IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for some MAC and security comments on 11mc/D3.0 (LB202) |
| Date: 2014-09-16 |
| 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 MAC CIDs 3023, 3313, 3314, 3318, 3323, 3324, 3359, 3360, 3365, 3377, 3382, 3478, 3479 and security CIDs 3426, 3427, 3429, 3432, 3439 on 11mc/D3.0.

r1: Add MAC CID 3020 and PIFS CIDs 3049, 3050, 3051, 3052, 3136, 3137, 3321.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3023Adrian Stephens9.7.12.21291.62 | "NOTE--Support for short GI on transmit cannot be determined." -- I may be one of life's simpler bunny-rabbits, but I fail to understand what this note is telling me. Surely the STA that is transmitting knows what it supports. | Remove NOTE or modify it so that it makes sense to simple bunny-rabbits. |

Discussion:

9.7.12.1 on the Rx Supported VHT-MCS and NSS Set has a NOTE at the end to clarify that even though the text above it only mentions long GI, the rx support for a given combination of VHT-MCS, NSS and bandwidth covers both long and short GI, inasmuch as short GI is supported at that bandwidth (as indicated by the Short GI for $nnn MHz subfields in the (V)HT Capabilities element(s). In other words, the transmitter has all the information needed to determine the exact extent of the receiver’s support.

9.7.12.2 on the Tx Supported VHT-MCS and NSS Set has a corresponding NOTE that in this case there is no signalling as to the short GI support of the transmitter. In other words, a receiver is unable to determine whether a transmitter might use short GI for any particular combination of VHT-MCS, NSS and bandwidth.

What is the Tx Supported VHT-MCS and NSS Set actually used for, though? I had a vague recollection it was used for some control response rules or something, but have been unable to find this by grepping for “supported VHT”.

NOTE—I have been unable to determine for sure whether “bunny rabbit” is a pleonasm, or whether it should have a hyphen, but the answers might be yes and no respectively.

Proposed resolution:

REVISED

Change the NOTE to read “In contrast to reception, s~~S~~upport for short GI ~~on~~ transmi~~t~~ssions by a STA cannot be determined by other STAs.” Give the commenter a carrot.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3313Mark RISON9.3.2.8.11243.64 | "An STBC-capable STA shall choose between control frame operation using either STBC frames or non-STBC frames. [...] This choice is a matter of policy local at the STA." does not appear to be restricted to operation in the context of dual CTS | Add words to constrain this requirement to the context of dual CTS operation |
| CID 3314Mark RISON9.3.61259.43 | "An STBC-capable STA shall discard either all received group addressed Data frames that are STBC frames or all received group addressed Data frames that are non-STBC frames. How it makes this decision is outside the scope of this standard." runs the risk of causing data broadcasts to be lost, since there is no requirement to transmit them once with STBC and once without, except for dual Beacons | Make/move the paragraph to be specific to dual Beacon operation |

Discussion:

STBC is one of life’s great mysteries.

The only rules regarding use of STBC in Control frames appear to be those to do with dual CTS in 9.3.2.8, 9.7.6.3 and 9.7.6.5.3.

The rules regarding use of STBC in group-addressed Data frames are in 10.2.2.

The term “STBC-capable STA” is not defined, and the natural interpretation of “has STBC implemented” means any rules using this term apply even if STBC is not actually enabled. “$foo STA” is the more usual term for a STA which has $foo both implemented and enabled (there are moves afoot in the ARC SC, at TGmc’s behest, to canonicalise this).

The term “control frame operation” is vague too – does it mean everything including non-response control frames? If so, how is the alleged freedom to choose between STBC and non-STBC compatible with 9.7.6.5.3’s apparently definitive “If the frame eliciting the response was an STBC frame and the Dual CTS Protection bit is equal to 1, the CandidateMCSSet shall contain only the basic STBC MCS.”?

Fortunately dual Beacon and dual CTS are both deprecated, so we don’t need to lose too much sleep over them.

Oh, and “policy local at the STA” is a singleton, and “local policy” only appears in the context of BSS Available Admission Capability, SSPN and SAE groups. “outside the scope of this standard” is the canonical form.

Proposed changes:

Change 1243.64 as follows:

An STBC~~-capable~~ STA operating in a BSS which uses dual CTS protection shall ~~choose between control frame operation using either STBC frames or non-STBC frames. In the non-STBC frame case, it~~ discard~~s~~ either all Control frames from the BSS that are STBC frames ~~it receives. In the STBC frame case, it discards~~ or all Control frames from the BSS that are non-STBC frames ~~received from its own BSS~~. ~~This choice is a matter of policy local at the STA.~~ How it makes this decision is outside the scope of this standard. I still don’t really get this. If e.g. it chooses to discard STBC Control frames, and the peer Acks using STBC frames per 9.7.6.5.3, then what?

Change 1259.43 as follows:

An STBC~~-capable~~ STA operating in a BSS which uses dual Beacons shall discard either all ~~received~~ group addressed Data frames from the BSS that are STBC frames or all ~~received~~ group addressed Data frames from the BSS that are non-STBC frames. How it makes this decision is outside the scope of this standard.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3313 and 3314, which effect the change proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3318Mark RISON9.7.6.5.51284.29 | "A STA shall not transmit a control response frame with TXVECTOR parameter FEC\_CODING set to LDPC\_CODING unless it is in response to a reception of a frame with the RXVECTOR parameter FEC\_CODING equal to LDPC\_CODING." does not require an LDPC control response to an LDPC frame. How then is the transmitter of the original LDPC frame supposed to determine the correct Duration value? Ditto other options which affect the TXTIME of a frame, e.g. STBC, SGI, etc. | Not sure how to fix this without affecting existing implementations! |

Discussion:

As the commenter suggests, it is not always possible to determine the duration of the TXOP responder’s frames. However, the horse has already bolted, the milk has already been spilt, the chickens have hatched, etc.

Proposed resolution:

REVISED

Add the following after the first paragraph of 8.2.5.2:

NOTE 1—Estimated times might prove to be inexact, if the TXOP responder has a choice of PHY options (e.g. BCC v. LDPC, use of STBC, use of short GI, PHY header/preamble format options) or MAC options (e.g. use of HT Control)). Heuristics such as the TXOP responder’s previous choices and channel conditions might be used to minimise the inexactitude.

Number the existing NOTE as NOTE 2.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3321Mark RISONB.4.17.12733.46 | What does HTM17.1 mean when it says AP support for SMPS is mandatory? The implication of HTM17.3 and HTM17.4 is that this actually just means advertising the current state in the HT Capabilties | Clarify. See other comment on whether the thing being advertised is a capability or a state |
| CID 3323Mark RISON10.2.51561.6 | It's not clear whether the SM Power Save subfield of the HT Capabilities Info is a capability or a current state, nor whether it's support on tx or rx. 10.2.4 suggests that at least for non-AP STAs it's actually a current state and for rx, but the situation is not clear for APs (especially since the PICS suggests something is mandatory for APs but not mandatory for non-AP STAs) | Clarify. Note that the current situation appears to be that for non-AP STAs it's a state not a capability, which is contrary to the agreed intent of the HT Capabilties IE (and more generally with the principle that capabilities are fixed, and things which change are in other elements, called e.g. operation) |

Discussion:

The general rule is that the stuff in HT Capabilities Info is static. However, it seems the SM Power Save aspect of this is in fact dynamic. This can’t be changed due to existing implementations, but at least needs to be made clear. It should also be made clear that this subfield is only for use by non-AP STAs (cf. 1561.42).

There is also suggestion that SM can be enabled “during” association. This is vague, and makes little sense since the AP only finds out the STA’s SMPS mode after association. Or is the intent to apply the SMPS mode to the (Re)Association Response? Is this really worth it, given that the Authentication would not have benefited from this (assuming the AP had determined the STA supported 2SS, from e.g. a Probe Request)? Also 1561.45 only mentions “after association”.

It is true that non-AP STA support for SMPS is optional in the PICS. It is not entirely clear whether this means a non-AP STA being able to operate in SMPS mode or a non-AP STA being able to operate with an AP in SMPS mode. Arguably there is not so much benefit for APs being able to be in SMPS mode, so probably the answer is that only non-AP STAs can go into SMPS and APs are required to support this.

However the reference at 1561.48 to DLS spoils this a bit – how is a STA supposed to know whether another non-AP STA supports sending under SMPS constraints? Well, it just doesn’t work.

Oh, and a STA in SMPS mode might have decided to constrain rx to 1SS for other reasons, e.g. operating mode (not useful per se, but might help reduce signalling overheads). Ah, and MCSes do not encode NSS, for VHT.

Usual editorial pedantry, too.

Proposed changes:

Delete “during and” at 871.24.

At the bottom of the right-most cell at 871.26 add:

Reserved for an AP STA. Hm, or might existing AP STAs be using 3 = disabled, rather than 0 = static SMPS?

