4.2.  
   (#3187)
2. The Base MCS field in the L-Header is set to the value such that the following conditions are met:

* , where , and are the parameters chosen based on the value of the Base MCS field as described in section 20.6.3. If this condition is fulfiled, the *Length* to be calculated in step d) and e) doesn’t exceed the maximum value of the Length field in the L-Header, 218-1(#3188).
* If and , the Base MCS field should(#3188,#3190) be set to the value that is greater than 5 to apply algorithm in step c) (#3188).

1. One of the combinations of(#3188) the parameters and which denote, respectively, the number of SC symbol blocks and the Training Length in a DMG SC mode PPDU with the spoofed TXTIME of the EDMG PPDU are calculated as follows:

**If** the Base MCS > 5 (π/2-QPSK, π/2-16-QAM and π/2-64-QAM) **then**

**Endif**

**If** the Base MCS ≤ 5 (π/2-BPSK)(#3597) **then**

**if** **then**

**else** **if** **then**(#3597)

**If** **then**

**else**

**endif**

**endif**

**endif**

1. The maximum value that fulfills the requirement for the spoofing error specified in 29.3.3.2.4.1, , is calculated as , where is the parameter defined in section 20.6.3.2.3, and the value is chosen based on the value of the Base MCS field as described in section 20.6.3.
2. The spoofed values of the Length and Training Length fields of the EDMG PPDU are calculated as follows:

=

where:

is the value of the Compressed BW field in the L-Header as described in 29.3.3.2.4.1.

When the Base MCS field is set to 1, the calculated length may not satisfy the requirement for the spoofing error defined in 29.3.3.2.4.1. In that case, the Base MCS field shall be set to a value different from 1, and the Length and the Training Length fields shall be calculated by repeating c) to e).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3723 | 29.6.9.2.4 | 497.11 | The specific content of pad OFDM symbols should be clarified, like packet extension field of 11ax | Add "The pad OFDM symbols, when present, shall be transmitted with the same average power as the data field, and shall not cause significant power leakage outside of the spectrum used by the data field. Other than that, the contents are arbitrary." | **Revised** |

**Discussion**

**In subclause 29.6.9.2.4(MU PPDU padding and space-time streams mapping), the following is specified.**

|  |
| --- |
| **For an MU PPDU transmission, all user PPDUs shall be aligned in time. If necessary, user PSDUs shall be padded according to the following steps:**   * **Compute the maximum number of OFDM symbols over all users  for *iuser* = 1, 2, …, *Nuser*.** * **Update the number of OFDM symbols at step d) in 29.6.9.2.3 as for *iuser* = 1, 2, …, *Nuser*. Update the number of pad bits for the *iuserth* user, , accordingly.** * **The number of pad OFDM symbols for the MU PPDU transmission for the *iuserth* user is defined as**   **The number of pad symbols takes into account MU PPDU padding only and does not include the regular padding described in 29.6.9.2.3.** |

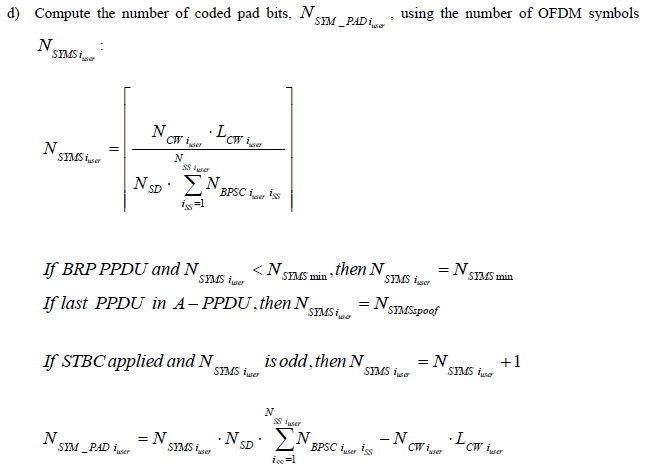
**This reads that the MU PPDU padding is performed by updating the number of pad bits in the encoding procedure. It is supposed that the remaining encoding process after step d) in 29.6.9.2.3 is performed to the MU PPDU pad bits as well.**

