IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions of CIDs assigned to Graham D5 | | | | |
| Date: 2016-15-02 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SRT Wireless | Davie, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

This submission proposes resolution for several CIDs on D5.0

7344, 7389, 7425, 7431, 7443, 7473, 7550, 7589, 7592, 7593, 7598, 7599, 7600, 7635, 7640, 7654, 7769, 7772, 7773, 7786

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.

R1 Added Brian’s response to CID 7786 and changed proposal.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7344  Mark Rison  11.2.6.3.3  1612.57 | It says "The PCP provides the PBSS timing synchronization (TSF)" -- but the TSF is more than just that | Delete "(TSF)" |

Discussion:

This is a Note in 11.2.6.3.3 PCP operation with a wakeup schedule

PCP is PBSS control point in a DMG BSS

Full text:

*NOTE—The PCP provides the PBSS timing synchronization (TSF). Transmitting frequent TSF information through DMG Beacon or Announce frames is important when there are non-PCP STAs in the PBSS that rely on TSF information to communicate directly with each other.*

TSF is “Timing Synchronization Function” so on the face of it, “PBSS timing synchronization (TSF)” seems reasonable. Then again, deleting it does not alter the note in any way.

*Mark*

*The point is that TSF is “Timing Synchronisation \*Function\*”, not just the “timing synchronisation”*

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7389  Mark Rison  11.25.3.1.4  1805.16 | "the configured Query Response Length Limit" -- what's this?  A field in some frame?  dot11GASQueryResponseLengthLimit? | Either add "field in the <x> frame" after, or change to "dot11GASQueryResponseLengthLimit" |

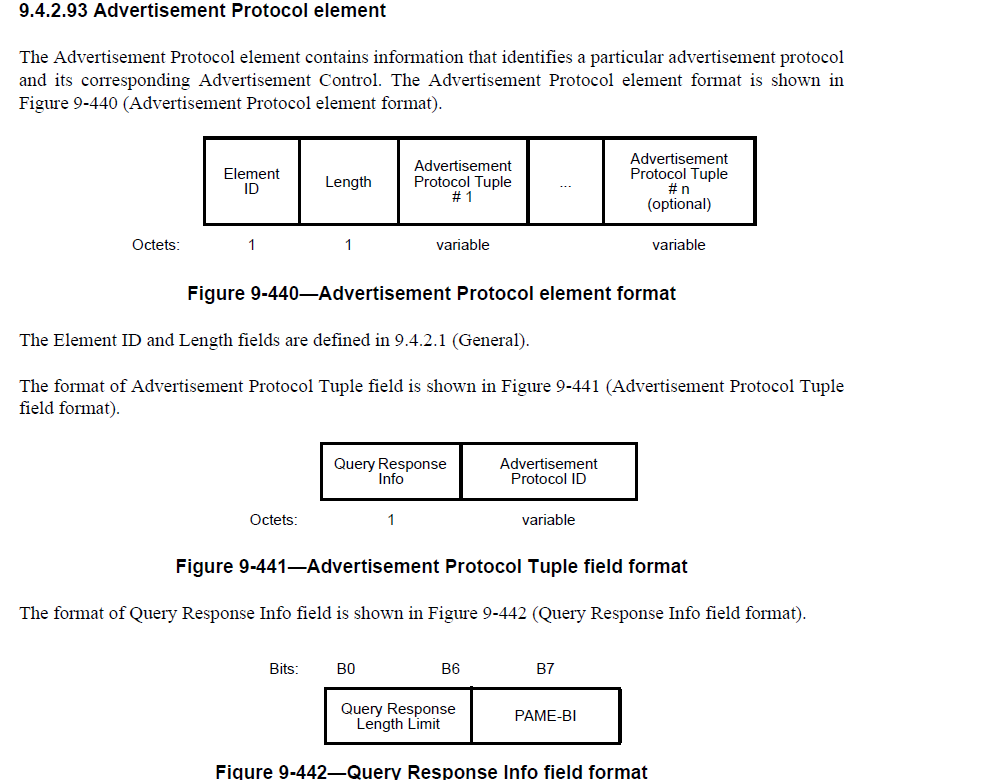
Discussion:

Full text from 11.25.3.14

***“After receiving a query response from the Advertisement Server,*** the responding STA shall buffer the query response for a minimum of dot11GASResponseBufferingTime after the expiration of the GAS Comeback Delay or until the query response is delivered. If the responding STA does not receive a GAS Comeback Request frame whose source MAC address and dialog token match the source MAC address and value of the Dialog Token field respectively of the corresponding GAS Initial Response frame within this time, it may drop the query response. **If the query response is larger than the configured Query Response Length Limit,** the responding STA shall discard the response and instead return a status code of GAS\_QUERY\_RESPONSE\_TOO\_ LARGE in the GAS Comeback Response frame. This behavior helps to prevent abuses of the medium that may be caused by overly general queries, which evoke a very large query response.”

We have a Status Code Table 9-46 P665.19

63 GAS\_QUERY\_RESPONSE\_TOO\_ LARGE GAS Response is larger than query response length limit



So Query Response Length Limit is in the Advertisement Protocol element.

We also have

1805.61

“If the Query Response received from the Advertisement Server is larger than dot11GASQueryResponseLengthLimit or requires more than 128 fragments for transmission

to the requesting STA, it shall be dropped by the responding STA.”

That appears to to be the same instruction so let’s go with that.

*Mark R*

*I’m confused. So you ignore the Query Response Length Limits in the Advertisement Protocol Tuples in the Advertisement Protocol element?*

*Have you checked with Stephen that this is OK?*

GS - Yes, I await an answer.

Proposed Resolution

REVISED

At P1805.16

Replace “the configured Query Response Length Limit”, with “dot11GASQueryResponseLengthLimit”

“If the query response is larger than dot11GASQueryResponseLengthLimit,”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7425  Mark Rison  11.24.6.2  1772.36 | "NOTE---The mechanism by which t1' and t4' are derived from the TOD and TOA fields, and the mechanism by which t2 and t3 are determined, are implementation dependent." -- also the mechanism by which the TOD and TOA fields are determined for transmission.  Also the primes around here seem to have variable italicness and indeed sex (sexless or not) | Change to "At the responding STA, the mechanism by which t1' and t4' are derived from the TOD and TOA fields, and the mechanism by which t2 and t3 are determined, are implementation dependent.  At the initiating STA, the mechanism by which the TOD and TOA fields are determined is implementation dependent." Make sure all the primes are the same throughout this subclause |

Discussion:

Here is the text:

‘The round trip time (RTT) is defined by Equation (11-5).

