IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some MAC, PICS and security comments on 11mc/D3.0 (LB202) | | | | |
| Date: 2014-12-05 | | | | |
| 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 3020, 3023, 3212, 3213, 3313, 3314, 3318, 3323, 3324, 3345, 3355, 3359, 3360, 3365, 3368, 3369, 3370, 3374, 3377, 3382, 3386, 3390, 3431, 3440, 3477, 3478, 3479, 3483, PICS CIDs 3049, 3050, 3051, 3052, 3136, 3137, 3325 and security CIDs 3426, 3427, 3429, 3432, 3433, 3439, 3444 on 11mc/D3.0.

r1: Added MAC CID 3020 and PICS CIDs 3049, 3050, 3051, 3052, 3136, 3137, 3325.

r2: Updated during Athens F2F (reached CIDs 3323/3325). Added MAC CIDs 3355 and 3477. Removed articles before “HMAC-hash-len” and noun groups following “HMAC-hash-len” in the resolution of CID 3429 et al.

r3: Updated prior to San Antonio F2F. Added MAC CIDs 3213, 3345, 3374, 3386 and 3440. Added Security CID 3433.

r4: Updated prior to San Antonio F2F. Added MAC CIDs 3212 and 3431.

r5: Updated for San Antonio F2F.

r6: Updated for San Antonio F2F. Added MAC CIDs 3368, 3369, 3370, 3390, 3483.

r7: Updated prior to Atlanta F2F. Added Security CID 3444.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3023 Adrian Stephens  9.7.12.2  1291.62 | "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.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3313  Mark RISON  9.3.2.8.1  1243.64 | "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 3314  Mark RISON  9.3.6  1259.43 | "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 [taken over by Dorothy]

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3318  Mark RISON  9.7.6.5.5  1284.29 | "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 3323  Mark RISON  10.2.5  1561.6 | 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) |
| CID 3325  Mark RISON  B.4.17.1  2733.46 | 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 |

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 (it indicates the state immediately after (re)association). 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). It’s not immediately obvious what value existing AP implementations would have used here, so need to be flexible.

There is also suggestion that SMPS 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. [The intent might have been to apply the SMPS mode to the (Re)Association Response, but this does not really seem 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:

Only valid in a (Re)Association Request frame sent to an AP. Reserved and shall be set to 0 or 3 otherwise.

NOTE—This subfield indicates the operational state immediately after (re)association, 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 HT 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.”

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 (SM  Power Save  frame format),  10.2.5 (SM  power 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 (SM  power 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 3323 and 3325, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3324  Mark RISON  10.2.5  1561.6 | 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 3359  Mark 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 3360  Mark 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 3377  Mark RISON | "OperationalRateSet, which is a parameter of the MLME-JOIN.request primitive" -- also the START | Add "and MLME-START.request primitive" |
| CID 3020  Adrian Stephens  9.7.5.3  1274.61 | 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. Wait for SB to fix DMG-related stuff.)

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).

*<paragraph break>*

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).

*<paragraph break>*

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).

*<paragraph break>*

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).

*<paragraph break>*

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 and is supported by the non-AP STA, or corresponds to an HT MCS in the AP’s operational HT MCS set at a bandwidth supported by the non-AP STA and permitted in the BSS, or to a VHT-MCS and NSS in the AP’s operational VHT-MCS and NSS set at a bandwidth supported by the non-AP STA and permitted in the BSS, for an uplink TS.

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

— it is in both the AP’s and the non-AP STA’s operational rate set ~~and non-AP STA’s operational rate set~~ and is in the basic rate set and is supported by the non-AP STA, or corresponds to an HT MCS in both the AP’s and the non-AP STA’s operational HT MCS set at a bandwidth supported by the non-AP STA and permitted in the BSS, or to a VHT-MCS and NSS in both the AP’s and the non-AP STA’s operational VHT-MCS and NSS set at a bandwidth supported by the non-AP STA and permitted in the BSS, 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.”

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

Make the changes described in $thisdoc under “Proposed changes:” for CID 3359, 3360 and 3377. These delete 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 3359, 3360 and 3377, 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 3365  Mark RISON  8.6.2.3.1  1078.7 | 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 (note deletion of “t” in “not”).
* “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 3382  Mark RISON  C.3  2814.53 | 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
* The range does not support the full range allowed (65535 x 32 microseconds = ~ 2 s)
* 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: changes made by CID 3776 not folded in

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, in multiples of 32 microseconds. 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, in multiples of 32 microseconds. 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 3432  Mark RISON  11.6.1.7  1935.46 | 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 3433  Mark RISON  11.10.2  2010.18 | What is the difference between destroying something and "irretrievably destroying" something | Delete "irretrievably" |

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).

Proposed changes:

Change “destroy” to “delete” at 102.56, 103.7, 103.13, 1671.12, 1695.5, 1695.40, 1863.33, 1870.5, 1870.14, 1870.20, 1911.1, 1938.43, 2062.45.

Change “destroyed” to “deleted” at 102.55, 238.62, 1862.12, 1867.52, 1870.25, 1922.49, 1922.50, 2010.18.

Change “destruction” to “deletion” at 1173.24.

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 1937.44 as follows: “~~securely~~irretrievably delete ~~all unused~~the other bits”.

Change 1938.43 as follows: “— Truncate-128(-) returns the first 128 bits of its argument and ~~securely destroys~~ irretrievably deletes the remainder.”

Do the msbs need to be irretrievably deleted at 1941.63 (EAPOL-Key MIC), 1896.4 (BIP-CMAC) and 959.5 (Emergency Alert Identifier Hash)?

Delete the extra space at 1952.24.

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

Proposed resolution for CID 3432:

REVISED

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

Proposed resolution for CID 3433:

REVISED

Rather than deleting “irretrievably”, replace “destroying” with “deleting”. Make the changes described in $thisdoc under “Proposed changes:” for CID 3433.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3426  Mark RISON | "HMAC-SHA-256" (6 instances) is confusing as 256 is not the output length | "HMAC-SHA256" |
| CID 3427  Mark RISON  11.6.1.3  1932.36 | "HMAC-SHA1-128" | "Truncate128(HMAC-SHA1-160" for consistency with other PMKIDs. Also at 1935.35 |
| CID 3429  Mark 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:

Regarding terminology, it seems the hashes themselves are SHA-1, SHA-256 and SHA-384 (see FIPS PUB 180-3-2008, normatively referenced in clause 2).

However, the HMACs which use the latter two should be (and generally are) HMAC-SHA*n*[-*len*] to avoid confusion with the truncated HMACs (see IETF RFC 2104, normatively referenced in clause 2, which “must be understood and used”).

[References: HMAC is described in IETF RFC 2104, which is listed in clause 2. Clause 2 starts as follows (my emphasis):

The following referenced documents are indispensable for the application of this standard (i.e., they **must be understood and used**

The notation for truncation of HMAC is described in section 5 of IETF RFC 2104 (my emphasis):

We propose denoting a realization of HMAC that uses a hash function H with t bits of output as HMAC-H-t. **For** **example, HMAC-SHA1-80** denotes HMAC computed using the **SHA-1** function and with the output truncated to 80 bits.

It is therefore very clear that the notation – which “must be understood and used” according to clause 2 – is to exclude any hyphen from the name of the hash used in an HMAC.  (Speculation as to why this was done would not be relevant here.)]

It would be defensible, though, to keep HMAC-SHA-1 since it seems harder to think the 1 might be a truncation length, and this aligns with IETF RFC 2202 (“Test Cases for HMAC-MD5 and HMAC‑SHA‑1”, informatively referenced in annex A). If this is not preferred by the group, however, then delete the material highlighted in purple below.

A desire has been expressed to consider HMAC-SHA1-64 a proper noun rather than an adjective.