**Thus, we suppose we don’t need to add an additional specification as proposed by the commenter, but propose to add a text to clarify the step in the encoding procedure.**

**Proposed changes to D2.2**

29.6.9.2.3 LDPC encoding

***Editor: Insert a bullet after bullet d) in subclause 29.6.9.2.3 as follows (P526L19 of D2.2):***

****

1. **For an MU PPDU transmission, update the number of OFDM symbols as described in 29.6.9.2.4, then update the number of pad bits as described in step d) using updated number of OFDM symbols .**
2. **Concatenate coded bits with zero bits. They are scrambled using the continuation of the scrambler sequence that scrambled the PSDU input bits and data pad bits in step a).**
3. **Distribute the encoded and padded bits over the spatial streams on a group basis with the number of bits in a group. The first group of bits goes to the first spatial stream, the second group of bits goes to the second spatial stream, and so on. The procedure is repeated when the maximum number of spatial streams, , is reached. The procedure ends when all PSDU encoded bits, including pad bits, are distributed over the spatial streams.**

29.6.9.2.4 MU PPDU padding and space-time streams mapping

***Editor: Change the text in subclause 29.6.9.2.4 as follows (P529L6 of D2.2):***

**For an MU PPDU transmission, all user PPDUs shall be aligned in time. If necessary, user PSDUs shall be padded according to the following steps:**

* **Compute the maximum number of OFDM symbols over all users   
  for *iuser* = 1, 2, …, *Nuser*.**
* **Update the number of OFDM symbols at step e) in 29.6.9.2.3 as for *iuser* = 1, 2, …, *Nuser*. Update the number of pad bits for the *iuserth* user, , accordingly.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3388 | 29.9.1.1 | 526 | For the SISO phase of MU-MIMO beamforming, initiator TXSS subphase (i.e., Short SSW packet transmission) is followed by SISO feedback subphase. There is no setup subphase. | change "Setup Duration" in Figure 195 and Table 108 to "SISO Feedback Duration"  change "setup subphase" in Table 108 to "SISO feedback subphase". | **Accepted** |

**Discussion**

1. Agreed on the comment. The field name and the description should be changed.
2. Additionally, the name of the TXVECTOR parameter corresponds to the field should be changed.
3. Also, the MAC section should use TX/RXVECTOR parameters instead of references to PHY fields, as proposed below.

**Proposed changes to D2.2**

10.43.10.2.3.2 SISO phase

***Editor: Change the third and fourth paragraphs in subclause 10.43.10.2.3.2 as follows (P275L12 of D2.2):***

**The initiator performs the Initiator TXSS subphase through the use of the Short SSW packet (see 29.9.1). In each Short SSW packet transmitted as part of the Initiator TXSS, the initiator shall set the TXVECTOR parameter SSSW\_DIR to indicate Initiator, shall set the TXVECTOR parameter SSSW\_ADD\_MODE to indicate GroupAddr and shall set the TXVECTOR parameter SSSW\_DESTINATION\_AID to contain a group ID announced by the PCP or AP in the last transmitted EDMG Group ID Set element. In addition, the TXVECTOR parameter SSSW\_CDOWN shall be set to the number of Short SSW packets remaining until the end of the Initiator TXSS subphase and the TXVECTOR parameter SSSW\_SISO\_FEEDBACK\_DURATION shall be set to the duration of the following SISO Feedback subphase.**