*RTT* = [(*t4*’ – *t1’*) – (*t3* – *t2*)] (11-5)

where *t1’* and *t4’* are the time at which the Fine Timing Measurement frame was transmitted and the time at which the Ack was received, respectively, as determined by the initialing STA.

NOTE—The mechanism by which *t1’* and *t4’* are derived from the TOD and TOA fields, and the mechanism by which *t2* and *t3* are determined, are implementation dependent.’

See Figure 11-37 (P1771)

*t1’* and *t4’* are derived at the Responding STA and transmitted to the Initiating STA

*t2* and *t3* are at the Initiating STA.

Is the Note confusing as it stands? I personally don’t think so. Changing to the commenter’s text is however correct so why not?

The “prime” comment is right. We have two varieties.

[(*t4*’ – *t1’*)

And

*[(t2 - t1') - (t4' - t3)]/2*

*Mark R - I’m discussing this with Jonathan and Carlos, so probably better to hold off doing anything for now*

Proposed Resolution (awaiting any further input from Mark, Jonathan and Carlos)

REVISE (effectively Accept)

At 1772.36 change

“NOTE—The mechanism by which *t1’* and *t4’* are derived from the TOD and TOA fields, and the mechanism by which *t2* and *t3* are determined, are implementation dependent.’  
To

"At the responding STA, the mechanism by which t1' and t4' are derived from the TOD and TOA fields, and the mechanism by which t2 and t3 are determined, are implementation dependent.  At the initiating STA, the mechanism by which the TOD and TOA fields are determined is implementation dependent."

At the following locations, use the same symbol for ‘prime’ P1772 lines 31, 36, 45.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7431  Mark Rison  11.3.5  1622.07 | There are 6 instances of "set to State 4(,) or State 3 if RSNA establishment is required" -- -- how does the MLME know?  Using the presence of the RSNE in the MLME-ASSOC.resp?  No, it's not defined there.  Using the MIB variable?  It's not clear an RSNA is required if dot11RSNAActivated is set to true ("When this object is true, this indicates that RSNA is enabled on this entity.") | Change "if RSNA establishment is required" to "if dot11RSNAActivated is true" in each case, after verifying whether this is indeed necessary and sufficient |

Discussion:

Six places.

P1623.51

d) If an Association Response frame is received with a status code of SUCCESS, the state for the AP or

PCP shall be set to State 4 or State 3 if RSNA Establishment is required.

e) An MM-SME coordinated STA that receives an Association Response frame with a status code of

SUCCESS containing an MLME element with the Single AID field equal to 1, all of the STAs coordinated by the MM-SME are associated with the AP or PCP (i.e., shall be set to State 4 or State

3 if RSNA Establishment is required).

1626.5

l) If an Association Response frame with a status code of SUCCESS is acknowledged by the STA, the state for the STA shall be set to State 4, or to State 3 if RSNA establishment is required.

1626.63

c) If a Reassociation Response frame is received with a status code of SUCCESS, the state variable for the new AP or PCP shall be set to State 4, or to State 3 if RSNA establishment is required

1627.63

e) An MM-SME coordinated STA that receives a Reassociation Response frame with a status code of

SUCCESS containing an MLME element with the Single AID field equal to 1, all of the STAs coordinated by the MM-SME are reassociated with the AP or PCP (i.e., shall be set to State 4 or

State 3 if RSNA Establishment is required).

1630.7

l) If a Reassociation Response frame with a status code of SUCCESS is acknowledged by the STA, the

state for the STA shall be set to State 4, or to State 3 if RSNA establishment is required and the reassociation is not part of a fast BSS transition.

All are concerned with (Re) Associastion Response frames.

We find at P1622.47 the following:

*“If an MM-SME coordinated STA receives an Association Response frame with a result code equal to SUCCESS and with the value of the Single AID field within MMS element equal to 1, then*

*— For each of its MAC entities advertised within the MMS element and* ***for which dot11RSNAEnabled is true, the state is set to State 3****. Progress from State 3 to State 4 occurs independently in each such MAC entity.*

*— For each of its MAC entities advertised within the MMS element and for which dot11RSNAEnabled is false, the state is set to State 4.”*

Soo…The setting to State 3 is indeed when “*dot11RSNAEnabled is true*”

*Comment from Mark R*

*Unfortunately, this MIB variable does not actually exist (in C.3)! The MIB variables in C.3 are dot11RSNAOptionImplemented and dot11RSNAActivated. However, it’s not clear to me that either of these means “RSNA establishment is required”*

Response from GS

There are 16 instances of ‘dot11RSNAEnabled” but as Mark points out, none in C.3

I looked in 802.11 – 2007 and sure enough it is there in Annex D

dot11RSNAEnabled OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"When this object is set to TRUE, this shall indicate that RSNA is

enabled on this entity. The entity will advertise the RSN Information

Element in its Beacon and Probe Response frames. Configuration

variables for RSNA operation are found in the dot11RSNAConfigTable.

This object requires that dot11PrivacyInvoked also be set to TRUE."

::= { dot11PrivacyEntry 7 }

dot11RSNAPreauthenticationEnabled OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"When this object is set to TRUE, this shall indicate that RSNA

preauthentication is enabled on this entity.

This object requires that dot11RSNAEnabled also be set to TRUE."

::= { dot11PrivacyEntry 8 }

I look further:

I notice that dot11PrivacyInvoked uses *dot11RSNAEnabled* in 2007 but in D5.0 this is replaced by *dot11RSNAActivated.* There are 64 instances of *dot11RSNAActivated*

As I check it looks as though at some time *dot11RSNAEnabled* was replaced by *dot11RSNAActivated*.

See P2924.33 dot11PrivacyInvoked

**“For RSNA-capable clients, an additional variable dot11RSNAActivated indicates whether RSNA is enabled.”**

In 2007 it says

**“For RSNA-capable clients, an additional variable dot11RSNAEnabled indicates whether RSNA is enabled.”**

But they did not catch all the changes?