Proposed changes:

Change 958.63 as follows: “The value of this field is the hash produced by ~~the~~ HMAC-SHA1-64 ~~hash algorithm~~”.

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 HMAC-SHA1-64 ~~hash algorithm~~”.

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 delete bits 128 onwards.” Also move the tab stop for this list to the right so that you don’t get “)From” at 1929.3.

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 1941.62 and 1941.63.

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.

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.

Proposed resolution for CID 3429:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3439  Mark RISON  11.6.1.7.2  1937.23 | 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 strings 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 null

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 null

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 null

At 1932.57 add:

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

At 1935.45 add:

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

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 null.

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 null.

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 null.

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 3478  Mark RISON  8.7.1  1214.38 | 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 3479  Mark RISON  10.40.4  1823.9 | 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 (does “non-VHT STA” also mean “non-TVHT STA” per 4.3.13?):

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.

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? The intent was "does use VTPe and does not use PCe for TPC"] 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 3049  Adrian Stephens  B.4.4.2  2647.29 | Why is there are reference to Annex E? It doesn't seem relevant.  Ditto at 2650.26. | Remove reference to Annex E. |
| CID 3050  Adrian Stephens  B.4.4.2  2651.12 | The changes to FR11 from CID 2425 leave the Status cell empty. | Specify an non-blank status. |
| CID 3051  Adrian Stephens  B.4.17.1  2731.14 | 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 3052  Adrian Stephens  B.4.19  2762.47 | "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 3136  Mitsuru Iwaoka  B.4.3  2627.60 | 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 3137  Mitsuru Iwaoka  B.4.3  2629.26 | 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 shouldn’t need a CF29:M. There’s a CF29:M for CF16.2. Unfortunately nothing requires CF16 if CF16.2 is supported. Oops.

Yup, the references to the FTM range stuff are wrong. I am indebted to Brian Hart for hints as to the correct wording.

Ooh, yup, 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 [sic] 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 CID 3051:

REVISED

Delete “CF29:M” at 2731.14.

Add “CF29:M” to the Status for CF16 at 2629.27.

Change “O” to “O.2” at 2630.35.

Proposed resolution for CID 3136:

ACCEPTED

Proposed resolution for CID 3052:

REVISED

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

Change the protocol capability and reference cell values at 2762.53 to: “Receiver of Fine Timing Measurement Range request and transmitter 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).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3355  Mark RISON  10.1.4.3.5  1527.16 | If a Request element includes something which would anyway be included in a Probe Response, does the element still get included at the end (i.e. twice)? | Suggest saying may choose not to include at the end, to make text most likely to be compatible with existing devices |

Discussion:

The handling of the Request element is grossly under-specified. The question is how to specify it while maximising the chance of maintaining compatibility with existing implementations. The informal summary of the proposal is:

* Unnecessary requests, i.e. requests for things which are returned anyway, should not be made (new, but merely a recommendation)
* Unnecessary requests may be returned at the end (in addition to their normal position, i.e. they may, but are not required to, be included twice; the clarification sought by the commenter)
* The requests at the end are in the order they were requested (no change)
* Do not request the same thing twice (new, but should be safe)

A request has been made to say “include” rather than “return”.

Proposed changes:

Change 10.1.4.3.5 as follows:

**10.1.4.3.5 Contents of a probe response**

A STA that responds to a ~~p~~Probe ~~r~~Request frame according to 10.1.4.3.4 (Criteria for sending a probe response) shall transmit a Probe Response frame ~~as follows:~~

~~— The Probe Response frame is~~ individually addressed to the STA that ~~generated~~transmitted the Probe Request frame.

If there was a Request element in the Probe Request frame, then:

— Each element requested in ~~a~~the Request element shall be included in the Probe Response frame if the responding STA supports that element and shall not be included otherwise.

— Elements that would not have been included otherwise shall be included after all the elements that would have been included even in the absence of the Request element.

— Elements that would have been included even in the absence of the Request element shall be included in their normal position (see Table 8-42), and may be included again after all the elements that would have been included even in the absence of the Request element.

NOTE—An element that would necessarily be included anyway is not expected to be requested.

— Elements after all the elements that would have been included even in the absence of the Request element ~~In the Probe Response frame, the STA~~ shall be ~~return~~included ~~the requested elements~~ in the same order as ~~requested~~ in the Request element.

— If dot11RadioMeasurementActivated is true and ~~if the Request element of the Probe Request includes~~ the RCPI element ~~ID~~ was requested, ~~the STA shall include in the Probe Response~~ an RCPI element containing the ~~measured~~ RCPI ~~value~~ of the ~~received~~ Probe Request frame shall be included. If no measurement result is available, the RCPI value shall be set to indicate that a measurement is not available (see 8.4.2.37).

Add at the end of the para at 718.56: “The Requested Element IDs should not include an element ID that corresponds to an element that will be included in the Probe Response frame even in the absence of the Request element, or will be excluded from the Probe Response frame even in the presence of the Request element, per the notes in Table 8-42. A given element ID is included at most once among the Requested Element IDs.”

Change the reference at 718.59 to 10.1.4.3.5.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3355, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3477  Mark RISON  9.13.6  1298.33 | The second bullet appears to allow a VHT single MPDU (i.e. one with EOF = 1) to be followed by null subframes with EOF = 0. Once EOF has been signalled, it makes no sense to unsignal it (cf. 145.33) | Change "0 in the EOF field" to "the same value in the EOF field as the preceding A-MPDU subframe" |

Discussion:

As the commenter suggests, by definition once one has hit logical EOF one cannot cease to be at logical EOF within the “frame” (i.e. PPDU). Furthermore, allowing null frames with EOF = 0 after a VHT single MPDU wastes power at the receiver if the MPDU delimiter for the VHT single MPDU is corrupted (i.e. the receiver does not know EOF was signalled in it). EOF signalling should be “sticky”.

The change proposed by the commenter is as follows:

An A-MPDU pre-EOF padding (see 9.13.2 (A-MPDU length limit rules)) is constructed for each user from any of the following:

— A-MPDU subframes constructed from the MPDUs available for transmission that have a TID value that maps to the primary AC

— A-MPDU subframes with 0 in the MPDU Length field and ~~0 in the EOF field~~ the same value in the EOF field as the preceding A-MPDU subframe

This is not right either, since if the first A-MPDU subframe contained a VHT single MPDU (i.e. EOF = 1), following null frames with EOF = 1 are by definition EOF padding so can’t be in an APEP.

Note: the reference to 145.33 is to 11ac/D5.0. The reference in 11mc/D3.0 should have been to 1299.48:

An A-MPDU subframe with EOF set to 1 and with MPDU Length field set to 0 shall not be added before any A-MPDU subframe with EOF set to 0.

That requirement addesses EOF = 0 after null frames with EOF = 1, but does not address EOF = 0 after non-null frames with EOF = 1 (i.e. VHT single MPDUs). Therefore the simplest solution is to reduce that sentence to:

An A-MPDU subframe with EOF set to 1 ~~and with MPDU Length field set to 0~~ shall not be added before any A-MPDU subframe with EOF set to 0.

This is probably better expressed as:

An A-MPDU subframe with EOF set to 0 shall not be added after any A-MPDU subframe with EOF set to 1.