NOTE—This subfield indicates an operational state, as well as (if not set to 3) a capability.

Change 871.23 as follows: “Set to 3 for SM ~~P~~power ~~S~~save disabled or not supported”.

Change 3007.33 as follows: “equal to 3 for SM power save disabled or not supported”.

Change “STA” to “non-AP VHT STA” at 1561.10.

Change 1561.21 as follows: “The receiver shall, subject to its spatial stream capabilities (see 8.4.2.55.4 and 8.4.2.157.3) and operating mode (see 10.42), be capable of receiving a PPDU that is sent using ~~an MCS that indicates~~ more than one spatial stream a SIFS after the end of its response frame transmission.”

Change “a STA” to “the STA” at 1561.18.

Change “An HT STA” to “The STA” at 1561.41.

Change “A non-AP HT STA” to “The STA” at 1561.41.

Change 1561.48 as follows: “A STA that has one or more DLS links shall ~~notify all STAs with which it has a DLS link of any change in SM power save mode before operating in that mode~~ not operate in SM power save mode.” Should we allow a let-out for the case where all these DLS peers would only use 1SS anyway (e.g. through use of OMN or because of their tx capability), i.e. only the AP might use >1SS to the STA?

Change 1828.15 as follows: “NOTE 2—An AP cannot change the maximum number of spatial streams it is able to receive from ~~—Using the SM power save mechanism defined in 10.2.5 (SM power save) for~~ HT STAs that are not operating mode notification capable”.

Delete NOTE 2 at 1828.22 (“NOTE 2—An AP that is reducing the maximum number of spatial streams the AP is able to receive and that has associated HT STAs that are not operating mode notification capable would use the SM power save mechanism to notify the STAs that the AP is operating with a single receive chain.”).

Change “the receiver” to “the STA” at 1561.21, 1561.24, 1561.31.

Change 1561.39 as follows: “~~A STA i~~In static SM power save mode, the STA maintains only a single receive chain active.” (for consistency).

Change “Association” to “(Re)Association” at 1561.43.

Change “association” to “(re)association” at 1561.45.

Change “SM Power Save” to “SM power save” at 1561.9.

Change “SM Power Save bits” to “the SM Power Save subfield” at 1561.43.

Change “SM Power Save Mode” to “SM power save mode” at 1561.51, 1561.54.

Change 2733.46 as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \*HTM17.1 | AP support for non-AP STA dynamic and static SM power save mode | 10.2.5 (SM power save) | (CF16 AND CF1):M(CF30 AND CF1):M | Yes  No  N/A  |
| \*HTM17.2 | STA support for local dynamic and static SM power save mode | 10.2.5 (SM power save) | (CF16 AND CF2):O(CF30 AND CF2):O | Yes  No  N/A  |
| HTM17.3 | Transmit SM Power Save state information using HT ~~c~~Capabilities element, or SM Power Save frame | 8.6.12.3 (SMPower Saveframe format),10.2.5 (SMpower save) | ~~(HTM17.1 OR~~HTM17.2~~)~~:M | Yes  No  N/A  |
| HTM17.4 | Receive SM Power Save state information and support frame exchanges with STAs in SM Power Save mode~~STAs~~ | 10.2.5 (SMpower save) | ~~CF16:M~~~~CF30:M~~HTM17.1:M | Yes  No  N/A  |

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CIDs 3321 and 3323, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3324Mark RISON10.2.51561.6 | How do OMN and SMPS interact? If SMPS is active but OMN says 2SS, can 2SS be used for the first transmission in a TXOP? For subsequent ones, if the SMPS is dynamic? | Maybe the answer is that the OMN gives the post-initial maximum for dynamic SMPS, and is ignored for static SMPS? If so, say so |

Discussion:

The interpretation suggested by the commenter in the proposed change seems plausible. It would make little sense for OMN to override SMPS, since the whole point of SMPS is to allow quiescent operation with fewer SSes. A NOTE is probably sufficient.

Proposed resolution:

REVISED

Add the following at 1829.25: “NOTE 3—The number of spatial streams might be further restricted if the receiving STA is in SM power save mode (see 10.2.5).” Increment the number of the two following NOTEs.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3359Mark RISON | The OperationalRateSet is a set of integers in the range 0-127 representing pre-11n datarates (as rate / 500 kbps) and hence does not contain anything to do with MCSes | Make sure that all references to "operational rate" or "OperationalRate" do not involve MCSes |
| CID 3360Mark RISON | Fix OperationalRateSet to be the set of rates which the STA can receive at, and nothing more (specifically not anything about the maximum rate for transmit, for example -- see e.g. 1276.41, 1287.41, 2637.65) | As it says |
| CID 3377Mark RISON | "OperationalRateSet, which is a parameter of the MLME-JOIN.request primitive" -- also the START | Add "and MLME-START.request primitive" |
| CID 3020Adrian Stephens9.7.5.31274.61 | Why are only 2 of 3 of these rate/mcs things "parameters" in this para? | Unify terminology here. |

Discussion:

There are three separate operational sets: the operational rate set, used for pre-11n PPDUs and for 11ad PPDUs, the operational MCS set, used for 11n PPDUs, and the operational VHT-MCS and NSS set, used for 11ac PPDUs. The first is expressed in terms of the PHY datarate, in units of 500 kbps (for pre-11n PPDUs) or the MCS (for 11ad), the last is expressed in terms of the combination of the (VHT) MCS and the NSS, and the second is expressed in terms of the (HT) MCS, which despite its name encodes the NSS too. Note that the operational sets are entirely about the receive capabilities of the STA advertising them, not its transmit capabilities.

There are three analogous basic sets. The difference between the two sets of sets is that the operational sets indicate the PPDU formats a given STA is able to receive, while the basic sets indicate the PPDU formats all STAs in the BSS are required to both be able to receive and transmit. The point is that if a STA knows that another STA is able to receive a given PPDU format, even though not all STAs in the BSS might be able to, it could still in some situations use it (and thereby achieve better performance). The basic sets are specified by the STA which starts the BSS; the operational sets are specified by all STAs (either when the BSS is started or when it is joined).

(For 11ad it seems the usage is different: the operational rate set is essentially the basic rate set (which is not used) and all devices need to be able to both tx and rx at the MCSes in the set (plus 0). Don’t ask me why they didn’t use the basic rate set like everyone else. I fear that this breaks all the other bits of the spec which talk about the basic rate set, but I currently propose to close my eyes and put my fingers in my ears.)

At 1274.61 everything ends up in a parameter. The BSSBasicRateSet is a parameter, and the Basic MCS Set field is in the HT Operation parameter or in the (HT Operation row of the) SelectedBSS parameter (linebreaks inserted in a desperate attempt at increased clarity):

If the BSSBasicRateSet **parameter** is empty and

the Basic MCS Set field of the HT Operation **parameter** of the MLME-START.request primitive or Basic MCS Set field of the HT Operation row of the SelectedBSS **parameter** of the MLME-JOIN.request primitive

is not empty, the frame shall be transmitted in an HT PPDU using one of the MCSs included in

the Basic MCS Set field of the HT Operation **parameter** of the MLME-START.request primitive or Basic MCS Set field of the HT Operation row of the SelectedBSS **parameter** of the MLME-JOIN.request primitive.

A set of editorial issues was identified along the way, as usual.

Proposed changes:

Change the fourth (penultimate) cell at 148.54 as follows: “Non-DMG BSS: The set of data rates that the peer STA is able to use~~s~~ for communication within the BSS. The peer STA is able to receive at each of the data rates listed in the set. This set is a superset of the rates contained in the BSSBasicRateSet parameter.

DMG BSS: The set of MCS indexes that the peer STA uses for communication within the BSS.”

Change the fourth (penultimate) cell at 148.51 as follows: “Non-DMG BSS: The set of data rates that all STAs in the BSS are able to use for communication. ~~shall be supported by a~~All STAs ~~that join~~in the BSS are able to receive and transmit at each of the data rates listed in the set.

DMG BSS: Empty.”

Change the fourth (last) cell at 157.55 as follows: “Non-DMG BSS: The set of data rates that the STA is able to use~~s~~ for communication within the BSS. The STA ~~shall be~~is able to receive at each of the data rates listed in the set. This set is a superset of the rates contained in the BSSBasicRateSet parameter.

DMG BSS: The set of MCS indexes that the STA uses for communication within the BSS.”

Change 158.63 as follows: “If the MLME of a VHT STA receives an MLME-JOIN.request primitive with a SelectedBSS parameter containing ~~a BSSDescription with~~ a Basic VHT-MCS and NSS Set field in the VHT Operation ~~element~~ parameter”.

Add at 159.3: “If the MLME of a DMG STA receives an MLME-JOIN.request primitive with the SelectedBSS parameter containing a BSSBasicRateSet parameter that is not empty, or with the OperationalRateSet parameter containing any unsupported MCSs, the MLME response in the resulting MLME-JOIN.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.”