Proposed Resolution

REVISED

At the following locations: 1623.53, 1623.61, 1626.10, 1626.64, 1627.63, 1630.9

Replace:

“if RSNA establishment is required”

With

“if dot11RSNAActivated is true”

AND

Globally Replace “dot11RSNAEnabled” with “dot11RSNAActivated” (16 places)

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7443  Mark Rison  11.11.15.2  1710.18 | "in the Supported RM Capabilities Enabled bitmask element" -- there is no such element | Change to "in the RM Enabled Capabilities element" |

Discussion:

Correct, “Supported RM Capabilities Enabled” occurs just once at this location. The correct element is RM Enabled Capabilities

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7473  Mark Rison | According to Solomon TRAININ, HT delayed is not supported in DMG.  Where is this in the spec? | Add a statement to that effect |

Discussion:

P1400.27

**10.24.8 HT-delayed block ack extensions**

**10.24.8.1 Introduction**

Subclauses 10.24.8.2 (HT-delayed block ack negotiation) and 10.24.8.3 (Operation of HT-delayed block ack) define an HT extension to the block ack feature to support operation on delayed block ack agreements established between HT STAs. Other than the exceptions noted in 10.24.8.1 (Introduction) through 10.24.8.3 (Operation of HT-delayed block ack), the operation of HT-delayed block ack is the same as is described in 10.24.7 (HT-immediate block ack extensions). The HT-delayed extensions simplify the use of delayed block ack in an A-MPDU and reduce resource requirements.

**A DMG STA shall not use HT-delayed block ack.**

Is this not the statement?

Proposed Resolution

REJECT

At P1400.43 it is stated that “A DMG STA shall not use HT-delayed block ack.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7550  Mark Rison  11.24.6  1764.23 | When may an FTM session be implicitly terminated (i.e. no FTM with DT 0)? | Add a statement that the responding STA may terminate an FTM session at any point (not just after the last FTM frame of the last burst instance) |

Discussion:

Reached out to Ganesh, response was:

Cl. 11.24.6.6 fine timing measurement termination lists four ways to terminate a FTM session. The fourth mechanism is the implicit termination – when the negotiated number of FTM bursts have completed, the session terminates.

Looking at just the comment – it appears that the commenter is asking a question/clarification. Not proposing a change to the specification. If you agree with this interpretation, you could just point the commenter to the fourth bullet in the list in CL. 11.24.6.6 and you would be done.

However, if you look at the comment and the proposed change (the proposed change does not seem to address the comment) then maybe there is a need to change the specification (and probably do more than what the commenter is seeking)! If this is what you prefer, here is my proposal:

There are four ways an FTM session is terminated:

* At any time during the FTM session, the responding STA sends a Fine Timing Measurement frame with the Dialog Token field set to 0
* At any time during the FTM session, the initiating STA sends a Fine Timing Measurement Request frame with the Trigger field set to 0. This frame shall not include:
  + A Measurement Request element
  + A Fine Timing Measurement Parameters element
* At any time during the FTM session, the initiating STA terminates the current session and requests a new session with modified Fine Timing Measurement Parameters (see 11.24.6.5 (Fine timing measurement parameter modification))
* After the number of burst instances indicated in the Number of Bursts Exponent field in the initial Fine Timing Measurement frame has been reached.

*Comment from Mark R*

*I’m discussing this with Ganesh, so probably better to hold off doing anything for now*

Proposed Resolution (awaiting response from Mark and Ganesh)

REVISED

At P1773.40 make the following edits:

“There are four ways an FTM session is terminated:

— At any time during the FTM session, the responding STA sends a Fine Timing Measurement frame with the Dialog Token field set to 0.

— At any time during the FTM session, the initiating STA sends a Fine Timing Measurement Request frame with the Trigger field set to 0.

This frame shall not include:

— a Measurement Request element

— a Fine Timing Measurement Parameters element

— At any time during the FTM session, the initiating STA terminates the current session and requests a new session with modified Fine Timing Measurement parameters (see 11.24.6.5 (Fine timing measurement parameter modification)).

— After the number of burst instances indicated in the Number of Bursts Exponent field in the initial Fine Timing Measurement frame has been reached.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7589  Mark Rison  11.14  1719.55 | "If a non-AP STA that has an SA with its AP for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the AP" -- this should be in the clauses dealing with receipt of deauth/disassoc | Move the behavioural description to subclauses 11.3.4.5 and 11.3.5.9, splitting it into the form "if get this frame then invoke SA as defined in x.x" |

Discussion:

11.14 SA Query procedures

If dot11RSNAProtectedManagementFramesActivated is true, then the STA shall support the SA Query procedure.

……

If a non-AP and non-PCP STA that has an SA with its AP or PCP for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the AP or PCP, the non-AP and non-PCP STA may use this as an indication that there might be a mismatch in the association state between itself and the AP or PCP. In such a case, the non-AP and non-PCP STA’s SME may initiate the **SA Query procedure** with the AP or PCP to verify the validity of the SA **by issuing one MLME-SA-QUERY.request** primitive every dot11AssociationSAQueryRetryTimeout TUs until a matching MLME-SAQUERY.confirm primitive is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the **SA Query procedure** has passed. If the AP or PCP responds to the **SA Query request with a valid SA Query response** that has a matching transaction identifier, the non-AP STA should continue to use the SA. **If no valid SA Query response** is received, the non-AP and non-PCP STA’s SME may delete the SA and temporal keys held for communication with the STA by issuing an MLME-DELETEKEYS.request primitive and the non-AP and non-PCP STA may move into State 1 (or State 2, for a DMG STA) with the AP.

I see “SA Query” used several times in this pargraph. Hence, without going deep into it, it appears that it is valid to have this text here.

Proposed Resolution

A good case can be made for keeping the text where it is as is certainly deals with SA query response. To change the text into another form, as proposed, a submission would be required.

Recommend CID be transferred to Mark R for a submission.