Proposed resolution:

REVISED

Change the sentence at 1299.48 to say “An A-MPDU subframe with EOF set to 0 shall not be added after any A-MPDU subframe with EOF set to 1.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3212  Qi Wang  9.35.6.5  1442.37 | The formula for guard time calculation makes use of constant C, which is defined "equal to aClockAccuracy, in units of ppm". The aClockAccuracy parameter has been defined as +/-20 ppm, so it is not clear what C shoud be set to. | Remove the +/- sign from the definition of aClockAccuracy in DMG MAC sublayer parameter values. Also use a less generic name such as aDMGTSFAccuracy. |
| CID 3213  Qi Wang  10.1.3.9  1521.50 | "The accuracy of the TSF timer shall be no worse than +/-0.01%." State DMG requirements if different. | DMG defines aClockAccuracy as +/-20 ppm; if the same level of accuracy is meant for TSF in DMG, sentence should state the DMG requirement separately; for example, "The TSF timer accuracy shall be +/-20 ppm for DMG networks and +/-100 ppm for non-DMG networks" or similar (Accuracy requirements throughout the specification seem to have been defined in ppm; sugggest to use 100 ppm instead of .01% for consistency). |
| CID 3345  Mark RISON  10.1.3.9  1521.50 | What is the required TSF accuracy for an AP? The position of the current 0.01% requirement suggests it's only on non-AP STAs | Promote the 0.01% requirement to the top of the subclause so it applies to all STAs |
| CID 3374  Mark RISON  10.1.3.9  1521.30 | Need to specify whether the worst-case TSF drift between two devices is 0.01% or 0.02% | Add a NOTE to confirm it's 0.02% |

Discussion:

The current wording of the only direct reference to the TSF accuracy is “The accuracy of the TSF timer shall be no worse than ±0.01%.” “the TSF timer” is, from earlier sentences in the same paragraph, “the STA’s TSF timer”. “the STA” is, from the first paragraph in the subclause, a STA which has received a Beacon etc. Therefore the current wording, prima facie, only refers to non-AP STAs and leaves open the question of APs’ TSF timer accuracy. However, there is general agreement that this is the same as for non-AP STAs, i.e. 0.01% (except for DMG STAs – see below).

In turn, if the AP is allowed to be up to 0.01% off in one direction, and the non-AP STA is allowed to be up to 0.01% off in the other, it follows that the worst-case TSF drift between them is 0.02%. However, since there has been some confusion on this point, a NOTE is in order.

DMG STAs have a different tolerance, though. As indicated through the aClockAccuracy parameter (see 1820.36), the TSF is required to be accurate to 20 ppm (0.02%). It would help if this parameter actually included “TSF” (cf. aTSFResolution), and the ± makes it hard to use in an equation. Actually, the equations which use the TSF accuracy or resolution are a bit editorially inconsistent; worth tidying up. Similarly, the value of aSBIFSAccuracy is given as a range, which makes it hard to use in an equation.

It would indeed seem more consistent to use ppm rather than %.

Carlos Cordeiro has pointed out that a couple of mistakes were made when incorporating 11ad into REVmc: in one place division by 10-6 is indicated, when division by 106 should have been, and in another place division by 106 has been forgotten entirely. Also, there’s a Floor(TXTIME)+1 which should be a Ceil(TXTIME) just in case the TXTIME happens to be an exact multiple of the granularity.

Proposed changes:

REVISED

Change the para at 1238.3 as follows:

The SBIFS shall be used to separate multiple transmissions from a single transmitter during a receive sector sweep or when each transmission occurs with a different transmit antenna configuration and no SIFS-separated response transmission is expected. The duration of SBIFS is determined by the aSBIFSTime PHY characteristic. The SBIFS is the time from the end of the last symbol of the previous frame to the beginning of the first symbol of the preamble of the subsequent frame as seen at the air interface. A STA shall not allow the space between frames that are defined to be separated by a SBIFS time, as measured on the medium, to be less than aSBIFSTime or to be more than aSBIFSTime + ~~vary from the nominal SBIFS value (aSBIFSTime) by more than~~ aSBIFSAccuracy. Two frames separated by a SBIFS shall both be DMG PPDUs.

Delete “[0, +” and “]” at 2431.37.

Delete the sentence at 1521.49: “The accuracy of the TSF timer shall be no worse than ±0.01%.”.

Add a paragraph at the start of subclause 10.1.3.9: “The accuracy of a non-DMG STA’s TSF timer shall be no worse than ± 100 ppm. The accuracy of a DMG STA’s TSF timer shall be no worse than ± 20 ppm.” Or “A non-DMG STA’s TSF timer shall be accurate to within ± 100 ppm. A DMG STA’s TSF timer shall be accurate to within ± 20 ppm.”, to deal with the slightly odd talk of the accuracy being no worse than a ppm (inaccuracy)?

Add a NOTE immediately below this: “NOTE—The worst-case drift between two non-DMG STAs is, therefore, ± 200 ppm, and between two DMG STAs, ± 40 ppm.”

Change 1820.35 as follows: “a~~Clock~~TSFAccuracy”. Delete “± ” at 1820.35.

At 1434.3 change “10–6” to “106”.

Change 1434.6 as follows:

*C* is ~~the clock accuracy~~aTSFAccuracy, in p~~arts~~ p~~er~~ m~~illion~~

*TDI* is the time elapsed since a synchronizing reference event, in µs. The synchronizing event is the reception of the Timestamp field from the AP or PCP~~.~~

*TP* is aAirPropagationTime, in µs

*TTR* is aTSFResolution, in µs

Change 1442.37 as follows, and then indicate division by 106 (N.B.: not 10-6) of the term highlighted in cyan, as at 1434.2 (after the change indicated above):

*Tguard* = Ceil(((*Ai* + 1) × *C* × *Di*) + ((*Ai* +1 + 1) × *C* × *Di* +1) + *SIFS* + *T~~p~~P,* *T~~resolution~~TR*)

where

*Ai* is the value of MLB allocation *i*, and the value of *Ai* for each allocation depends on whether the allocation is pseudo-static. *Ai* is 0 for a nonpseudo-static allocation and is equal to dot11MaxLostBeacons if the allocation is pseudo-static~~.~~

*C* is ~~equal to~~ a~~Clock~~TSFAccuracy, in ~~units of~~ ppm~~.~~

*Di* is the time elapsed since a synchronizing reference event, in µs, and is not greater than the beacon interval. The synchronizing event is the reception of the Timestamp field from the AP or PCP. For a pseudo-static allocation, *Di* is equal to the beacon interval~~.~~

*SIFS* is aSIFSTime, in µs

*T~~p~~P* is ~~the value of~~ aAirPropagationTime, in µs, which accounts for the propagation delay between the STAs participating in the adjacent allocations~~.~~

*T~~resolution~~TR* is ~~the resolution of the TSF timer (10.39 (DMG MAC sublayer parameters))~~ aTSFResolution, in µs~~.~~

Change 1448.47 as follows:

*Di,n* is the duration of the remaining poll transmissions*~~i, n~~*, in µs

*Om* is the offset of SPR transmission *m*, in µs

SPR*m* is SPR transmission *m*

*TTR* is aTSFResolution, in µs

Change 1449.1 as follows and then move the last definition to be immediately after the *SBIFS* one, the penultimate definition to be immediately after the *Oj* equations, and the one before that to immediately after the *S* one:

*Di,n* ~~represents~~ is the duration of the remaining poll transmissions, ~~and is~~ given by

*Di,n* = Ceil ( ∑ *~~TXTIME~~*TXTIME (Poll*k*) + *SBIFS* + *Ak* + *~~a~~S~~BIFSAccuracy~~*, *T~~resolution~~TR*)

Poll*k* is Poll transmission *k*

*SBIFS* is aSBIFSTime, in µs

*S* is aSBIFSAccuracy, in µs

*Oj* ~~represents~~ is the offset of SPR transmission *j*, ~~defined as~~given by

*Oj* = { *~~T~~~~space~~SIFS*, *j* = 1

*Oj−1* + ~~Floor~~Ceil (*~~TXTIME~~*TXTIME (SPR*j*) + *SIFS*, *T~~resolution~~TR*) ~~+ 1~~, 2 < *j* ≤ *m*