Change “BSSBasicRateSet element” to “BSSBasicRateSet parameter” at 158.52.

Change “elements” to “parameters” at 147.47 and 155.24.

Change “element” to “parameter” at 1826.28.

Change “HT Operation row of the SelectedBSS parameter” to “HT Operation parameter of the SelectedBSS parameter” throughout the document; there are 17 instances.

Change the fourth (last) cell at 200.12 as follows: “Non-DMG BSS: The set of data rates that the STA is able to use~~s~~ for communication within the BSS. The STA ~~shall be~~is able to receive at each of the data rates listed in the set. This set is a superset of the rates contained in the BSSBasicRateSet parameter.

DMG BSS: The set of MCS indexes that the STA uses for communication within the BSS.”

Change the fourth (last) cell at 200.7 as follows: “Non-DMG BSS: The set of data rates that all STAs in the BSS are able to use for communication. ~~shall be supported by a~~All STAs ~~to join this~~in the BSS~~. T~~, including the STA that is creating the BSS, ~~shall be~~are able to receive and transmit at each of the data rates listed in the set.

DMG BSS: Empty.”

Add at 203.24: “If the MLME of a DMG STA receives an MLME-START.request primitive with a BSSBasicRateSet parameter containing any rates, or with the OperationalRateSet parameter containing any unsupported MCSs, the MLME response in the resulting MLME-START.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.”

Change 1232.29 as follows:

All non-DMG STAs that are members of a BSS are able to receive and transmit at all of the data rates in the BSSBasicRateSet parameter of the MLME-START.request primitive or BSSBasicRateSet parameter of ~~the BSSDescription representing~~ the SelectedBSS parameter of the MLME-JOIN.request primitive; see 6.3.4.2.4 (Effect of receipt) and 6.3.11.2.4 (Effect of receipt). All HT STAs ~~and DMG STAs~~ that are members of a BSS are able to receive and transmit using all of the MCSs in the Basic MCS Set field of the HT Operation parameter of the MLME-START.request primitive or Basic MCS Set field of the HT Operation parameter of ~~the BSSDescription representing~~ the SelectedBSS parameter of the MLME-JOIN.request primitive; see 6.3.4.2.4 (Effect of receipt) and 6.3.11.2.4 (Effect of receipt). All VHT STAs that are members of a BSS are able to receive and transmit using all the <VHT-MCS, NSS> tuples in the BSS basic VHT-MCS and NSS set (see 10.40.7 (BSS basic VHT-MCS and NSS set operation)) except as constrained by the rules of 9.7.12 (Rate selection constraints for VHT STAs). All DMG STAs that are members of a BSS are able to receive and transmit using all of the MCSs in the OperationalRateSet parameter of the MLME-START.request primitive or OperationalRateSet parameter of the SelectedBSS parameter of the MLME-JOIN.request primitive; see 6.3.4.2.4 (Effect of receipt) and 6.3.11.2.4 (Effect of receipt). To support the proper operation of the RTS/CTS by non-DMG STAs, RTS/DMG CTS by DMG STAs, and the virtual CS mechanism, a non-DMG STA shall be able to interpret Control frames with the Subtype field equal to RTS or CTS, and a DMG STA shall be able to interpret Control frames with the Subtype field equal to RTS or DMG CTS.

Change “BSSDescription parameter” to “SelectedBSS parameter” at 1529.5.

Change “BSSDescription” to “SelectedBSS parameter” at 1529.23.

Change “BSSDescription” to “BSSDescriptionSet” at 2059.18, 2138.11 and 2138.16.

Delete the bullet at 1276.40: “— A STA that transmits a frame at a rate not specified by an MCS or a <VHT-MCS, NSS> tuple shall not transmit the frame at a data rate higher than the greatest rate in the OperationalRateSet parameter of the MLME-JOIN.request primitive.” (covered by 1275.53).

Change 1287.34 as follows (deleted material covered by non-deleted material):

An individually addressed Data or Management frame shall be sent using an~~y~~ MCS ~~subject to the following constraints:~~

~~— A STA shall not transmit a frame using an MCS that is not~~ supported by the receiver STA, as reported in the maximum receive MCS subfields in the Supported MCS Set field in Management frames transmitted by the receiver STA.

~~— A STA shall not transmit a frame at an MCS index higher than the highest Transmission MCS in the OperationalRateSet, which is a parameter of the MLME-JOIN.request primitive.~~

Change 1589.32 as follows:

The value of the Minimum PHY Rate in a TSPEC shall satisfy the following constraints:

— it is in the AP’s operational rate set, or corresponds to an HT MCS in the AP’s operational HT MCS set or to a VHT-MCS and NSS in the AP’s operational VHT-MCS and NSS set, for an uplink TS.

— it is in the non-AP STA’s operational rate set, or corresponds to an HT MCS in the non-AP STA’s operational HT MCS set or to a VHT-MCS and NSS in the non-AP STA’s operational VHT-MCS and NSS set, for a downlink TS.

— it is in both the AP’s operational rate set and non-AP STA’s operational rate set, or corresponds to an HT MCS in both the AP’s and the non-AP STA’s operational HT MCS set or to a VHT-MCS and NSS in both the AP’s and the non-AP STA’s operational VHT-MCS and NSS set, for a bidirectional TS.

Set the second cell at 2637.63 to “*Reserved*” and the third, fourth and fifth cells blank.

Change 2823.19 as follows: “This attribute specifies the set of non-HT data rates at which the station ~~may transmit~~is able to receive data.” Do we want to extend this for DMG?

Change “2-127” to “1-127” at 171.26, 175.18, 185.30, 188.50 (for consistency).

Change the underscores to hyphens at 719.43 (twice).

Change “BSSBasicMCSSet” to “BSS basic HT MCS set” at 1274.20.

Change 1278.40 to delete the space/linebreak in “BSS BasicRateSet”.

Change “SupportedVHTMCS\_NSSSet” to “operationalVHT-MCS and NSS set” at 1278.57

Change “BSSBasicVHTMCS\_NSSSet” to “BSS basic VHT-MCS and NSS set” at 1829.48. Delete the definition at 25.20.

Change “OperationalVHTMCS\_NSSSet” to “operationalVHT-MCS and NSS set” at 1829.49.

Proposed resolution for CIDs 3359 and 3377:

REVISED

The resolution for CID 3360 deletes the text which links the operational rate set with MCSs and which omits the MLME-START.request primitive (1287.41).

Proposed resolution for CID 3360:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3360, which address the issue raised by the commenter.

Proposed resolution for CID 3020:

REJECTED

Everything ends up in a parameter. The BSSBasicRateSet is a parameter, and the Basic MCS Set field is in the HT Operation parameter or in the (HT Operation row of the) SelectedBSS parameter

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3365Mark RISON8.6.2.3.11078.7 | There appears to be nothing to ensure that the UPs in multiple TCLAS elements in ADDTS Request (and any other frame which can carry multiple TCLAS elements) specify the same UP | Add something to that effect somewhere |

Discussion:

As stated in 8.4.2.32, the TCLAS Processing element is present in the ADDTS Request, ADDTS Response, FMS Request, DMS Request, and TFS Request MMPDUs if there are multiple TCLAS elements associated with the request. It indicates how a PDU or MSDU should be processed by the classifier.

(Well, except that the element is also present in some other MMPDUs. And it’s only part of indicating how the PDU/MSDU is processed; TCLAS elements are needed too. And it may be present if there are no TCLAS elements (specifically for the type 2 “do not belong to any other TS” specifiers), but only for ADDTS, not FMS/DMS/TFS/SCS, right?.)

However, the commenter is a nitwit: the UP is in the TSPEC element, not the TCLAS element(s). So multiple TCLAS elements don’t result in multiple UPs. So all we are left with is editorials spotted in the course of investigating this comments.

Proposed changes:

Change the first para of 8.4.2.32 as follows:

The TCLAS Processing element is present in ~~the~~ ADDTS Request, ADDTS Response, FMS Request, FMS Response, DMS Request, DMS Response, ~~and~~ TFS Request and SCS Descriptor frames if there are multiple TCLAS elements associated with the request, response or descriptor. It may also be present in the ADDTS Request and ADDTS Response frames if there are no TCLAS elements. Together with the TCLAS element(s), if present, i~~I~~t indicates how a PDU or MSDU should be processed by the classifier.

Also make the following changes:

* “TCLASs” to “TCLAS elements” at 1598.49 and 1598.52.
* “TCLAS processing” to “TCLAS Processing” at 1077.37, 1552.16, 1593.37, 1593.40, 1593.47, 1593.49, 1593.53, 1595.2, 1736.16, 1736.24.
* “there ~~are~~are no~~t any~~ associated TCLAS elements” at 842.51.
* “The TCLAS Processing Element field is present when more than one TCLAS element~~s are~~ is present in the TCLAS Elements field and contains a TCLAS Processing element which defines how the multiple” at 986.20.
* “The TCLAS Processing element is present when there ~~are~~is more than one TCLAS element” at 1078.6.