*Mark R*

*I will bring such a submission*

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7592  Mark Rison  11.2.2.6  1581.34 | If in a U-APSD SP an AP ends the SP part-way through a fragmented MSDU/MMPDU, what happens at the next SP?  Does the AP start from the beginning? | Add "If the BU is fragmented but not all fragments are transmitted within the current service period, it shall start the next service period with the first unacknowledged frame." |

Discussion:

The cited para is for PS-Poll

“For a STA using U-APSD, the AP transmits one BU destined for the STA from any AC that is not delivery-enabled in response to PS-Poll frame from the STA. The AP should transmit the BU from the highest priority AC that is not delivery-enabled and that has a buffered BU. When all ACs associated with the STA are delivery-enabled, the AP transmits one BU from the highest priority AC that has a BU. The AP can respond with either an immediate Data or Management frame or with an Ack frame, while delaying the responding Data or Management frame.”

Of course the STA should be sending a trigger Qos Data Null not a PS-Poll. But if the STA is stupid enough to send a PS-Poll…

*Comment from Mark R*

*Ah, good point. Changes are also needed at 1580.51, i.e. step d) for USPs*

GS – I have proposed changes to d)

A PS-Poll only causes one BU to be sent, I am surprised that two parts of a fragmented packet may be sent as the result of a single PS-Poll and one could argue that is not true as each part of a fragmented packet is individually ACKed then one might assume that each needs its own PS-Poll.

For example, does the STA note that it received a fragment and **not** send another PS-Poll and does the AP send the second fragment as soon as it gets the ACK? I wonder. If I was a STA I think (know) I would send another PS-Poll anyway. (Mark R, yes it can, but need not)

Reached out to Mark H:

I'd say that things are a little messed up (what's new?).  Here are some quotes:

9.3.4.4 (**10.3.4.4** in REVmc):

A STA in PS mode, in an ESS, initiates a frame exchange sequence by transmitting a PS-Poll frame to request data from an AP. In the event that neither an ACK frame nor a data frame is received from the AP in response to a PS-Poll frame, then the STA shall retry the sequence, by transmitting another PS-Poll frame. If the AP sends a data frame in response to a PS-Poll frame, but fails to receive the ACK frame acknowledging this data frame, the next PS-Poll frame from the same STA may cause a retransmission of the last MSDU. If the AP responds to a PS-Poll by transmitting an ACK frame, then responsibility for the data frame delivery error recovery shifts to the AP because the data are transferred in a subsequent frame exchange sequence, which is initiated by the AP. **The AP shall attempt to deliver one MSDU to the STA that transmitted the PS-Poll**, using any frame exchange sequence valid for an individually addressed MSDU. If the PS STA that transmitted the PS-Poll returns to Doze state after transmitting the ACK frame in response to successful receipt of this MSDU, but the AP fails to receive this ACK frame, then the AP retries transmission of this MSDU until the relevant retry limit is reached. See Clause 10 for details on filtering of extra PS-Poll frames.

The problem in the above is that “data frame” and “MSDU” get interchanged.  We have agreed that “frame” means MPDU.  So, we have a mess.

10.2.1.1 (**11.2.2.1** in REVmc): In a BSS operating under the DCF, or during the CP of a BSS using the PCF, upon determining that a BU is currently buffered in the AP, a STA operating in the PS mode shall transmit a short PS-Poll frame to the **AP, which shall respond with the corresponding buffered BU immediately, or acknowledge the PS-Poll and respond with the corresponding BU at a later time**.

This one, above, as you seem have triggered on, uses “BU”.  Which is, of course, an MSDU.

And, in Annex G, we have this for a “frame sequence” (which are all separated by SIFS):

( [**CTS** | **RTS CTS** | **PS-Poll**] {frag-frame **ACK**} last-frame **ACK** )

**Which brings to mind the idea from way back that a fragmented MSDU would (almost always) be delivered as a rapid sequence of MPDUs, not as MPDUs handled like individual frames/frame sequences.**

To me, this all comes down to how things are queued, during power saving.  In my mind, MSDUs (BUs) are queued, not MPDUs.  The TIM indicates BUs, APSD talks about delivering BUs, etc.  So, when an AP is triggered by PS-Poll, U-APSD trigger, etc., it releases a BU.  It is downstream from there that the BU gets fragmented, encrypted, etc., and finally goes out as one or more MPDUs to make it to the PS STA.  The PS STA needs to understand that the power save interaction is not complete until the appropriate MSDUs (not MPDUs) are received correctly.

So, my conclusion is that the intent is for an entire MSDU (really, a BU) to be delivered in response to the PS-Poll, but the language in 9.3.4.4 (10.3.4.4) should be fixed to replace “data frame” with “data frame(s)”.  (Or, better yet, “BU”.)  That is, **I do think the intent is to deliver the entire MSDU at once, in response to the poll,** so the STA knows that the buffered state/status in the AP now reflects the next MSDU, the AP can be done with MSDU, etc.  Otherwise, a partially delivered MSDU (only some fragments delivered) is very messy to handle with power save buffering.

All this of course brings up the question of why you are asking?  Nobody really does fragmentation anymore, do they?

OK so both Mark’s agree that a fragmented BU is delivered with just one PS-Poll – or should be (my experience with APs doing PS would lead me to be sceptical). Hence we shall recommend to ACCEPT the comment proposal.

Should I attempt to fix 10.2.4.4? Why not?

Also look at 1580 d)

Proposed Resolution

OPTION A

ACCEPT

OPTION B

REVISED

At P1581.41 add at end of paragraph

"If the BU is fragmented but not all fragments are transmitted within the current service period, it shall start the next service period with the first unacknowledged frame."

AND

Make following changes 10.3.4.4

At P1294.9

“A STA in PS mode, in an infrastructure BSS, initiates a frame exchange sequence by transmitting a PS-Poll frame to request one buffered BU from an AP. If no Ack, Data, or Management frame is received from the AP in response to a PS-Poll frame, then the STA shall retry the sequence, by transmitting another PS-Poll frame. If the AP sends a BU in response to a PS-Poll frame, but fails to receive the Ack frame acknowledging this BU, the next PS-Poll frame from the same STA may cause a retransmission of the last BU 30. If the AP responds to a PS-Poll frame by transmitting an Ack frame, then responsibility for the BU delivery error recovery shifts to the AP because the BUs are transferred in a subsequent frame exchange sequence, which is initiated by the AP. The AP shall attempt to deliver one BU, MSDU or MMPDU, to the STA that transmitted the PS-Poll frame, using any frame exchange sequence valid for an individually addressed MSDU or MMPDU. If the PS STA that transmitted the PS-Poll frame returns to doze state after transmitting the Ack frame in response to successful receipt of this BU, but the AP fails to receive this Ack frame, then the AP retries transmission of this BU until the relevant retry limit is reached. See 11.2.2.8 (Receive operation for STAs in PS mode during the CP) for details on filtering of extra PS-Poll frames.