SPR*j* is SPR transmission *j*

*T~~resolution~~TR* is ~~the resolution of the TSF timer~~ aTSFResolution, in µs

*~~T~~~~space~~SIFS* is aSIFSTime, in µs, the time interval between the end of the last Poll frame transmitted by the AP or PCP and the expected start time of the first SPR frame by the non-AP and non-PCP STA~~, and is defined as Tspace = SIFS~~

*Ak* is the antenna switching time, in µs, which is ~~equal to~~ 0 if the AP or PCP uses the same antenna to transmit frame k and frame k+1 and is equal to dot11AntennaSwitchingTime otherwise

(For reference, the outcome after all the scar tissue has been removed is:

*Di,n* is the duration of the remaining poll transmissions, given by

*Di,n* = Ceil ( ∑ TXTIME (Poll*k*) + *SBIFS* + *Ak* + *S*, *TTR*)

Poll*k* is Poll transmission *k*

*SBIFS* is aSBIFSTime, in µs

*Ak* is the antenna switching time, in µs, which is 0 if the AP or PCP uses the same antenna to transmit frame k and frame k+1 and is equal to dot11AntennaSwitchingTime otherwise

*S* is aSBIFSAccuracy, in µs

*TTR* is aTSFResolution, in µs

*Oj* is the offset of SPR transmission *j*, given by

*Oj* = { *SIFS*, *j* = 1

*Oj−1* + Ceil (TXTIME (SPR*j*) + *SIFS*, *TTR*), 2 < *j* ≤ *m*

*SIFS* is aSIFSTime, in µs, the time interval between the end of the last Poll frame transmitted by the AP or PCP and the expected start time of the first SPR frame by the non-AP and non-PCP STA

SPR*j* is SPR transmission *j*

)

Don’t all these equations apply to the *Di,n* and *Om* above (at 1448.47)? If so, shouldn’t they be moved to there (but I’m not clear whether the *Oj* definition applies to *Om* too)?

At the end of 2.55 add “The two parameter form, Floor (*x*,*y*), is the largest multiple of *y* smaller than or equal to *x*; this operator is not used in this Standard if *y* is negative.”. Add a space after the last “Ceil” at 2.58 and add “; this operator is not used in this Standard if *y* is negative” before the full stop at the end of the para.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CIDs 3212, 3213, 3345 and 3374, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | t’9.so the resolution of CID nDU is to different users.concern.ports th with an EEIDone-ocB lgorithmActivated set to truend PRComment | Proposed change |
| CID 3431  Mark RISON  11.6  1928.45 | "L(-)" (3 instances) and "Truncate-128(-)" | Delete the "(-)"s |
| CID 3440  Mark RISON  1.5  2.51 | Define | (bitwise or), L(bitstring, start, len), <the bitwise xor symbol>, << (shift left), >> (logical shift right), >>> (arithmetic shift right, if used), Truncate-128, etc. in 1.5 and not repeatedly all over the place | As it says |

Discussion:

This is mostly straightforward. It turns out arithmetic shift right is not used, and where >>> is used it is used for rotation (as is <<< for the other direction). If ever we do need arithmetic shift right, we’ll have to find other symbols for the rotates (maybe >>< and <<>?).

There seem to be some repeated references to (one of) the UTF-8 specification(s), which are superfluous since UTF-8 is normatively referenced in clause 2.

Proposed changes:

At 1885.61 delete “The XOR (⊕) operation, the bit-wise-and (&) operation, and the addition (+) operation are used in the Phase 1 specification. A loop counter, *i*, and an array index temporary variable, *j*, are also employed.”

At 1886.53 change “The pseudo-code specifying the Phase 2 mixing function employs one variable: *PPK*,” to “The pseudo-code specifying the Phase 2 mixing function employs a variable, *PPK*,”. Delete “The” at 1886.54.

At 1886.54 delete “The pseudo-code also employs a loop counter, *i*.”

At 1886.60 change “The XOR (⊕) operation, the addition (+) operation, the AND (&) operation, the OR (|) operation, and the right bit shift (>>) operation are used in the specification of Phase 2. See Figure 11-15 (Phase 2 key mixing).” to “Phase 2 key mixing is specified in Figure 11-15.”

At 2.51 change “Mathematical usage” to “Mathematical and other usage”. Any better term than “other”, which would cover Boolean and bitwise operators, bases and bit string manipulation? Should there be a separate subclause “Other usage”?

*C AND (&&)*

At 4.3 add “x && y is the short-circuiting Boolean AND.”

At 1480.58, 1481.23, 1490.27, 1490.59 change “&” to “and”.

*Concatenation (||)*

At 4.3 add: “*x* || *y* is the concatenation of *x* and *y*, except in code, where it sometimes is the short-circuiting Boolean OR (as determined by the context).”

Delete “where || symbolizes concatenation” at 1864.42, “(“||” is concatenation)” at 1892.43 and 1900.58, “; and || denotes concatenation” at 1930.10.

Change “(AAD || Management Frame Body including MME)” to “AAD and the management frame body including MME” at 1897.40.

Change “(AAD || Management Frame Body || MME)” to “AAD, the management frame body and MME,” at 1898.18.

Change “Management frame body” to “management frame body” at 710.33, 1305.21

Change “|” to “||” at 3469.22 (3 times), 3469.29 (2 times), 3470.15 (3 times), 3470.60 (3 times), 3471.21 (2 times), 3471.36 (6 times), 3472.9 (2 times), 3472.18 (2 times).

*Logical shift left and right (<< and >>)*

At 4.3 add: “*x* >> *y* is *x* logically shifted right (i.e. zeros are inserted at the most significant end) by *y*; this operator is not used in this Standard if *y* is negative.” Hm, are we sure it’s never arithmetic shift right, for pseudo-C-ode with x being a signed variable? E.g. “int data[4] … data[1] >> 31” on page 3481 is very suspect…

At 4.3 add: “*x* << *y* is *x* shifted left (i.e. zeros are inserted at the least significant end) by *y*; this operator is not used in this Standard if *y* is negative.”

*Bitwise AND and OR (& and |)*

At 4.3 add “*x* & *y*, where *x* and *y* are numbers, is the bit-wise AND of *x* and *y*.” (caveat because & is also used in text).

At 4.3 add “*x* | *y*, where *x* and *y* are numbers, is the bit-wise OR of *x* and *y*.” (again caveat, though this time it’s because e.g. in G.1 it is stated that | is used for selection among alternatives).

At 859.3 delete “| indicates the OR operation”.

*Hex (0x)*

At 4.3 add “0x introduces a hexadecimal number. For example, 0x12 is 18 decimal.”

On page 809, change “Hex value” to “hexadecimal value” (10 times).

At 1767.23 delete the two double quotes.

In the tables in Annex L, change “hex val” (full words case-insensitively) to “Hexadecimal value”, “hex value” (full words case-insensitively) to “Hexadecimal value” and “binary val” (full words case-insensitively) to “Binary value” (20, 87 and 21 instances respectively, but this includes repeated headings for the same table).

At 3457.58, 3457.59, 3462.59, 3463.9 change “hex” to “hexadecimal”.

At 3463.14 delete “In the text discussion outside of tables, integer values are represented in either hex notation using a “0x” prefix or in decimal notation using no prefix. For example, the hex notation 0x12345 and the decimal notation 74565 represent the same integer value.”

*UTF-8*

At 1051.54, 1052.31, 1061.63 delete “UTF-8 format is defined in IETF RFC 3629.”

At 1761.21 change “UTF-8 encoded” to “ASCII encoded”.