Proposed resolution:

REVISED

The commenter is a nitwit: the UPs are in the TSPEC element, not the TCLAS element(s). So multiple TCLAS elements don’t result in multiple UPs. However, some editorials were spotted in the course of investigating this comment. Make the changes described in $thisdoc under “Proposed changes:” for CID 3365.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3382Mark RISONC.32814.53 | dot11EDCATableTXOPLimit is not defined for Clause 20; dot11QAPEDCATableTXOPLimit is not defined for Clauses 20 or 21 | Add references to these clauses to the description |

Discussion:

The default TXOP Limits for non-AP non-OCB STAs are given in Tables 8-144 (826.18). The defaults for OCB STAs are given in table 8-145 (827.1). No defaults are given for AP STAs.

The defaults given in the description of dot11QAPEDCATableTXOPLimit and dot11EDCATableTXOPLimit in the MIB should be aligned with these (it’s worse than the commenter suggested: many other PHYs are missed). Note that 1226.8 makes it clear that dot11EDCATableTXOPLimit is not used OCB. Also note that Table 8-144 says DMG has zero TXOP Limits, but dot11EDCATableTXOPLimit doesn’t; assuming the former is right.

The defaults given in the description of dot11QAPEDCATableTXOPLimit appear to come from 802.11-2012, before they were changed for non-AP non-OCB STAs; it seems reasonable to take them as being the same as for non-AP non-OCB STAs

There are various editorial inconsistencies. The rules are, or appear to be, or should be:

* The (sub)field should be uppercased, i.e. “TXOP Limit”
* The general concept should be lowercased, i.e. “TXOP limit”

Futhermore:

* EDCA Parameter Sets can also appear in Probe and Association Responses
* There is an explicit reference to the transmission order of a multi-octet field, which (a) is confusing (is it not the usual 802.11 order?) and (b) I thought we’d deleted a while ago
* There is also rather loose wording for TXOP Limit 0 in QoS (+)CF-Polls
* There is a bogus spelling: “dot11EDCAQAPTableTXOPLimit” (should be QAPEDCA)
* The units are only given in the textual description
* A “QAP” has made it into the description of the non-QAP MIB variable/attribute
* There is a reference to a mysterious “OFDM/CCK-OFDM PHY”
* Many references to 9.22.2.2 (EDCA backoff procedure) should be to 9.22.2.8 (TXOP limits)
* “nonzero” is to be preferred over “non-zero” (IEEE is hyphen-phobic, sorry, hyphenphobic)

Proposed changes:

Change 3145.11 as follows (note deletion of “QAP”):

dot11EDCATableTXOPLimit OBJECT-TYPE

SYNTAX Unsigned32 (0..65535)

UNITS "microseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC upon receiving an EDCA Parameter Set ~~in a Beacon~~

~~frame~~.

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum number of microseconds of an EDCA

TXOP for a given AC, for a non-AP non-OCB STA. The default value for this attribute is

 \ dot11EDCATableIndex 1 2 3 4

PHY Clause

16 (DSSS), 17 (HR/DSSS) 3264 3264 6016 3264

18 (OFDM), 19 (ERP), 20 (HT), 22 (VHT) 2080 2080 4096 2080

23 (TVHT) with BCU 6 or 7 MHz 0 0 22560 11280

23 (TVHT) with BCU 8 MHz 0 0 16920 8460

other, including 21 (DMG) 0 0 0 0"

~~1) 2080 microseconds for Clause 18 (Orthogonal frequency division multi-plexing (OFDM) PHY specification) and Clause 19 (Extended Rate PHY (ERP)~~

~~specification) PHY and 3264 for Clause 17 (High rate direct sequence~~

~~spread spectrum (HR/DSSS) PHY specification) PHY, if~~

~~dot11QAPEDCATableIndex is 1 or 2,~~

~~2) 4096 microseconds for Clause 18 (Orthogonal frequency division multi-plexing (OFDM) PHY specification), Clause 19 (Extended Rate PHY (ERP)~~

~~specification), and Clause 21 (Directional multi-gigabit (DMG) PHY speci-fication) PHY; and 6016 microseconds for Clause 17 (High rate direct~~

~~sequence spread spectrum (HR/DSSS) PHY specification) PHY, if~~

~~dot11EDCATableIndex is 3,~~

~~3) 2080 microseconds for Clause 18 (Orthogonal frequency division multi-plexing (OFDM) PHY specification), Clause 19 (Extended Rate PHY (ERP)~~

~~specification)), and Clause 21 (Directional multi-gigabit (DMG) PHY spec-ification) PHY; and 3264 microseconds for Clause 17 (High rate direct~~

~~sequence spread spectrum (HR/DSSS) PHY specification) PHY, if~~

~~dot11EDCATableIndex is 4."~~

::= { dot11EDCAEntry 5 }

Change 3147.59 as follows:

dot11QAPEDCATableTXOPLimit OBJECT-TYPE

SYNTAX Unsigned32 (0..65535)

UNITS "microseconds"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum number of microseconds of an EDCA

TXOP for a given AC ~~at the~~, for an AP. The default value for this attribute is

 \ dot11EDCATableIndex 1 2 3 4

PHY Clause

16 (DSSS), 17 (HR/DSSS) 3264 3264 6016 3264

18 (OFDM), 19 (ERP), 20 (HT), 22 (VHT) 2080 2080 4096 2080

23 (TVHT) with BCU 6 or 7 MHz 0 0 22560 11280

23 (TVHT) with BCU 8 MHz 0 0 16920 8460

other, including 21 (DMG) 0 0 0 0"

~~1) 0 for all PHYs, if dot11QAPEDCATableIndex is 1 or 2; this implies that~~

~~the sender can send one MSDU in an EDCA TXOP,~~

~~2) 3008 microseconds for Clause 18 (Orthogonal frequency division multi-plexing (OFDM) PHY specification) and Clause 19 (Extended Rate PHY (ERP)~~

~~specification) PHY and 6016 microseconds for Clause 17 (High rate direct~~

~~sequence spread spectrum (HR/DSSS) PHY specification) PHY, if~~

~~dot11QAPEDCATableIndex is 3,~~

~~3) 1504 microseconds for Clause 18 (Orthogonal frequency division multi-plexing (OFDM) PHY specification) and Clause 19 (Extended Rate PHY (ERP)~~

~~specification) PHY and 3264 microseconds for Clause 17 (High rate direct~~

~~sequence spread spectrum (HR/DSSS) PHY specification) PHY, if~~

~~dot11QAPEDCATableIndex is 4."~~

::= { dot11QAPEDCAEntry 5 }

Also:

* change “dot11EDCAQAPTableTXOPLimit” to “dot11QAPEDCATableTXOPLimit” at 580.59
* change “TXOPlimit value” to “TXOP limit” at 1342.43
* change “TXOP Limit” to “TXOP limit” at 827.4, 1315.36, 1316.17, 1316.42, 1316.44, 1316.59, 1324.25, 2144.4, 3492.56
* change “TXOP limit duration values” to “TXOP limits” at 1315.45
* change “TXOP limit value” to “TXOP Limit subfield value” at 564.1 (twice)
* change “TXOP limit value of 0” to “TXOP limit of 0” at 580.46, 1315.48
* change “TXOP limit values” to “TXOP limits” at 1226.8
* change “TXOP Limit value 0” to “a TXOP limit of 0” at 1226.41
* change “TXOP limit is greater than 0” to “TXOP limit is nonzero” at 1322.47
* change “9.22.2.2” to “9.22.2.8” at 580.45, 826.11, 1226.42, 1298.44, 1314.23, 1320.10
* delete “with the least significant octet transmitted first,” at 826.9
* change 564.2 as follows: “0 ~~implies~~ indicates that only one MPDU or one QoS Null frame is to be transmitted immediately following the QoS (+)CF-Poll frame.”
* delete “OFDM/CCK-OFDM PHY” at 827.5
* change “non-zero” to “nonzero” at 1315.42, 3492.56, 1161.48, 2442.17

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3382, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3432Mark RISON11.6.1.71935.46 | Why do some things get to be securely destroyed, and others not? Specifically "securely delete all unused bits" and "securely destroys the remainder". And what's the difference between deleting and destroying anyway? | Delete this text, or put it in other places too |
| CID 3426Mark RISON | "HMAC-SHA-256" (6 instances) is confusing as 256 is not the output length | "HMAC-SHA256" |
| CID 3427Mark RISON11.6.1.31932.36 | "HMAC-SHA1-128" | "Truncate128(HMAC-SHA1-160" for consistency with other PMKIDs. Also at 1935.35 |
| CID 3429Mark RISON | Is it SHA256 or is it SHA-256? Ditto SHA(‑)384 | Pick one (or two, if the answers for the hash name on its own and when combined to form a HMAC (e.g. HMAC-SHA256) are different, to avoid confusion between the hash name and the output length) |

Discussion:

There is no definition of the terms “destroy” (as distinct from “delete”) or “securely”. The term “delete” can be used throughout instead of “destroy”, and the adverb “irretrievably”, already used in one place, can be used throughout instead of “securely”.