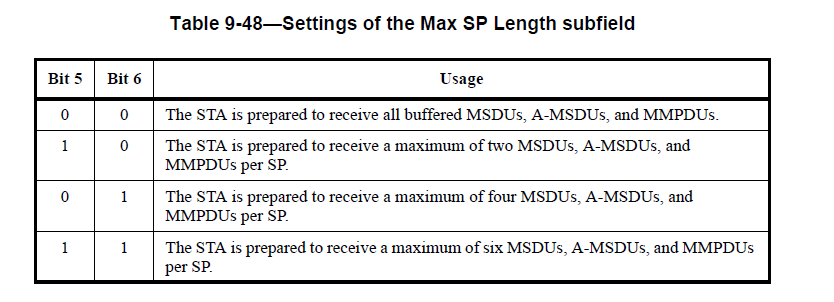
AND

d) If a STA has set up a scheduled SP, it shall automatically wake up at each SP. Therefore, the APSDcapable AP shall transmit frames associated with admitted traffic with the APSD subfield equal to 1 in the TSPECs buffered for the STA during a scheduled SP. If the STA has set up to use unscheduled SPs, the AP shall buffer BUs using delivery-enabled ACs until it has received a trigger frame using a trigger-enabled AC or a PS-Poll frame from the non-AP STA, which indicates the start of an unscheduled SP. A trigger frame received by the AP from a STA that already has an unscheduled SP underway shall not trigger the start of a new unscheduled SP. The AP transmits BUs destined for the STA and using delivery-enabled ACs during an unscheduled SP. A PS-Poll frame received by the AP from a STA starts a new unscheduled SP, see 10.3.4.4. The bit for AID 0 (zero) in the Bitmap Control field of the TIM element shall be set to 1 when non-GCR-SP group addressed traffic is buffered, according to 9.4.2.6 (TIM element).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7593  Mark Rison  11.2.2.5.1  1576.53 | Does the part-BU of the previous SP count as one or zero (if the Max SP Length was not indeterminate)? | After "An unscheduled SP ends after the AP has attempted to transmit at least one BU using a delivery-enabled AC and destined for the STA, but no more than the number indicated in the Max SP Length field of the QoS Capability element of the STA's (Re)Association Request frame if the field has a nonzero value" add ", including any BU that was already partially transmitted in a previous unscheduled SP" |

Discussion:

“If there is no unscheduled SP in progress, the unscheduled SP begins when the AP receives a trigger frame from a STA, which is a QoS Data or QoS Null frame using an AC the STA has configured to be trigger enabled. An A-MPDU that contains one or more trigger frames acts as a trigger frame. **An unscheduled SP ends after the AP has attempted to transmit at least one BU using a delivery-enabled AC and destined for the STA, but no more than the number indicated in the Max SP Length field of the QoS Capability element of the STA’s (Re) Association Request frame if the field has a nonzero value, i**ncludingany BU that was already partially transmitted in a previous unscheduled SP. By setting the EOSP field to 1 in the last frame sent during the SP, an unscheduled SP may be terminated before the maximum number of BUs in the SP has been reached. The times at which an AP may transmit during an unscheduled SP might be constrained by the U-APSD coexistence mechanism (see 11.2.2.5.2 (U-APSD coexistence)).”



So the STA can specify the maximum number of BUs it is willing to accept per SP (although I struggle to understand why). The comment is concerned with a part BU left over from the previous SP and supports the proposed solution to the previous comment.

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7598  Mark Rison  11.2.2.1  1574.26 | "In a BSS operating under the DCF, or during the CP of a BSS using the PCF, upon determining that a BU is currently buffered in the AP, a STA operating in the normal (non-APSD) PS mode transmits a PS-Poll frame to the AP, which responds with the corresponding buffered BU immediately, or acknowledges the PS-Poll frame and respond with the corresponding BU at a later time." -- also under EDCA | Add "or EDCA" before the first comma |

Discussion:

Yes, this is the action if using PS-Poll.

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7599  Mark Rison  11.2.2.6  1581.34 | "For a STA using U-APSD, the AP transmits one BU destined for the STA from any AC that is not delivery-enabled in response to PS-Poll frame from the STA. The AP should transmit the BU from the  highest  priority  AC  that  is  not  delivery-enabled  and  that  has  a  buffered  BU.  When  all  ACs associated with the STA are delivery-enabled, the AP transmits one BU from the highest priority AC that has a BU. The AP can respond with either an immediate Data or Management frame or with an Ack frame, while delaying the responding Data or Management frame." -- this last sentence also needs to be made when using legacy PS | After the first sentence of step g) add "The AP shall respond after SIFS with either a Data or Management frame or with an Ack frame." |

Discussion:

g) When the AP receives a PS-Poll frame from a STA that has been in PS mode, it shall forward to the STA a single buffered BU. The AP shall respond after SIFS with either a Data or Management frame or with an Ack frame.

*Mark R - I’m wondering whether this too needs a “****,*** *while delaying the responding Data or Management frame” as in the next para*

*GS – Agree, I have proposed such wording*

(continued)Until the transmission of this BU either has succeeded or is presumed failed (when maximum retries are exceeded), the AP shall acknowledge but ignore all PS-Poll frames from the same STA. This prevents a retried PS-Poll frame from being treated as a new request to deliver a buffered BU.

For a STA using U-APSD, the AP transmits one BU destined for the STA from any AC that is not delivery-enabled in response to PS-Poll frame from the STA. The AP should transmit the BU from the highest priority AC that is not delivery-enabled and that has a buffered BU. When all ACs associated with the STA are delivery-enabled, the AP transmits one BU from the highest priority AC that has a BU. **The AP can respond with either an immediate Data or Management frame or with an Ack frame,** while delaying the responding Data or Management frame.”