*Bitstring manipulation (L() and Truncate-128())*

Change 1929.1 as follows:

The description of the key hierarchies uses the ~~following two functions:~~

~~— L(~~*~~Str~~*~~,~~ *~~F~~*~~,~~ *~~L~~*~~)From~~ *~~Str~~* ~~starting from the left, extract bits~~ *~~F~~* ~~to~~ *~~F~~*~~+~~*~~L~~*~~–1, using the IEEE Std 802.11 bit conventions from 8.2.2 (Conventions).~~

~~— PRF-~~*~~n~~* ~~P~~pseudorandom function producing *n* bits of output, PRF-*n*, defined in 11.6.1.2 (PRF).

At 4.4 add “L (*S*, *F*, *L*) is bits *F* to *F*+*L*–1 of the bit string *S* starting from the left, using the IEEE Std 802.11 bit conventions from 8.2.2 (Conventions).” Using L as the name of the function and also one of the arguments (albeit italicised) is a bit awkward – use N instead?

Delete the line at 1896.7 (“where L is defined in 11.6.1 (Key hierarchy).”).

Delete the line at 1938.6 (“— L(-) is defined in 11.6.1 (Key hierarchy).”).

Delete the line at 1939.53 (“where L(-) is defined in 11.6.1 (Key hierarchy).”).

Delete the lines at 1975.61 to 1975.63 (“where” and “L(-) is defined in 11.6.1 (Key hierarchy).”).

Deindent the line at 1975.57/58.

At 4.4 add “Truncate-128 (*S*) is bits 0 to 127 of the bit string *S* starting from the left, using the IEEE Std 802.11 bit conventions from 8.2.2 (Conventions). Other bits are irretrievably discarded.”. Or “Truncate-128 (*S*) is L (*S*, 0, 128); bits 128 onwards of *S* are irretrievably discarded.”? (Or “deleted”?)

Delete the line at 1938.42 (“— Truncate-128(-) returns the first 128 bits of its argument and securely destroys the remainder.”).

If these changes are accepted, then the resolution for CID 3432 et al. will need a bit of tweaking, since it moves Truncate-128() around too. Also, if we decide we need secure annihilation for the BIP-CMAC and Emergency Alert Identifier Hash, we should generalise Truncate-128() to Truncate-*n*(), so they can use Truncate-64().

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3440, which effect the change proposed by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3386  Mark RISON | There is a zoo of terminology: "operating [band]width", "channel [band]width", "operating channel width", "BSS operating width" (and probably other more esoteric forms) | Pick one term and humanely kill all the others |

Discussion:

The following three terms would be clear and consistent:

* PPDU bandwidth: the bandwidth used to transmit the data in a PPDU (CH\_BANDWIDTH for HT and VHT, for example; see also the n MHz PPDU defintions in subclause 3.2)
* mask bandwidth: the bandwidth of the transmit mask for a PPDU transmission (called “transmit spectrum mask” or “transmit spectral mask” in most PHYs; DMG just calls it “transmit mask”; see also the n MHz mask PPDU definitions in subclause 3.2)
* BSS bandwidth: the maximum PPDU bandwidth of transmissions in a BSS (currently called “BSS” followed by some random combination of one or more of “operating”, “channel”, “width”, “bandwidth” and probably other things)

Note: I received feedback suggesting making it clear that the PPDU bandwidth being referred to here is something in units of Hz (rather than something in units of bps).

Proposed changes:

Add the following definition at 8.7: “basic service set (BSS) bandwidth: The maximum physical layer (PHY) protocol data unit (PPDU) bandwidth of transmissions in a basic service set (BSS).”

Add the following definition at 32.50: “mask bandwidth: The bandwidth of the spectral mask for a physical layer (PHY) protocol data unit (PPDU) transmission.” Add the following NOTE immediately below: “NOTE *i*—An *n* MHz mask PPDU has a mask bandwidth of *n* MHz.”, where *i* is the appropriate NOTE number, and renumber subsequent NOTEs.

Add the following definition at 38.38: “physical layer (PHY) protocol data unit (PPDU) bandwidth: The frequency bandwidth used to transmit the data of a physical layer (PHY) protocol data unit (PPDU).” Add the following NOTE immediately below: “NOTE *j*—An *n* MHz PPDU has a PPDU bandwidth of *n* MHz.”, where *j* is the appropriate NOTE number, and renumber subsequent NOTEs.

Change 15.35 as follows: “**operating channel**: The operating channel is the primary channel in which beacons are transmitted.” Delete the NOTE at 15.36 and renumber subsequent NOTEs.

Make the changes indicated in the following table:

|  |  |  |
| --- | --- | --- |
| Location | Change from | To |
| 541.40 | BSS operating channel | BSS bandwidth |
| 541.43 | BSS operating channel | BSS bandwidth |
| 542.41 | BSS operating channel | BSS bandwidth |
| 543.3 | BSS operating channel | BSS bandwidth |
| 1034.18 | BSS operating channel width | BSS bandwidth |
| 1034.15 | operating channel width | BSS bandwidth |
| 1034.17 | operating channel width | BSS bandwidth |
| 1034.18 | operating channel width | BSS bandwidth |
| 1034.19 | operating channel width | BSS bandwidth |
| 1034.22 | operating channel width | BSS bandwidth |
| 1034.26 | operating channel width | BSS bandwidth |
| 1034.32 | operating channel width | BSS bandwidth |
| 1038.35 | BSS operating channel width | BSS bandwidth |
| 1038.36 | BSS operating channel width | BSS bandwidth |
| 1038.40 | BSS operating channel width | BSS bandwidth |
| 1038.41 | BSS operating channel width | BSS bandwidth |
| 1038.46 | BSS Operating Channel Width | BSS bandwidth |
| 1038.48 | BSS operating channel width | BSS bandwidth |
| 1038.50 | BSS operating channel width | BSS bandwidth |
| 1039.2 | BSS operating channel width | BSS bandwidth |
| 1039.3 | BSS operating channel width | BSS bandwidth |
| 1046.44 | BSS operating channel width | BSS bandwidth |
| 1046.43 | operating channel width | BSS bandwidth |
| 1046.44 | operating channel width | BSS bandwidth |
| 1046.45 | operating channel width | BSS bandwidth |
| 1046.46 | operating channel width | BSS bandwidth |
| 1046.47 | operating channel width | BSS bandwidth |
| 1046.50 | operating channel width | BSS bandwidth |
| 1046.54 | operating channel width | BSS bandwidth |
| 1046.60 | operating channel width | BSS bandwidth |
| 1102.12 | BSS operating channel width | BSS bandwidth |
| 1623.37 | BSS operating channel width | BSS bandwidth |
| 1683.14 | BSS operating width | BSS bandwidth |
| 1821.21 | BSS operating channel width | BSS bandwidth |
| 1821.37 | BSS operating channel width | BSS bandwidth |
| 1821.29 | BSS operating channel width | BSS bandwidth |
| 1821.59 | BSS operating channel width | BSS bandwidth |
| 1824.1 | BSS operating channel width | BSS bandwidth |
| 1824.2 | BSS operating channel width | BSS bandwidth |
| 1824.46 | BSS operating channel width | BSS bandwidth |
| 1829.57 | BSS operating channel width | BSS bandwidth |
| 1830.1 | BSS operating channel width | BSS bandwidth |
| 1830.5 | BSS operating channel width | BSS bandwidth |
| 2444.38 | BSS operating channel width | BSS bandwidth |
| 2575.30 | BSS operating channel width | BSS bandwidth |
| 2575.37 | BSS operating channel width | BSS bandwidth |
| 3321.17 | BSS operating channel widths | BSS bandwidths |
| 884.42 | BSS Channel Width | BSS Bandwidth |
| 885.1 | BSS Channel Width | BSS Bandwidth |
| 1673.35 | BSS channel width | BSS bandwidth |
| 1673.36 | BSS channel width | BSS bandwidth |
| 1682.37 | BSS channel width | BSS bandwidth |
| 1682.61 | BSS channel width | BSS bandwidth |
| 1682.63 | BSS channel width | BSS bandwidth |
| 1683.4 | BSS channel width | BSS bandwidth |
| 1683.6 | BSS channel width | BSS bandwidth |
| 1683.10 | BSS channel width | BSS bandwidth |
| 1683.21 | BSS channel width | BSS bandwidth |
| 1683.32 | BSS channel width | BSS bandwidth |
| 1683.34 | BSS channel width | BSS bandwidth |
| 1683.36 | BSS channel width | BSS bandwidth |
| 1683.37 | BSS channel width | BSS bandwidth |
| 1683.41 | BSS channel width | BSS bandwidth |
| 1683.44 | BSS channel width | BSS bandwidth |
| 1683.45 | BSS channel width | BSS bandwidth |
| 1683.48 | BSS channel width | BSS bandwidth |
| 1683.49 | BSS channel width | BSS bandwidth |
| 1683.51 | BSS channel width | BSS bandwidth |
| 1683.54 | BSS channel width | BSS bandwidth |
| 1683.59 | BSS channel width | BSS bandwidth |
| 1684.4 | BSS channel width | BSS bandwidth |
| 1684.7 | BSS channel width | BSS bandwidth |
| 1684.16 | BSS channel width | BSS bandwidth |
| 3127.29 | BSS channel width | BSS bandwidth |
| 3571.32 | BSS channel width | BSS bandwidth |
| 884.42 | BSS Width | BSS Bandwidth |
| 885.15 | BSS Width | BSS Bandwidth |
| 885.55 | BSS Width | BSS Bandwidth |
| 886.12 | BSS Width | BSS Bandwidth |
| 1674.38 | BSS width | BSS bandwith |
| 1682.35 | BSS Width | BSS Bandwidth |
| 1682.48 | BSS Width | BSS Bandwidth |
| 1683.26 | BSS Width | BSS Bandwidth |
| 1684.15 | BSS Width | BSS Bandwidth |
| 1684.32 | BSS Width | BSS Bandwidth |
| 3532.43 | BSS Width | BSS Bandwidth |
| 3532.62 | BSS Width | BSS Bandwidth |
| 3532.63 | BSS Width | BSS Bandwidth |
| 3533.3 | BSS width operation | BSS bandwidth |
| 1691.64 | the channel width of the BSS to which the TDLS peer STAs are associated | the BSS bandwidth of the BSS which the TDLS peer STAs are members of |
| 3531.32 | operating width of the BSS | BSS bandwidth |
| 717.49 | operating channel width | BSS bandwidth |
| 717.50 | operating channel width | BSS bandwidth |
| 717.52 | operating channel width | BSS bandwidth |
| 717.55 | operating channel width | BSS bandwidth |
| 717.60 | operating channel width | BSS bandwidth |
| 717.62 | operating channel width | BSS bandwidth |
| 730.29 | operating channel width | BSS bandwidth |
| 731.62 | operating channel width | BSS bandwidth |
| 737.57 | operating channel width | BSS bandwidth |
| 764.57 | operating channel width | BSS bandwidth |
| 771.19 | operating channel width | BSS bandwidth |
| 1038.55 | operating channel width | BSS bandwidth |
| 1822.1 | operating channel width | BSS bandwidth |
| 1822.6 | operating channel width | BSS bandwidth |
| 1822.10 | operating channel width | BSS bandwidth |
| 1822.35 | operating channel width | BSS bandwidth |
| 1822.39 | operating channel width | BSS bandwidth |
| 1822.42 | operating channel width | BSS bandwidth |
| 1822.45 | operating channel width | BSS bandwidth |
| 1822.47 | operating channel width | BSS bandwidth |
| 1822.48 | operating channel width | BSS bandwidth |
| 1822.51 | operating channel width | BSS bandwidth |
| 1823.31 | operating channel width | BSS bandwidth |
| 1823.35 | operating channel width | BSS bandwidth [not sure about this one] |
| 1823.46 | operating channel width | BSS bandwidth |
| 1823.54 | operating channel width | BSS bandwidth |
| 1823.59 | operating channel width | BSS bandwidth |
| 1824.3 | operating channel width | BSS bandwidth |
| 1824.5 | operating channel width | BSS bandwidth |
| 1824.9 | operating channel width | BSS bandwidth |
| 1824.16 | operating channel width | BSS bandwidth |
| 1824.21 | operating channel width | BSS bandwidth |
| 1824.30 | operating channel width | BSS bandwidth |
| 1824.35 | operating channel width | BSS bandwidth |
| 1824.41 | operating channel width | BSS bandwidth |
| 1825.1 | operating channel width | BSS bandwidth |
| 1825.44 | switches the BSS to a lower operating channel width | reduces the BSS bandwidth |
| 1830.35 | operating channel width | BSS bandwidth |
| 1830.42 | operating channel width | BSS bandwidth |
| 2443.56 | operating channel width | BSS bandwidth |
| 2443.63 | operating channel width | BSS bandwidth |
| 2444.8 | operating channel width | BSS bandwidth |
| 2444.27 | operating channel width | BSS bandwidth |
| 3310.38 | the supported channel width rather than the operating channel width. | the maximum BSS bandwidth rather than the actual BSS bandwidth |
| 3310.42 | the supported bandwidth rather than the operating channel width | the maximum BSS bandwith rather than the actual BSS bandwidth |
| 3312.35 | the supported channel width rather than the operating channel width. | the maximum BSS bandwidth rather than the actual BSS bandwidth |
| 3312.39 | the supported bandwidth rather than the operating channel width | the maximum BSS bandwith rather than the actual BSS bandwidth |
| 3316.16 | the supported channel width rather than the operating channel width. | the maximum BSS bandwidth rather than the actual BSS bandwidth |
| 3316.19 | the supported bandwidth rather than the operating channel width | the maximum BSS bandwith rather than the actual BSS bandwidth |
| 3319.39 | the supported channel width rather than the operating channel width. | the maximum BSS bandwidth rather than the actual BSS bandwidth |
| 3319.42 | the supported bandwidth rather than the operating channel width | the maximum BSS bandwith rather than the actual BSS bandwidth |
| 3320.59 | the supported channel width rather than the operating channel width. | the maximum BSS bandwidth rather than the actual BSS bandwidth |
| 3320.62 | the supported bandwidth rather than the operating channel width | the maximum BSS bandwith rather than the actual BSS bandwidth |
| 3531.29 | the current operating channel width of either the AP or the BSS | the current operating channel width of the AP or the BSS bandwidth |
| 2170.24 | spectrum | spectral |
| 2170.10 | Spectrum | Spectral |
| 2170.1 | spectrum | spectral |
| 2200.27 | spectrum | spectral |
| 2201.20 | spectrum | spectral |
| 2201.4 | Spectrum | Spectral |
| 2236.51 | spectrum | spectral |
| 2236.54 | spectrum | spectral |
| 2237.8 | Spectrum | Spectral |
| 2237.26 | spectrum | spectral |
| 2237.38 | Spectrum | Spectral |
| 2237.56 | spectrum | spectral |
| 2238.4 | Spectrum | Spectral |
| 2238.22 | spectrum | spectral |
| 2279.1 | spectrum | spectral |
| 2279.2 | spectrum | spectral |
| 2279.5 | spectrum | spectral |
| 2279.12 | spectrum | spectral |
| 2339.45 | spectrum | spectral |
| 2374.34 | Transmit mask | Transmit spectral mask |
| 2374.36 | spectrum | spectral |
| 2374.45 | transmit mask | transmit spectral mask |
| 2374.58 | Transmit mask | Transmit spectral mask |
| 2520.15 | spectrum | spectral |
| 2522.8 | spectrum | spectral |
| 2522.45 | spectrum | spectral |
| 2523.40½ | spectrum | spectral |
| 2601.9 | spectrum | spectral |
| 2602.9 (end) | spectrum | spectral |
| 2678.24 | Spectrum | Spectral |
| 2680.31 | Spectrum | Spectral |
| 2680.36 | Spectrum | Spectral |
| 2680.40 | Spectrum | Spectral |
| 2680.45 | Spectrum | Spectral |
| 2680.49 | Spectrum | Spectral |
| 2680.53 | Spectrum | Spectral |
| 2680.58 | Spectrum | Spectral |
| 3304.31 | spectrum | spectral |
| 3304.33 | spectrum | spectral |
| 3304.38 | spectrum | spectral |
| 3304.43 | spectrum | spectral |
| 3304.48 | spectrum | spectral |
| 3305.1 | Spectrum | Spectral |
| 3305.19 | Spectrum | Spectral |
| 3305.37 | Spectrum | Spectral |
| 3306.14 | Spectrum | Spectral |
| 3306.32 | spectrum | spectral |
| 2374.38 | transmit spectrum | transmitted spectrum |
| 2474.5 | transmit spectrum | transmitted spectrum |
| 2520.31 | transmit spectrum | transmitted spectrum |
| 2521.3 | transmit spectrum | transmitted spectrum |
| 2522.7 | transmit spectrum | transmitted spectrum |
| 2522.44 | transmit spectrum | transmitted spectrum |
| 2523.39 | transmit spectrum | transmitted spectrum |
| 2602.9 (start) | transmit spectrum | transmitted spectrum |
| 1685.38 | transmit mask | mask bandwidth |
| 2174.53 | transmit mask | transmit spectral mask |
| 2205.55 | transmit mask | transmit spectral mask |
| 2242.35 | transmit mask | transmit spectral mask |
| 2242.41 | Transmit mask | Transmit spectral mask |
| 2243.17 | transmit mask | transmit spectral mask |
| 2382.29 | transmit mask | transmit spectral mask |
| 2700.57 | transmit mask | transmit spectral mask |
| 3306.35 | Transmit Mask | Transmit Spectral Mask |
| 3306.38 | transmit mask | transmit spectral mask |