Furthermore, there is no consistency as to the things which need to be deleted/destroyed securely, though the intent seems to be that HMAC-*hash*-*len* does not irretrievably delete the unused bits while Truncate‑128 does. Finally there are requirements which inappropriately constrain implementations (e.g. talk of “memory pool”s).

Regarding terminology, it seems the hashes themselves are SHA-1, SHA-256 and SHA-384. However, the HMACs which use the latter two should be (and generally are) HMAC-SHA*n*[-*len*] to avoid confusion with the truncated HMACs. It seems OK, though, to keep HMAC-SHA-1 since it seems harder to think the 1 might be a truncation length, and this aligns with the referenced RFC 2202 at 2619.48.

Proposed changes:

Change “destroy” to “delete” at 102.55, 102.56, 103.7, 103.13, 238.62, 1671.12, 1695.5, 1695.40, 1862.12, 1863.33, 1867.52, 1870.5, 1870.14, 1870.20, 1870.25, 1911.1, 1922.49, 1922.50, 1938.43, 2010.18, 2062.45.

Change “destruction” to “deletion” at 1173.24.

Add at 959.5: “HMAC-SHA1-64 is the first 64 bits of the HMAC-SHA-1 of its argument list.”

Change 1767.6 as follows: “shall be computed using the HMAC-SHA1-64 hash algorithm”.

Change 1867.53 as follows: “Protocol instances that transition into *Nothing* state ~~will~~ shall immediately be ~~destroyed with their state zeroed and returned to the memory pool~~ irretrievably deleted.”

Change 1870.5 as follows: “The parent process ~~also destroys~~ shall delete protocol instances ~~by zeroing out the state of the protocol instance and returning it to the memory pool~~ irretrievably.”

Change 1932.36 as follows: “PMKID = Truncate-128(HMAC-SHA-1~~-128~~(PMK, "PMK Name" || AA || SPA))

~~Here, HMAC-SHA1-128 is the first 128 bits of the HMAC-SHA1 of its argument list.~~”

Change 1932.58 as follows: “NOTE 5—When the PMKID is calculated for the PMKSA as part of RSN preauthentication, the AKM has not yet been negotiated. In this case, the HMAC-SHA-1-~~128~~ based derivation is used for the PMKID calculation.” Shouldn’t this be normative (probably with the deletion of the term “RSN”, since “RSN preauthentication” appears nowhere else)?

Change 1935.34 as follows: “SMKID = Truncate-128(HMAC-SHA-1~~-128~~(SMK, "SMK Name" || PNonce || MAC\_P || INonce || MAC\_I))

~~Here, HMAC-SHA1-128 is the first 128 bits of the HMAC-SHA1 of its argument list.~~”

Delete the line at 1938.43 (“— Truncate-128(-) returns the first 128 bits of its argument and securely destroys the remainder.”).

Insert at 1929.5 the following line: “— Truncate-128(*Str*) From *Str* starting from the left, extract bits 0 to 127, using the IEEE Std 802.11 bit conventions from 8.2.2 (Conventions). Irretrievably discard bits 128 onwards.” Also move the tab stop for this list to the right so that you don’t get “)From” at 1928.3. Or would “delete” be preferred over “discard”?

Change “HMAC-SHA-256” to “HMAC-SHA256” at 1932.40, 1932.44, 1932.46, 1932.50, 1935.39, 1935.43.

Change “HMAC-SHA-384” to “HMAC-SHA384” at 1932.52, 1932.56.

Change “HMAC-SHA1” to “HMAC-SHA-1” at 1941.63. Do the msbs need to be irretrievably deleted here? What about at 1896.4 (BIP-CMAC)? And 959.5 (Emergency Alert Identifier Hash)?

Delete the extra space at 1952.24.

Change “SHA256” to “SHA-256” at 812.55 (twice), 812.58, 812.61, 813.20, 813.36.

Change “SHA1” to “SHA-1” at 1941.62.

Change “from the keyseed” to “from *keyseed*” at 2009.50 and change “Keyseed” to “*keyseed*” at 2010.18.

Proposed resolution for CIDs 3432 and 3429:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3432 and 3429.

Proposed resolution for CID 3426:

ACCEPTED

Note to the editor: the 6 instances are 1932.40, 1932.44, 1932.46, 1932.50, 1935.39, 1935.43. The resolution to CID 3429 addresses the two instances of “HMAC-SHA-384” at 1932.52, 1932.56.

Proposed resolution for CID 3427:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3427, which effect the change proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3439Mark RISON11.6.1.7.21937.23 | It is not specified how to convert from a character string to a bit string (8.2.2 says nothing about this) | Specify (a) the encoding (ASCII?) and (b) whether the string is to be considered to have a terminating NUL (the answer to this is probably no, given things like ""FT-R0" is 0x46 0x54 0x2D 0x52 0x30.") In turn, things like that quoted in the previous parenthesis can be deleted |

Discussion:

Various cryptographic functions (KDFs, PRFs, HMACs and hashes) are passed strings, but nowhere except for FT-related ones is the encoding of these string specified. Most importantly, it is not specified whether these strings are to be considered to have a terminating NUL (as in C). Less importantly, the encoding is not specified, so in theory it could be EBCDIC or even [the ZX81 character set](http://www.soxlamps.com/zx81_files/ZX81_charset.gif) (well, except when the label has lowercase characters, since these were not available on the ZX81 (though they did appear on the Spectrum (but I was an Amstrad CPC man))).

The encodings are not specified for the following; it is reasonable to assume (based on the encodings provided in FT-related cases) that they are intended to be ASCII without a terminator:

1. PRF-something

1931.62: PTK ← PRF-X(PMK, “Pairwise key expansion”

1933.54: GTK ← PRF-X(GMK, “Group key expansion”

1934.62: STK ← PRF-X(SMK, "Peer key expansion"

2. KDF-something

1858.48: pwd-value = KDF-z(pwd-seed, “SAE Hunting and Pecking”

1861.9: pwd-value = KDF-z(pwd-seed, “SAE Hunting and Pecking”

1862.56: KCK || PMK = KDF-512(keyseed, “SAE KCK and PMK”

1975.41: TPK = KDF-N\_KEY(TPK-Key-Input, "TDLS PMK"

2009.54: PMK = KDF-256(keyseed, “AP Peerkey Protocol”

2082.1: AEK ← KDF-256(PMK, “AEK Derivation”

2082.7: MTK ← KDF-X(PMK, “Temporal Key Derivation”

3. HMAC-something

959.1: AIH =HMAC-SHA1-64(“ES\_ALERT”

1932.35: PMKID = HMAC-SHA1-128(PMK, "PMK Name"

1932.44: PMKID = Truncate-128(HMAC-SHA-256(PMK, "PMK Name"

1932.50: PMKID = Truncate-128(HMAC-SHA-256(KCK, "PMK Name"

1932.56: PMKID = Truncate-128(HMAC-SHA-384(KCK, "PMK Name"

1935.34: SMKID = HMAC-SHA1-128(SMK, "SMK Name"

1935.43: SMKID = Truncate-128(HMAC-SHA-256(SMK, "SMK Name"

The encodings are specified for the following, but should be aligned with the way the instances above are addressed:

4. KDF-something

1937.58: R0-Key-Data = KDF-Hash-Z(XXKey, "FT-R0"

1938.54: PMK-R1 = KDF-Hash-Z(PMK-R0, "FT-R1"

1939.23: PTK = KDF-Hash-PTKLen(PMK-R1, "FT-PTK"

5. SHA-something

1938.37: PMKR0Name = Truncate-128(SHA-256("FT-R0N"

1939.6: PMKR1Name = Truncate-128(SHA-256(“FT-R1N”

1940.20: PTKName = Truncate-128(SHA-256(PMKR1Name || “FT-PTKN”

The encodings are not specified for the following, but this doesn’t matter as they are mere recommendations/informational:

6. "Init Counter"

1951.12: PRF-256(Random number, “Init Counter”

3461.20: result = PRF-256(0, "Init Counter"

3461.44: Global key counter = result = PRF-256(0, "Init Counter"

3462.49: Global key counter = PRF-256(0, "Init Counter"

Proposed changes:

1.

Change 1930.9 as follows:

*A* is a unique label for each different purpose of the PRF, treated as a sequence of ASCII-encoded octets without a terminating NUL

2.