Only question is whether necessary to include SIFS which is not in the cited sentence. (See next CID)

In the next para we see the phrase “while delaying the responding Data or Management frame”. This refers to the case when the ACK is sent, but it is not that clear. Also as the commenter observed, this should be included.

Proposed Resolution

REVISED

At P1581.34 Insert after the first sentence of g)

“The AP shall respond after SIFS with either an immediate Data or Management frame or, while delaying the responding Data or Management frame, with an Ack frame.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7600  Mark Rison  11.2.2.6  1581.39 | "The AP can respond with either an immediate Data or Management frame or with an Ack frame, while delaying the responding Data or Management frame." -- exactly when is this "immediate" frame to be sent? | Change to "The AP shall respond after SIFS with either a Data or Management frame or with an Ack frame." |

Discussion:

“For a STA using U-APSD, the AP transmits one BU destined for the STA from any AC that is not delivery-enabled in response to PS-Poll frame from the STA. The AP should transmit the BU from the highest priority AC that is not delivery-enabled and that has a buffered BU. When all ACs associated with the STA are delivery-enabled, the AP transmits one BU from the highest priority AC that has a BU. **The AP can respond with either an immediate Data or Management frame or with an Ack frame,** while delaying the responding Data or Management frame.”

Proposed Resolution

REVISE

At 1581.39 replace

“The AP can respond with either an immediate Data or Management frame or with an Ack frame, while delaying the responding Data or Management frame.”

with

“The AP shall respond after SIFS with either an immediate Data or Management frame or, while delaying the responding Data or Management frame, with an Ack frame.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7635  Mark Rison  11.1.4.3  1564.44 | What does "process all received probe responses" (2 instances) mean, exactly? | Change each to "process all received probe responses to construct BSSDescriptions corresponding to each" |

Discussion:

P1565.14 (non-DMG)

“g) Wait until the timer reaches MaxChannelTime and process all received probe responses.”

Then we have the instruction at line 43 (after Figure 11-4)

“When all channels in the ChannelList have been scanned, the MLME shall issue an MLME-SCAN.confirm primitive with the BSSDescriptionSet containing all of the information gathered during the scan.”

P1566.35 (DMG)

“h) When the timer reaches MaxChannelTime, process all received probe responses.”

No equivalent instruction.

Proposed Resolution

ACCEPT

Note: REVISED by M.R. 4/24/16

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7640  Mark Rison  11.1.4.3.4  1567.15 | Re CID 5208: The assertion "multi-band capable non-AP STAs can respond to Probe Requests" needs some backing evidence (i.e. a specific spec location where this is required/allowed, other than the location which was the subject of that comment) | Delete this criterion |

Discussion:

“A STA that receives a Probe Request frame shall not respond if any of the following apply:

a) The STA does not match any of the following criteria:

1) The STA is an AP.

2) The STA is an IBSS STA.

3) The STA is a mesh STA.

4) The STA is a DMG STA that is not a member of a PBSS and that is performing active scan as defined in 11.1.4.3.3 (Active scanning procedure for a DMG STA).

5) The STA is a PCP.

6) **The STA is a multi-band capable non-AP STA for which the last received probe request included a Multi-band element**.”

Note that a non-AP STA shall not respond.

So this list is for those who CAN RESPOND, including **the multi-band capable non-AP STA for which the last received probe request included a Multi-band element**.

P1029.20 9.4.2.138 Multi-band element

*“The Multi-band element indicates that the STA transmitting this element (the transmitting STA) is within a multi-band device capable of operating in a frequency band or operating class or channel other than the one in which this element is transmitted and that the transmitting STA is able to accomplish a session transfer from the current channel to a channel using another STA in the same device, in the other or same band.”*

Note that this description includes APs and non-AP STAs.

So in this case a multi-band non-AP STA sends a probe request and the rule says that another multi-band non-AP STA shall respond with a Probe Response. Hmmm…does seem strange. But we must ask why this rule was added at all? What were they thinking? Sounds like a DMG thing to me.

OK part of the Multi-band element is “STA Role subfield”.

P1030.1

*NOTE—A STA can perform in more than one role in a channel, and the STA Role subfield identifies the role that is most relevant for the STA for that channel.*

Hence a multi-band non-AP STA can be an AP in another channel (I think), but the “*The STA Role subfield specifies the role the transmitting STA plays on the channel of the operating class indicated in this element*.”

Maybe we can imagine a case where a multi-band non-AP STA receives a probe request indicating ability in a channel where the multi-band non-AP STA can be an AP? Is that what was meant? If so it needs a lot more description than what is there and maybe the last part of the sentence somewhere got lost?

i.e. The STA is a multi-band capable non-AP STA for which the last received probe request included a Multi-band element **indicating support in a channel where the STA role is an AP.” (would need a lot of work)**

***CARLOS***

*I believe the intent of (6) had probably to do with receiving a Probe Request over, say, 2.4 GHz to discovery the capabilities over another band (5 or 60 GHz). But since this behavior is not well specified, it probably makes sense to delete (6).*

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7654  Mark Rison  11.2.2.2  1574.61 | "To  change  power  management  modes  a  STA  shall  inform  the  AP  by  completing  a  successful  frame exchange (as described in Annex G) that is initiated by the STA and that includes a Management frame, Extension frame or Data frame, and also an Ack or a BlockAck frame from the AP." does not make it clear that the frame exchange is required to include an Ack/BA (the NOTE 1 below does make this clear, but it's not normative) | Change to "To  change  power  management  modes  a  STA  shall  inform  the  AP  by  completing  a  successful  frame exchange (as described in Annex G) that is initiated by the STA and that is required to include a Management frame, Extension frame or Data frame, and also an Ack or a BlockAck frame from the AP." |

Discussion:

The proposed change would be:

To change power management modes a STA shall inform the AP by completing a successful frame exchange (as described in Annex G) that is initiated by the STA and is required to include a Management frame, Extension frame or Data frame, and also an Ack or a BlockAck frame from the AP. The Power Management subfield(s) in the Frame Control field of the frame(s) sent by the STA in this exchange indicates the power management mode that the STA shall adopt upon successful completion of the entire frame exchange, except where the Power Management field is reserved (see 9.2.4.1.7 (Power Management subfield)). A non- AP STA shall not change power management mode using a frame exchange that does not receive an Ack or BlockAck frame from the AP, or using a BlockAckReq frame.