Delete the space before the closing paren at 2374.38.

TBD: work out where “PPDU bandwidth” should be used.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3368  Mark RISON | Some parts of the spec, namely 160.58, 165.55, 1851.20 think dot11AuthenticationAlgorithm specifies a single algorithm; while this is technically true, it's in a table which lists allows algs, so should be worded as such; 1851.61 starts off well but refers to the variable not the table | Something along the lines of "If dot11AuthenticationAlgorithm does not include the value "Open System," might be good, but probably needs "Table" or something like that |

Discussion:

The way it is structured in the MIB is that dot11AuthenticationAlgorithmsTable is a set of all the authentication algorithms supported/implemented/defined. This table has a dot11AuthenticationAlgorithm column, which identifies an authentication algorithm, and a dot11AuthenticationAlgorithmsActivated (sic) column, which says whether that authentication algorithm is activated.

Proposed changes:

Delete “(when dot11AuthenticationAlgorithm is simultaneousAuthEquals (4))” at 160.57 and 165.55.

Change 1851.20 as follows: “Any non-DMG STA requesting Open System authentication may be authenticated if dot11AuthenticationAlgorithmsTable at the ~~recipient~~peer ~~non-DMG~~ STA includes an entry with dot11AuthenticationAlgorithm equal to openSystem and dot11AuthenticationAlgorithmActivated equal to true~~is Open System authentication~~”.

Change 1851.61 as follows: “If dot11AuthenticationAlgorithmsTable does not include an entry with dot11AuthenticationAlgorithm equal to openSystem and dot11AuthenticationAlgorithmActivated equal to true,~~the value “Open System,”~~ the result code shall not take the value “successful.””

Change 2857.39 as follows (note deletion of s in dot11AuthenticationAlgorithmsIndex and dot11AuthenticationAlgorithmsActivated):

dot11AuthenticationAlgorithmsTable OBJECT-TYPE

SYNTAX SEQUENCE OF Dot11AuthenticationAlgorithmsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This (conceptual) table of attributes is a set of all the authentication

algorithms ~~supported by the stations~~ and whether they are activated. ~~The following are the default values~~

~~and the associated algorithm:~~

~~Value = 1: Open system~~

~~Value = 2: Shared key~~

~~Value = 3: Fast BSS transition (FT)~~

~~Value = 4: Simultaneous authentication of equals (SAE)~~"

REFERENCE

"IEEE Std 802.11-<year>, 8.4.1.1 (Authentication Algorithm Number field)"

::= { dot11smt 2 }

dot11AuthenticationAlgorithmsEntry OBJECT-TYPE

SYNTAX Dot11AuthenticationAlgorithmsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An Entry (conceptual row) in the Authentication Algorithms Table.

ifIndex - Each IEEE Std 802.11 interface is represented by an ifEntry.

Interface tables in this MIB module are indexed by ifIndex."

INDEX { ifIndex,

dot11AuthenticationAlgorithmsIndex }

::= { dot11AuthenticationAlgorithmsTable 1 }

Dot11AuthenticationAlgorithmsEntry ::=

SEQUENCE {

dot11AuthenticationAlgorithm~~s~~Index Unsigned32,

dot11AuthenticationAlgorithm INTEGER,

dot11AuthenticationAlgorithm~~s~~Activated TruthValue }

dot11AuthenticationAlgorithm~~s~~Index OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The auxiliary variable used to identify instances of the columnar objects

in the Authentication Algorithms Table."

::= { dot11AuthenticationAlgorithmsEntry 1 }

dot11AuthenticationAlgorithm OBJECT-TYPE

SYNTAX INTEGER {

openSystem(1),

sharedKey(2),

fastBSSTransition(3),

simultaneousAuthEquals(4) }

MAX-ACCESS read-only

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 is the authentication algorithm described by this entry in

the table. The following values can be used here

Value = 1: Open system

Value = 2: Shared key

Value = 3: Fast BSS transition (FT)

Value = 4: Simultaneous authentication of equals (SAE)

A given value shall not be used more than once." Why wasn’t the auth alg identifier made the same as the table index? Can we make this change now?

::= { dot11AuthenticationAlgorithmsEntry 2 }

dot11AuthenticationAlgorithm~~s~~Activated OBJECT-TYPE

SYNTAX TruthValue

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, when true ~~at a station~~, enables the acceptance of the

authentication algorithm described in the corresponding table entry in

authentication frames received ~~by the station~~ that have odd authentication

sequence numbers. The default value of this attribute is true when the

value of dot11AuthenticationAlgorithm is ~~Open~~ openSystem and false otherwise."

::= { dot11AuthenticationAlgorithmsEntry 3 }

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3368, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3369  Mark RISON  3.2  24.34 | "active mode" has multiple meanings in the spec, but only one of them is given in the glossary | Add the other meanings to the glossary entry |

Discussion:

The definition of “active mode” is given as:

**active mode**: A mesh power mode in which the mesh station (STA) operates in the Awake state toward a neighbor mesh STA.

Clearly this is not generic enough. (It’s also a bit odd: it suggests you can be in different power states (not modes) w.r.t. different STAs.)

Furthermore, the capitalisation of the term is all over the place, as is that of “power save mode” etc.

Proposed changes:

Change 24.34 as follows:

**active mode**: A ~~mesh power~~ mode in which ~~the mesh~~a station (STA) ~~operates~~remains in the Awake state ~~toward a neighbor mesh STA~~.

Change “VHT TXOP Power Save Mode” to “VHT TXOP power save mode” at 1031.11, 1031.12, 1031.13, 1013.15, 1031.17.

Change “VHT TXOP Power Save mode” to “VHT TXOP power save mode” at 1031.14.

Change “TDLS Peer Power Save Mode” to “TDLS peer PSM” at 888.49.