Change 1937.32 as follows:

*label*, a string identifying the purpose of the keys derived using this KDF, treated as a sequence of ASCII-encoded octets without a terminating NUL

At 1859.7 and 1861.23 add:

where KDF-z is the key derivation function defined in 11.6.1.7.2

At 1862.59 add:

where KDF-512 is the key derivation function defined in 11.6.1.7.2

At 2009.63 add:

KDF-256 is the key derivation function defined in 11.6.1.7.2

At 2082.4 add:

where KDF-256 is the key derivation function defined in 11.6.1.7.2

At 2082.13 add:

where KDF-X is the key derivation function defined in 11.6.1.7.2

Note: the invocation at 1975.41 already has a reference to 11.6.1.7.2.

3.

At 959.4 add:

"ES\_ALERT" is treated as a sequence of ASCII-encoded octets without a terminating NUL

At 1932.57 add:

In all these cases, "PMK Name" is treated as a sequence of ASCII-encoded octets without a terminating NUL.

At 1935.45 add:

In both these cases, "SMK Name" is treated as a sequence of ASCII-encoded octets without a terminating NUL.

4.

Delete the lines at 1938.19 (“— "FT-R0" is 0x46 0x54 0x2D 0x52 0x30.”), 1938.65 (“— "FT-R1" is 0x46 0x54 0x2D 0x52 0x31.”), 1939.34 (“— "FT-PTK" is 0x46 0x54 0x2D 0x50 0x54 0x4B.”).

5.

Change 1938.41 as follows:

— "FT-R0N" is ~~0x46 0x54 0x2D 0x52 0x30 0x4E~~ treated as a sequence of ASCII-encoded octets without a terminating NUL.

Delete the line at 1938.44 (“— SHA-256 is as defined in FIPS PUB 180-3-2008.”).

Change 1939.10 as follows:

— "FT-R1N" is ~~0x46 0x54 0x2D 0x52 0x31 0x4E~~ treated as a sequence of ASCII-encoded octets without a terminating NUL.

Change 1940.25 as follows:

— "FT-PTKN" is ~~0x46 0x54 0x2D 0x50 0x54 0x4B 0x4E~~ treated as a sequence of ASCII-encoded octets without a terminating NUL.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3439, which effect the change proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3478Mark RISON8.7.11214.38 | During D4.0 comment resolution it was stated that "EOF pad" and "EOF padding" are two quite distinct things. While it is true that "EOF pad" is clearly defined as the 0-3 octets you might get at the end of an A-MPDU, "EOF padding" is never clearly defined, even though it is used twice (pages 98 and 322). It would be desirable to clarify what "EOF padding" is, exactly | Add something after the definition of "A-MPDU pre-EOF padding" like "EOF padding is the portion of the A-MPDU after the A-MPDU pre-EOF padding." |

Discussion:

A definition of “EOF pad” is given at 28.1. However there is no similar definition of “EOF padding”. (Note the page references given in the comment are wrong; they should be to 1031(.26) and 2534(.15).)

1214.62 indicates that “EOF padding” is the A-MPDU subframes starting from the first A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field, if any, any subframe padding in the last subframe (though 1215.2 is ambiguous as to which subframe is being referred to, this must be referring to the last one before the first one with 0 in the MPDU Length field and 1 in the EOF field) and any EOF pad (not -ding!).

Proposed changes:

Add a definition after 28.1 as follows:

**end-of-frame (EOF) pad:** The 0 to 3 octets used to pad an aggregate medium access control (MAC) protocol data unit (A-MPDU) to the last octet of the associated physical layer convergence procedure (PLCP) service data unit (PSDU) when the A-MPDU is carried in a very high throughput (VHT) physical layer (PHY) protocol data unit (PPDU).

**end-of-frame (EOF) padding:** The 0 to 3 octets used to pad the last aggregate medium access control (MAC) protocol data unit (A-MPDU) subframe before the first A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field, if there is one, or the last A-MPDU subframe if there is no A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field; plus the A-MPDU subframes starting with the first A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field, if there is one; plus the 0 to 3 octets of end-of-frame (EOF) pad. This padding is used when an A-MPDU is carried in a very high throughput (VHT) physical layer (PHY) protocol data unit (PPDU).

Change 1214.62 onwards as follows:

An A-MPDU pre-EOF padding is

— The portion of the A-MPDU up to but excluding the first A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field and also excluding any subframe padding in the last subframe before the first A-MPDU subframe with 0 in the MPDU Length field and 1 in the EOF field, or

— The portion of the A-MPDU up to and including the last A-MPDU subframe if no A-MPDU subframes with 0 in the MPDU Length field and 1 in the EOF field are present, but excluding any subframe padding in the last subframe.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3478. This addresses the comment in a different way to the way proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3479Mark RISON10.40.41823.9 | For non-VHT STAs to be able to fully benefit from the new power/regulatory/channel switching stuff, it is necessary for them e.g. to be able to receive a unicast (Extended) Channel Switch Announcement MMPDU with e.g. a VHT Transmit Power Envelope element | Add an Extended Capability bit to allow a non-VHT STA to indicate support for the VHT power/regulatory/channel switching stuff, and ensure the text requires VHT STAs to use the VHT power/regulatory/channel switching stuff with non-VHT devices which have indicated this capability |

Discussion:

802.11ac introduced a lot of things to clean up, hopefully once for all, the hodge-podge of power/regulatory/channel switching stuff, broken to various extents, which had accreted over the years. It would be highly desirable for non-VHT STAs to be able to use these things too, in the hope that the broken stuff will just fade away.

Also, some TVHT MIB variables/attributes were overlooked.

Various lacunae in the handling of the Wide Bandwidth Channel Switch (sub)element were identified in passing.

Proposed changes:

Change 616.42 and 629.61 as follows:

dot11VHTOptionImplemented, dot11TVHTOptionImplemented or dot11ExtendedSpectrumManagementImplemented is true;

Change 616.47 as follows:

The Channel Switch Wrapper element is optionally present if dot11VHTOptionImplemented, dot11TVHTOptionImplemented or dot11ExtendedSpectrumManagementImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the Beacon frame and the Channel Switch Wrapper element contains at least one subelement.

~~The Channel Switch Wrapper element is optionally present if dot11TVHTOptionImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the Beacon frame and the Channel Switch Wrapper element contains at least one subelement.~~

Change 630.6 as follows:

The Channel Switch Wrapper element is optionally present if dot11VHTOptionImplemented, dot11TVHTOptionImplemented or dot11ExtendedSpectrumManagementImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the ~~Beacon~~Probe Response frame and the Channel Switch Wrapper element contains at least one subelement.

~~The Channel Switch Wrapper element is optionally present if dot11TVHTOptionImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the Beacon frame and the Channel Switch Wrapper element contains at least one subelement.~~

Insert a new penultimate row at 823.43:

|  |  |  |
| --- | --- | --- |
| <ANA+1>  | Extended Spectrum Management Capable | The STA sets the Extended Spectrum Management Capable field to 1 when dot11ExtendedSpectrumManagementImplemented is true and dot11VHTOptionImplemented and dot11TVHTOptionImplemented are false, and sets it to 0 otherwise.Editor’s note: The <ANA+1> flag will be replaced by a number assigned by the 802.11 ANA. |

Insert at 1304.58: “The following, and only the following, are extended spectrum management capable: a VHT STA, a TVHT STA, a STA that has dot11ExtendedSpectrumManagementImplemented true. A non-VHT non-TVHT STA that has dot11ExtendedSpectrumManagementImplemented true shall indicate that it is extended spectrum management capable using the Extended Spectrum Management Capable field of the Extended Capabilities element.” Or does “non-VHT STA” also mean “non-TVHT STA” per 4.3.13?

Insert the following at 1627.10 (in 10.9.8.2 Selecting and advertising a new channel in a non-DMG infrastructure BSS), based on text in 10.40.4 Channel switching methods for a VHT BSS; ignore material with a yellow background:

If a Channel Switch Announcement frame is used to announce a switch to a 20 MHz operating channel width, then neither a Wide Bandwidth Channel Switch element nor a Secondary Channel Offset element shall be present in the frame, except that a Secondary Channel Offset element may be present in a Channel Switch Announcement frame if the Secondary Channel Offset field within the Secondary Channel Offset element is set to SCN. [already implicitly covered by 8.6.2.6 at 1075.58 and 1075.48 – arguably it could be deleted from 10.40.4]

If a Channel Switch Announcement element in a Beacon or Probe Response frame is used to announce a switch to a 20 MHz operating channel width, then a Wide Bandwidth Channel Switch subelement in a Channel Switch Wrapper element shall not be present in the same frame. [same as for VHT STAs at 1823.53]

If a Channel Switch Announcement frame is used to announce a switch to a 40 MHz operating channel width, then the following apply:

— The Secondary Channel Offset element shall be present in the frame.