NOTE 1—A PS-Poll frame exchange does not necessarily result in an Ack frame from the AP, so a non-AP STA cannot change power management mode using a PS-Poll frame.

Proposed Resolution

ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7769  Mark Rison  11.23.6  (1774.52)  1748.18  And  1749.26 | "any" v. "all" in  "Switching to a 40 MHz off-channel direct link is achieved by including the following information in the TDLS Channel Switch Request frame:  --- Operating Class field indicating 40 MHz Channel Spacing  --- Secondary Channel Offset field indicating SCA or SCB" implies all need to be present"  v.  "Switching to a wideband off-channel direct link is achieved by including any of the following information in the TDLS Channel Switch Request frame:  --- An Operating Class element indicating 40 MHz Channel Spacing  --- A Secondary Channel Offset element indicating SCA or SCB  --- A Wide Bandwidth Channel Switch element indicating 80 MHz, 160 MHz, or 80+80 MHz channel width" | State that 11.23.6.3 only applies to non-VHT HT STAs and 11.23.6.5 only applies to VHT STAs |

Discussion:

First we look at 11.23.6.3. The comment is to state that this only applies to non-VHT HT STAs.

**11.23.6.3 Setting up a 40MHz direct link**

**11.23.6.3.1 General**

“A 40 MHz off-channel direct link may be started if both TDLS peer STAs indicated 40 MHz support in the Supported Channel Width Set field of the **HT Capabilities element** (which is included in the TDLS Setup Request frame and the TDLS Setup Response frame).

Switching to a 40 MHz off-channel direct link is achieved by including the following information in the TDLS Channel Switch Request frame:  
  
--- Operating Class field indicating 40 MHz Channel Spacing  
  
--- Secondary Channel Offset field indicating SCA or SCB

This implies that both the Operating Class and the Secondary Offset field be included.

In 11.23.6.5.1 it clearly states “any of the following information”

In the Channel Switch Request:

Operating Class

1 octet field that specifies the operating class for the target channel.

The secondary channel offset

**is present** if a switch to a 40 MHz direct link is indicated and is absent otherwise.

This is clear then “secondary channel offset” MUST be present. Operating Classes, as far as I know, are not mandatory to include. Therefore I conclude that this should be

“Switching to a 40 MHz off-channel direct link is achieved by including any of the following information in the TDLS Channel Switch Request frame”

Now let’s look at

**11.23.6.5. Setting up a wide bandwidth off-channel direct link**

**11.23.6.5.1 General**

“A wideband TDLS off-channel TDLS direct link is a 40 MHz, 80 MHz, 160 MHz, or 80+80 MHz off channel TDLS direct link.

A wideband off-channel TDLS direct link may be started if both TDLS peer STAs indicated wideband support in the **VHT Capabilities element VHT Capabilities Information field included** in the TDLS Setup Request frame or the TDLS Setup Response frame.

Switching to a wideband off-channel direct link is achieved by including any of the following information in the TDLS Channel Switch Request frame:  
  
--- An Operating Class element indicating 40 MHz Channel Spacing  
  
--- A Secondary Channel Offset element indicating SCA or SCB  
  
--- A Wide Bandwidth Channel Switch element indicating 80 MHz, 160 MHz, or 80+80 MHz channel width

11.23.6.3 is limited to 40MHz off-channel link whereas 11.23.6.3 expands it to 80 and 160.

In the Channel Switch Request

Wide Bandwidth Channel Switch

Wide Bandwidth Channel Switch element (optional). The Wide Bandwidth Channel Switch element **is included** when a switch to an 80 MHz, 160 MHz, or 80+80 MHz direct link is indicated.

The Secondary Channel Offset is only included if the switch is to 40MHz, and the Wide Bandwidth Channel Switch only if 80, 160 or 80+80. Hence the “any of the following” is correct.

NEXT THE HT/VHT question

Do we need to state that 11.23.6.3 only applies to non-VHT HT STAs?

It clearly states that the 40MHz support is set in the **HT Capabilities element**, so is that clear enough? I think it is,

Do we need to state that 11.23.6.5 only applies to VHT STAs?

“A wideband off-channel TDLS direct link may be started if both TDLS peer STAs indicated wideband support in the **VHT Capabilities element VHT Capabilities Information field included** in the TDLS Setup Request frame or the TDLS Setup Response frame.”

Is that not clear enough? I think it is.

*Mark - Have you checked with Menzo that this is OK? GS – I sent email, no response yet, but I feel confident on this.*

Proposed Resolution

REVISED

At P1748.18 edit as follows:

“Switching to a 40 MHz off-channel direct link is achieved by including any of the following information in the TDLS Channel Switch Request frame:”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7772  Mark Rison  11.3.5.5  1628.33 | Where is the AP/PCP definition of the reassociation initiation procedures on the current AP (which might as a special case be the same as the new AP), and in particular all the stuff which is deleted or reset (such as BA agreements)? | Add a: p) If  the  ResultCode  in  the  MLME-REASSOCIATE.response  primitive  is  SUCCESS and the CurrentAPAddress parameter in the MLME-REASSOCIATION.indication  primitive  had  the  new  AP's  MAC  address  in  the CurrentAPAddress parameter (reassociation to the same AP), the following states, agreements and allocations shall be deleted or reset to initial values: 1) All EDCAF state 2) Any block ack agreements 3) Sequence number 4) Packet number 5) Duplicate detection caches 6) Anything queued for transmission 7) Fragmentation and reassembly buffers 8) Power management mode 9) WNM sleep mode. The following states, agreements and allocations are not affected by the reassociation procedure: 1) PSMP sessions 2) Enablement/Deenablement 3) GDD enablement 4) STSL, DLS and TDLS agreements 5) SMKSAs, STKSAs and TPKSAs established with any peers 6) MMSLs 7) GCR agreements 8) DMS agreements 9) TFS agreements 10) FMS agreements 11) Triggered autonomous reporting agreements 12) FTM sessions 13) DMG SP and CBAP allocations. |

Discussion:

p) If  the  ResultCode  in  the  MLME-REASSOCIATE.response  primitive  is  SUCCESS and the CurrentAPAddress parameter in the MLME-REASSOCIATION.indication  primitive  had  the  new  AP's  MAC  address  in  the CurrentAPAddress parameter (reassociation to the same AP), the following states, agreements and allocations shall be deleted or reset to initial values:

1) All EDCAF state  
2) Any block ack agreements  
3) Sequence number  
4) Packet number  
5) Duplicate detection caches  
6) Anything queued for transmission  
7) Fragmentation and reassembly buffers  
8) Power management mode  
9) WNM sleep mode.