**An MU-MIMO capable EDMG STA that receives a Short SSW packet indicating MU-MIMO transmission determines that it is an intended recipient of the packet by matching the value of the RXVECTOR parameter SSSW\_DESTINATION\_AID in the packet with a value of the EDMG Group ID subfield contained in the last received EDMG Group ID Set element. In case a match is found, the EDMG STA is an intended recipient of the packet if its AID is included in the EDMG Group ID subfield of the corresponding group. Otherwise, the EDMG STA is not an intended recipient of the packet and can ignore the remaining of the Initiator TXSS and SISO Feedback subphase, which can be done through the use of the value of the RXVECTOR parameters SSSW\_CDOWN and SSSW\_SISO\_FEEDBACK\_DURATION of the received Short SSW packet.**

**Table 45 —TXVECTOR and RXVECTOR parameters**

***Editor: Change the name and description of the parameter SSSW\_SETUP\_DURATION in Table 45 as follows (P381 of D2.2):***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SSSW\_SISO\_FEEDBACK\_DURATION | FORMAT is EDMG | Specifies the duration, in microseconds, of the SISO Feedback**(#3388)** subphase that starts following the Short SSW packet transmission with CDOWN field equal to 0. | Y | Y |

***Editor: Change the name of the Setup Duration field in Figure 208 as follows (P559L19 of D2.2):***

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Packet Type | Direction | Addressing Mode | Source AID | Destination AID | CDOWN | RF Chain ID | SISO Feedback Duration (#3388) | Reserved | FCS |
| Bits | 1 | 1 | 1 | 8 | 8 | 11 | 3 | 10 | 1 | 4 |

**Figure 208 —Short SSW Payload field when the Direction field is 0 (I-TXSS) and Addressing Mode field is 1**

**Table 118 —Short SSW Payload field definition**

***Editor: Change the name and description of the Setup Duration field in Table 118(Short SSW Payload field definition) as follows (P560 of D2.2):***

|  |  |
| --- | --- |
| SISO Feedback Duration | Corresponds to TXVECTOR parameter SSSW\_SISO\_FEEDBACK\_DURATION. Specifies the duration, in microseconds, of the SISO Feedback subphase that starts following the Short SSW packet transmission with CDOWN field equal to 0. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3184 | 29.9.1.1 | 527.1 | Encoding of values is missing for RF Chain ID in Table 108 | Add sentence "Encoded as RF\_CHAIN\_ID-1" to Definitions for RF Chain ID | **Revised** |

**Proposed changes to D2.2**

**Table 118 —Short SSW Payload field definition**

***Editor: Change the description for the RF Chain ID field in Table 118 as follows (P560 of D2.2):***

|  |  |
| --- | --- |
| RF Chain ID | Corresponds to TXVECTOR parameter RF\_CHAIN\_ID. The content of this field is set to the value of the RF\_CHAIN\_ID parameter minus one. Identifies the transmit chain currently being used for the transmission. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| 3186 | 29.9.1.2 | 528.16 | Missing reference for CRC-16-CCITT and how bits are encoded | Add reference to how bits are encoded for CRC-16-CCITT | **Revised** |

**Proposed changes to D2.2**

10.43.11.4 Initiator operation for TDD group beamforming

***Editor: Change the fifth paragraph in subclause 10.43.11.4 as follows (P316L7 of D2.2):***

Finally, the Responder ID subfield is generated by taking the 10 MSBs of CRC-16-CCITT computed over the scrambled MAC address. The CRC-16 is computed as defined in subclause 20.3.7.

29.9.1.2 Short Scrambled BSSID subfield definition

***Editor: Change the fourth paragraph in subclause 29.9.1.2 as follows (P561L16 of D2.2):***

Finally, the Short Scrambled BSSID subfield is generated by taking the 10 MSBs of CRC-16-CCITT computed over the scrambled BSSID. The CRC-16 is computed as defined in subclause 20.3.7.

**Straw Poll:**

* **Do you agree to accept the comment resolution for CIDs** 3053, 3171, 3184, 3186, 3187, 3188, 3190, 3290, 3365, 3369, 3388, 3597, 3723 **in 19/0043r0?**

**References**

[1] Draft P802.11ay D2.0

[2] Draft P802.11ay D2.2

[3] 11-17/0750r00 Length Calculation in EDMG PPDU