— The Wide Bandwidth Channel Switch shall not be present in the frame. [already implicitly covered by 8.6.2.6 at 1075.58 and 1075.48 – arguably it could be deleted from 10.40.4]

If a Channel Switch Announcement element in a Beacon or Probe Response frame is used to announce a switch to a 40 MHz operating channel width, then a Wide Bandwidth Channel Switch subelement in a Channel Switch Wrapper element shall also be present in the same frame if the STA sending the frame is extended spectrum management capable. [it’s a “shall” for VHT STAs at 1824.15]

A Channel Switch Wrapper element shall not be included in Beacons and Probe Response frames if the element contains zero subelements.

Insert the following at 1633.47 (in 10.10.3.2 Selecting and advertising a new channel in an infrastructure BSS), based on text in 10.40.4 Channel switching methods for a VHT BSS; ignore material with a yellow background:

If an Extended Channel Switch Announcement element in a Beacon frame or Probe Response frame or an Extended Channel Switch Announcement frame is used to announce a switch to a 20 MHz operating channel width, then neither a Wide Bandwidth Channel Switch element nor a Wide Bandwidth Channel Switch subelement shall be present in the same frame. [WBCSse in CSWe covered by 8.4.2.162 at 1038.34; WBCSe covered by 8.6.8.7 at 1102.9]

If an Extended Channel Switch Announcement element in a Beacon or Probe Response frame is used to announce a switch to a 40 MHz operating channel width, then a Wide Bandwidth Channel Switch subelement in a Channel Switch Wrapper element may be present in the same frame if the STA sending the frame is extended spectrum management capable. [it’s also a “may” for VHT STAs at 1824.20]

Change 1644.56 as follows:

A ~~non-VHT~~ STA that is not extended spectrum management capable shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Beacon Request or Beacon Report. A ~~VHT~~ STA shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Beacon Request or Beacon Report sent to a ~~non-VHT~~ STA that is not extended spectrum management capable. If the Wide Bandwidth Channel Switch subelement is included in a Beacon Request or Beacon Report, then the Operating Class shall indicate a 40 MHz channel spacing.

Add a new paragraph at 1645.60 as follows:

A STA that is not extended spectrum management capable shall not include a Wide Bandwidth Channel Switch subelement in a Frame Request or Frame Report. A STA shall not include a Wide Bandwidth Channel Switch subelement in a Frame Request or Frame Report sent to a STA that is not extended spectrum management capable. If the Wide Bandwidth Channel Switch subelement is included in a Frame Request or Frame Report, then the Operating Class shall indicate a 40 MHz channel spacing.

Change 1646.24 as follows:

A ~~non-VHT~~ STA that is not extended spectrum management capable shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Channel Load Request or Channel Load Report. A ~~VHT~~ STA shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Channel Load Request or Channel Load Report sent to a ~~non-VHT~~ STA that is not extended spectrum management capable.

Change 1647.30 as follows:

A ~~non-VHT~~ STA that is not extended spectrum management capable shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Noise Histogram Request or Noise Histogram Report. A ~~VHT~~ STA shall not include a Wide Bandwidth Channel Switch subelement in ~~the~~a Noise Histogram Request or Noise Histogram Report sent to a ~~non-VHT~~ STA that is not extended spectrum management capable.

Add a new paragraph at 1661.56 as follows:

An AP that is not extended spectrum management capable shall not include a Wide Bandwidth Channel Switch subelement in a Measurement Pilot frame. If the Wide Bandwidth Channel Switch subelement is included in a Measurement Pilot frame, then the Operating Class shall indicate a 40 MHz channel spacing.

Change 768.45 as follows:

|  |  |  |
| --- | --- | --- |
| 2-~~220~~162 | Reserved |  |
| 163 | Wide Bandwidth Channel Switch | Yes |
| 164-220 | Reserved |  |

Change 1099.10 as follows:

|  |  |  |
| --- | --- | --- |
| 72-~~220~~162 | Reserved |  |
| 163 | Wide Bandwidth Channel Switch | Yes |
| 164-220 | Reserved |  |

Add the following paragraph at 736.23, 766.53, 769.5, 1098.60:

The Wide Bandwidth Channel Switch subelement has the same format as the corresponding element (see 8.4.2.160 (Wide Bandwidth Channel Switch element)), with the constraint that the New Channel Width field indicates an 80 MHz, 160 MHz, or 80+80 MHz operating channel width.

Change 767.32 as follows:

If the PPDU carrying the received frame comprises noncontiguous frequency segments, the Operating Class and Channel Number fields identify the center frequency of frequency segment 0, and a Wide Bandwidth Channel Switch subelement is included to identify the center frequency of frequency segment 1 (the other fields in the subelement are reserved *or* set to indicate 80+80 MHz width and the same center frequency of frequency segment 0?); otherwise the Wide Bandwidth Channel Switch subelement is not included.

Change “measurement request” to “measurement report” at 763.48, 763.49, 763.56, 763.59, 763.61, 764.6, 765.22, 765.25, 769.27, 769.29.

Change “measurement report” to “measurement request” at 733.21, 736.60.

Change “element” to “subelement” at 1098.29.

Change “VHT Transmit Power Envelope” to “Transmit Power Envelope” throughout (95 instances, including cross-references).

Change 1305.23 as follows:

A ~~VHT~~ STA that is extended spectrum management capable and that has dot11SpectrumManagementRequired or dot11RadioMeasurementActivated equal to true shall determine a local maximum transmit power from a VHT Transmit Power Envelope element for which the Local Maximum Transmit Power Unit Interpretation subfield indicates EIRP. [this is restricted to dot11OperatingClassesImplemented being true too – is that OK?]

Change 1305.32 as follows:

~~When~~If a ~~VHT~~ STA that is extended spectrum management capable finds an unknown value in the Local Maximum Transmit Power Unit Interpretation subfield in a VHT Transmit Power Envelope element, then the STA shall ignore that and subsequent VHT Transmit Power Envelope elements.

Change 1619.23 as follows:

If the Beacon or Probe Response frame most recently received from an AP by a ~~VHT~~ STA that is extended spectrum management capable and that has dot11SpectrumManagementRequired or dot11RadioMeasurementActivated equal to true includes one or more VHT Transmit Power Envelope elements, then the units of the Minimum Transmit Power Capability and Maximum Transmit Power Capability fields within the Power Capability element sent in the STA’s (Re)Association Request frame to the AP shall be interpreted according to the Local Maximum Transmit Power Unit Interpretation subfield in the Transmit Power Information field in the VHT Transmit Power Envelope element (see 8.4.2.161 (VHT Transmit Power Envelope element)) sent first in the Beacon or Probe Response frame; otherwise, the units of the Minimum Transmit Power Capability and Maximum Transmit Power Capability fields within the Power Capability element sent in the STA’s (Re)Association Request frame to the AP shall be interpreted as EIRP.

If the Beacon or Probe Response frame most recently received from a neighbor mesh STA by a ~~VHT~~ mesh STA that is extended spectrum management capable and that has dot11SpectrumManagementRequired or dot11RadioMeasurementActivated equal to true includes one or more VHT Transmit Power Envelope elements, then the units of the Minimum Transmit Power Capability and Maximum Transmit Power Capability fields within the Power Capability element sent in the Mesh Peering Open frame to the neighbor mesh STA shall be interpreted according to the Local Maximum Transmit Power Unit Interpretation subfield in the Transmit Power Information field in the VHT Transmit Power Envelope element (see 8.4.2.161 (VHT Transmit Power Envelope element)) sent first in the Beacon or Probe Response frame. Otherwise, the units of the Minimum Transmit Power Capability and Maximum Transmit Power Capability fields within the Power Capability element sent in the ~~VHT~~ mesh STA’s Mesh Peering Open frame to the neighbor mesh STA shall be interpreted as EIRP.

Change 1619.60 as follows:

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

— Unless the STA is ~~a VHT STA~~ extended spectrum management capable and has received a VHT Transmit Power Envelope element for a channel width of 20 MHz and 40 MHz, any local maximum transmit power received in the combination of a Country element and a 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 is extended spectrum management capable, a~~A~~ny local maximum transmit power received in a VHT Transmit Power Envelope element from the AP in its BSS, another STA in its IBSS, or a neighbor peer mesh STA in its MBSS

— Any local maximum transmit power for the channel regulatory domain known by the STA from other sources

Change 1620.42 as follows:

~~A VHT AP in a BSS, a VHT STA in an IBSS, and a VHT mesh STA in a MBSS~~ If an AP, IBSS STA or mesh STA is extended spectrum management capable, it shall advertise the local maximum transmit power for that STA’s operating channel in Beacon frames and Probe Response frames using one VHT Transmit Power Envelope element for each distinct value of the Local Maximum Transmit Power Unit Interpretation subfield that is supported by the BSS, IBSS, or MBSS, respectively. Each VHT Transmit Power Envelope element shall include a local power constraint for all channel widths supported by the BSS.