The following states, agreements and allocations are not affected by the reassociation procedure:

1) PSMP sessions  
2) Enablement/Deenablement  
3) GDD enablement  
4) STSL, DLS and TDLS agreements  
5) SMKSAs, STKSAs and TPKSAs established with any peers  
6) MMSLs  
7) GCR agreements  
8) DMS agreements  
9) TFS agreements  
10) FMS agreements  
11) Triggered autonomous reporting agreements  
12) FTM sessions  
13) DMG SP and CBAP allocations.

Discuss

Proposed Resolution

Inclined to ACCEPT

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7773  Mark Rison  11.16.9  1730.39 | "the STA may transmit a pending 40 MHz mask PPDU only if the secondary channel has also been idle during the times the primary channel CCA is performed (defined in 9.3.7 (DCF timing relations)) during an interval of a PIFS for the 5 GHz band and DIFS for the 2.4 GHz band immediately preceding the expiration of the backoff counter." -- why the difference? | Change to "the STA may transmit a pending 40 MHz mask PPDU only if the secondary channel has also been idle during the times the primary channel CCA is performed (defined in 9.3.7 (DCF timing relations)) during an interval of a PIFS immediately preceding the expiration of the backoff counter." |

Discussion:

**11.16.9 STA CCA sensing in a 20/40 MHz BSS**

This subclause defines CCA sensing rules for an HT STA that is not a VHT STA…

At the specific slot boundaries (defined in 10.3.7 (DCF timing relations)) determined by the STA based on the 20 MHz primary channel CCA, when the transmission begins a TXOP using EDCA (as described in 10.22.2.4 (Obtaining an EDCA TXOP)), *the STA may transmit a pending 40 MHz mask PPDU only if the secondary channel has also been idle during the times the primary channel CCA is performed (defined in 10.3.7 (DCF timing relations)) during an interval of a PIFS for the 5 GHz band and DIFS for the 2.4 GHz band immediately preceding the expiration of the backoff counter*.

Notet that Secondary channel CCA is idle for **PIFS in 5GHz band and DIFS in 2.4GHz band**.

Proposed change is

*the STA may transmit a pending 40 MHz mask PPDU only if the secondary channel has also been idle during the times the primary channel CCA is performed (defined in 10.3.7 (DCF timing relations)) during an interval of a PIFS immediately preceding the expiration of the backoff counter*.

PIFS is SIFS + 1 Slot time

DIFS is SIFS + 2 Slot times

I checked 802.11n D2.0 and the rule was “*PIFS (using short time slot for 5GHz band and long timeslot for 2.4GHz band).”* Hence, clearly the wait on 2.4GHz was meant to be greater than on 5GHz. No mention of what to do if short time slot used.

By 802.11n - 2009 this has become the words as in D5. I can assume that as the short time slot became the norm, this still maintans the longer time on 2.4GHz cf 5GHz.

Hence, to take back to PIFS overall woulod be a major change and would need justification, and could make existing implementations non-compliant.

Proposed Resolution

REJECT

11n specified this in 2009 and clearly wanted a longer idle time in the 2.4GHz band, changing it could make existing implementations non-compliant.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 7786  Mark Rison  11.11.9.1  1689.26 | In a Beacon report, how is the bandwidth indicated?  I don't think it's the Operating Class field, because an OC only gives the maximum BSS bandwidth, not necessarily the actual BSS bandwidth (e.g. you can operate a 20 MHz bandwidth in an OC which specifies a BSS bandwidth of "up to 40 MHz") | Add at the end of the subclause "NOTE---An operating class indicating 40 MHz (or up to 40 MHz) is used to indicate a 40 MHz PPDU only." |

Discussion:

In a Beacon Report the Request lists the Element IDs requested, so the BW could be obtained from the HT and VHT Capabilities. So I suppose the amount of detail that the requestor of the Beacon Report needs can be requested including the BW (or supported MCSs).

Operating Classes specify the Channel Spacing and, true, there are operating classes where the maximum radio BW is specified and the AP can operate in a 20/40 MHZ BSS, for example.

I have no idea as to validity of the proposed change, I feel however, that adding a note is opening a can of worms. Why pull out just the operating class, it is defined ad nauseu in Annex E.

*Mark R - Probably worth getting Brian to look at this*

*GS – Will do*

Brian,

Thanks for reaching out. My technical background – do with it as you please – is as follows.

BW is not directly signaled in the Beacon Report, but BW can be inferred as follows:

Operating class indicates 20 MHz or wider than 20 MHz

To identify the BW of a 40 MHz or wider BSS (or indeed of a 20 MHz BSS), include a Request subelement, listing the element IDs of the HT Operation and VHT Operation elements, within the Beacon Request.

The Beacon Report should then include the sniffed HT Operation and VHT Operation elements, if present, which contain BW-defining fields.

A note to clarify this (whole) mechanism makes sense to me.

Since BW is an important parameter, this mechanism could be optimized to allow the client to report BW only … e.g. allow the BW to be specifically requested (or added by default). E.g. the client could read the HT/VHT Operation elmennts and add a Wide Bandwidth Channel Switch element in the Beacon Report.

Probably too much work for you / 11mc ...?

Proposed Resolution

REVISED

Add at end of subclause 11.11.9.1, P1692.41

“NOTE - To identify the BW of a 20 MHz, 40 MHz or wider BSS, the Beacon Request may include a sub element listing the element IDs of the HT Operation and VHT Operation elements. The Beacon Report should then include the HT Operation and VHT Operation elements, if present, which contain the BW-defining fields.”

*Mark R - ROFL*