~~VHT~~ STAs that are extended spectrum management capable and that have dot11RadioMeasurementActivated equal to true should be able to reduce their EIRP to 0 dBm.

Change 1700.39 as follows:

A TDLS peer ~~VHT~~ STA that is extended spectrum management capable and that announces new TPC parameters that come into effect at the same time as the switch to an off-channel direct link, shall include at least one VHT Transmit Power Envelope element in the transmitted the TDLS Channel Switch Request frame. The recipient TDLS peer ~~VHT~~ STA that is extended spectrum management capable and that has dot11SpectrumManagementRequired or dot11RadioMeasurementActivated equal to true shall use the parameters in these received element(s) in the recipient STA's TPC calculations for the off-channel direct link.

Change 1824.52 as follows:

If new BSS TPC parameters are announced that come into effect at the same time as the channel switch, then ~~a STA that is a VHT AP, a VHT STA in an IBSS, or a VHT mesh STA in an MBSS~~ if an AP, IBSS STA or mesh STA is extended spectrum management capable, it shall include

— At least one New VHT Transmit Power Envelope element in a transmitted Channel Switch Announcement frame or Extended Channel Switch Announcement frame and

— At least one New VHT Transmit Power Envelope subelement in a transmitted Channel Wrapper element in Beacon and Probe Response frames.

A recipient ~~VHT~~ STA in the BSS ~~STA~~ that is extended spectrum management capable and that has dot11SpectrumManagementRequired or dot11RadioMeasurementActivated equal to true and that maintains association with the BSS after the switch shall use the parameters in these received elements and subelements in the recipient STA’s TPC calculations for the new operating channel and operating channel width (see 10.8 (TPC procedures)). If both New VHT Transmit Power Envelope elements and New VHT Transmit Power Envelope subelements are transmitted for the switch, the set of New VHT Transmit Power Envelope elements and set of subelements shall contain the same set of values for the Local Maximum Transmit Power Unit Interpretation subfield, and New VHT Transmit Power Envelope elements and subelements that have the same value for the Local Maximum Transmit Power Unit Interpretation subfield shall also have the same values for their other fields.

If a new country string, new operating classes or both, are coming into effect at the same time as the channel switch, then ~~a STA that is a VHT AP, a VHT STA in an IBSS, or a VHT mesh STA in an MBSS~~ if an AP, IBSS STA or mesh STA is extended spectrum management capable, it shall include

— A New Country element in a transmitted Extended Channel Switch Announcement frame and

— A New Country subelement in a transmitted Channel Wrapper element.

The New Country element or subelement shall contain all the Operating Classes for the BSS after the switch. The New Country element or subelement, transmitted in an Extended Channel Switch Announcement frame or in the same frame as an Extended Channel Switch Announcement element, respectively, shall include one Operating Triplet field that contains the same Operating Class as the New Operating Class field in the Extended Channel Switch Announcement frame or Extended Channel Switch Announcement element. A recipient ~~VHT~~ STA in the BSS ~~STA~~ that is extended spectrum management capable and that has dot11MultiDomainCapabilityActivated, dot11SpectrumManagementRequired, or dot11RadioMeasurementActivated equal to true and that maintains association with the BSS after the switch shall use the parameters in these received elements and subelements in order to maintain regulatory compliance. If both New Country elements and New Country subelements are transmitted for the switch, their fields shall be the same.

A Channel Switch Wrapper element shall not be included in Beacons and Probe Responses if the element contains zero subelements.

NOTE 4—Channel Switch Wrapper is not defined to carry subelements in the case of a switch to 20 MHz and when no change to the country string, operating classes or TPC parameters are announced.

A VHT STA uses the VHT Transmit Power Envelope element only [was this “uses only” fixed in the MDR?] for TPC of 80 MHz, 160 MHz, and 80+80 MHz transmissions. In the Country element, a VHT STA shall include zero Subband Triplet fields in a Operating/Subband Sequence field that contains an Operating Class field for which the “Channel Spacing (MHz)” column in the applicable table in Annex E equals 80 or 160.

An AP that switches the BSS to a lower operating channel width may recalculate the TS bandwidth budget and may delete one or more active TSs by invoking the MLME-DELTS.request primitive with a ReasonCode value of SERVICE\_CHANGE\_PRECLUDES\_TS.

A VHT STA that is a member of an IBSS shall not transmit values in the Wide Bandwidth Channel Switch element that change the frequency ordering of the primary 40 MHz channel and the secondary 40 MHz channel from the ordering of the most recently adopted operating channel, if the operating channel includes a secondary 40 MHz channel. A VHT STA that is a member of an IBSS shall not transmit values in the Wide Bandwidth Channel Switch element that change the frequency ordering of the primary 80 MHz channel and the secondary 80 MHz channel from the ordering of the most recently adopted operating channel, if the operating channel includes a secondary 80 MHz channel.

Note: I can’t find where the use/non-use of Transmit Power Envelope subelements in a Channel Switch Wrapper is specified.

Add the following MIB variable/attribute in Annex C:

dot11ExtendedSpectrumManagementImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute, when true, indicates that the non-VHT non-TVHT station implementation is capable of supporting extended spectrum management. The capability is disabled at the non-VHT non-TVHT station otherwise."

DEFVAL { false }

::= { dot11StationConfigEntry 24 }

TBD: check PICS SM20.4-9 and DSE9.4-12 and SM1.1 and MD13-15 and DSE5,6

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3479, which effect the change proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3049Adrian StephensB.4.4.22647.29 | Why is there are reference to Annex E? It doesn't seem relevant.Ditto at 2650.26. | Remove reference to Annex E. |
| CID 3050Adrian StephensB.4.4.22651.12 | The changes to FR11 from CID 2425 leave the Status cell empty. | Specify an non-blank status. |
| CID 3051Adrian StephensB.4.17.12731.14 | The change made by .11ac (insertion of CF29:M) to HTM8 is redundant given the change from CID 187. I.e. a VHT STA is an HT STA, and CF16:M suffices. | Remove CF29:M at cited location. |
| CID 3052Adrian StephensB.4.192762.47 | "type equal to Fine Timing Measurement Range request/report"There is no such type.Ditto at 2762.53. | Reword "Initiator of Measurement request/report with type equal to Fine Timing Measurement Range request/report" to remove "/" and use only defined terms for reports and types. |
| CID 3136Mitsuru IwaokaB.4.32627.60 | CF6 (OFDM) PHY shall be mandatory for TVHT PHY as it shall support non-HT PPDU format. | Add "CF30:M" to the Status column of the "\* CF6" row. |
| CID 3137Mitsuru IwaokaB.4.32629.26 | According to the resolutions of CID 5015-5017 of P802.11af Sponsor Ballot (see 11-12/1017r62), a TVHT STA is an HT STA, thus, CF16 shall be mandatory for CF30. | Insert a new "\* CF16.3" row as follows;\* CF16.3 | HT operation in TVWS band | | CF30:M | Yes [] No [] N/A [] |

Discussion:

The PICS is a splendid institution.

Yup, Annex E is not relevant to frame tx. Or indeed to frame rx.

Yup, CID 2425’s resolution left the cell blank. Well, there’s no point deauthing if you can’t auth, so make the former depend on the latter (same as for disassoc and (re)assoc).

Yup, a VHT STA is an HT STA, so if you have a CF16:M you don’t need a CF29:M.

The references to the FTM range stuff are wrong.

Ooh, yes, TVHT STAs need to support OFDM PPDUs (see 2565.32, 2567.25 and 2576.3). Groovy! However, the same is explicitly not true of HT PPDUs: “Transmission of HT PPDU is not supported in Clause 23” (23.2.4 at 2575.62; repeated for good measure in 23.3.9.2). I don’t know what the 11af CRC was smoking when it resolved CIDs 5015-5017.

Proposed resolution for CID 3049:

REVISED

Delete “, Annex E” at 2647.28, 2650.26.

Proposed resolution for CID 3050:

REVISED

Insert “FR10:M” in the Status column at 2651.12.

Proposed resolution for CIDs 3051 and 3136:

ACCEPTED

Proposed resolution for CID 3052:

REVISED

Change the protocol capability and reference cell values at 2762.45 to: “Initiator of Fine Timing Measurement Range request and responder to Fine Timing Measurement Range report” and “10.11.9.11”.

Change the protocol capability and reference cell values at 2762.53 to: “Responder of Fine Timing Measurement Range request and initiator of Fine Timing Measurement Range report” and “10.11.9.11”.

Proposed resolution for CID 3137:

REJECTED

The TVHT PHY does not require support for HT PPDUs (see 23.2.4 at 2575.62). The 11af CRC erred.

**References:**

802.11mc/D3.0