Change “TDLS Peer Power Save Mode” to “TDLS peer power save mode” at 1545.16 and 1545.19.

Change “Power Save Mode” to “PS modes” (note plural) at 1564.33.

Change “Active and Power Save Mode” to “active and PS modes” (note plural) at 1565.31.

Change “TXOP PS” to “VHT TXOP power save mode” at 1556.14.

Change “TXOP power save feature” to “VHT TXOP power save feature” at 555.43.

Change “TXOP power save mode” to “VHT TXOP power save mode” at 1556.3, 1556.7, 1556.10, 1557.5, 1557.9, 1826.5, 2442.33, 2481.54, 2573.53.

Change “TDLS Peer U-APSD” to “TDLS peer U-APSD” at 913.51.

Change “TDLS Peer PSM” to “TDLS peer PSM” at 913.54.

Change “TXOP Power Save” to “VHT TXOP power save mode” at 913.56.

Change “TXOP Power Save operation” to “VHT TXOP power save operation” at 3111.32, 3113.64.

Or should we just delete “VHT” before “TXOP power save mode”?

Change “VHT TXOP Power Save field” to “VHT TXOP PS field” at 1556.9.

Change “TXOP Power Saving” to “VHT TXOP power saving” at 2795.46, 2807.10.

Change “TDLS Peer U-APSD” to “TDLS peer U-APSD” at 305.1, 305.6, 305.41, 306.7, 306.46, 306.49, 307.23, 307.59, 307.62, 820.24 (leftmost), 1143.49, 1548.1, 1548.15 (twice), 1548.23, 1691.34, 2748.42, 2843.34.

Change “TDLS Peer U-APSD Buffer STA Support” to “TPU Buffer STA Support” at 820.21 (twice), 820.25, 820.26, 1548.9.

Change “TDLS Peer U-APSD Buffer STA” to “TPU buffer STA” at 820.22, 1548.6, 1548.11.

Change “TDLS Peer U-APSD Behavior” to “TDLS peer U-APSD behavior” at 1548.43, 1549.29.

Change “TDLS Peer PSM” to “TDLS peer PSM” at 312.1, 312.6, 312.7, 312.41, 313.7 (rightmost), 313.47, 314.24 (rightmost), 314.62 (rightmost), 820.29, 820.31, 1545.20, 1545.26 (twice), 1545.29 (twice), 1545.30, 1545.32 (twice), 1545.38, 1545.41 (twice), 1545.60, 1546.15, 1546.21 (rightmost), 1546.27 (rightmost), 1546.38, 1546.39, 1546.40, 1546.44, 1546.52, 1546.63, 1547.29, 1547.33, 1547.37, 1547.40, 1547.48, 1691.33, 1700.7, 2748.21, 2843.44.

Change “TPU Sleep STA” to “TPU sleep STA” at 1548.15.

Globally replace “WNM-Sleep mode” with “WNM-sleep mode” (about 41 instances, including cross-references).

Globally replace “WNM-Sleep Mode” with “WNM-sleep mode” when not immediately followed by “element”, “Element”, “Request”, “Response”, “subelement”, “GTK subelement”, “IGTK subelement”, “field” and where not at 819.40 (leftmost).

Ditto for “TIM Broadcast”.

Globally replace “Active mode” with “active mode” except at 1533.9, 1562.30, 2141.39, 2142.10 (about 24 – 4 instances, including cross-references).

Change “Active Mode or Power Saving” to “active mode or PS mode” at 3551.47.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3369, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3370  Mark RISON | What is the point of saying "-compliant"? (11 instances) | Delete throughout (also at places where the hyphen is missing, e.g. 548.15, 1856.44, 2235.45, 2238.27, 2373.48, 2378.27, 3303.58) |

Discussion:

It is implicit that devices are compliant (syn. conformant). Devices which are not compliant are not IEEE Std 802.11 devices and are outside the scope of IEEE Std 802.11. A single reference to compliance in subclause 1.3 is sufficient.

Note that compliant developers have been dealt with under CID 3159.

Proposed changes:

Change 1.58 as follows:

Specifically, in the context of IEEE Std 802.11™-compliant devices, this standard

— Describes the functions and services required by a~~n IEEE Std 802.11™-compliant~~ device to operate within independent, personal, and infrastructure networks as well as the aspects of ~~STA~~device mobility (transition) within those networks.

— Describes the functions and services that allow a~~n IEEE Std 802.11-compliant~~ device to communicate directly with another such device outside of an independent or infrastructure network.

— Defines the MAC procedures to support the MAC service data unit (MSDU) delivery services.

— Defines several PHY signaling techniques and interface functions that are controlled by the ~~IEEE 802.11~~ MAC.

— Permits the operation of a~~n IEEE Std 802.11-conformant~~ device within a wireless local area network (WLAN) that ~~may~~ coexists with multiple overlapping IEEE Std 802.11 WLANs.

— Describes the requirements and procedures to provide data confidentiality of user information and MAC management information being transferred over the wireless medium (WM) and authentication of ~~IEEE Std 802.11-conformant~~ devices.

— Defines mechanisms for dynamic frequency selection (DFS) and transmit power control (TPC) that may be used to satisfy regulatory requirements for operation in any band.

— Defines the MAC procedures to support local area network (LAN) applications with quality-of-service (QoS) requirements, including the transport of voice, audio, and video.

— Defines mechanisms and services for wireless network management of ~~STA~~devices that include BSS transition management, channel usage and coexistence, collocated interference reporting, diagnostic, multicast diagnostic and event reporting, flexible multicast, efficient beacon mechanisms, proxy ARP advertisement, location, timing measurement, directed multicast, extended sleep modes, traffic filtering, and management notification.

— Defines functions and procedures aiding network discovery and selection by ~~STA~~devices, information transfer from external networks using QoS mapping, and a general mechanism for the provision of emergency services.

— Defines the MAC procedures that are necessary for wireless multi-hop communication to support wireless LAN mesh topologies.

— Defines medium access control mechanisms to support the prioritization of Management frames.

— Defines mechanisms to improve audio video (AV) streaming ~~quality of service (~~QoS~~)~~ while maintaining data and voice performance.

— Defines the PHY signaling, MAC, and beamforming procedures required for operation with directional antenna patterns.

Change 103.26 as follows: “A~~n IEEE Std 802.11-compliant~~ STA can receive like-PHY ~~IEEE Std 802.11~~ traffic that is within range and can transmit to any other ~~IEEE Std 802.11~~ STA within range.” Add “like-PHY” to the transmit bit?

Change 2180.61 as follows: “~~IEEE Std 802.11-compliant device shall set the values of the bits~~ B0, B1, B3, B4, B5, and B6 are reserved and shall be set to 0.”

Delete “-compliant” at 2175.36, 2254.29, 2206.46. Delete the rightmost “ERP” at 2254.29.

Delete “compliant” at 548.15, 1856.44, 2235.45 (fix the article immediately before), 2378.27.

Change 1873.48 as follows: “A DMG RSNA STA~~s claiming RSNA compliance~~ shall support GCMP.” Why is this not in the GCMP clause, like the equivalent statement for CCMP is? Why is a specific strength of GCMP not mentioned, like it is for CCMP?

Change 1888.56 as follows: “~~In order to be compliant with RSN a~~A non-DMG RSNA STA shall support CCMP-128.”

Change 2173.46 as follows: “~~A vendor DSSS PHY implementation shall be compliant if f~~For all n =1000 samples, the following condition ~~is~~shall be met:” (note inserted comma).

Change 2204.50 as follows: “~~A vendor high rate PHY implementation shall be compliant if f~~For all n = 1000 samples, the following condition ~~is~~shall be met:”.

Delete “from compliant devices” at 2238.27, 3303.58.

Change 2373.23 as follows: “~~STAs compliant with the physical layer defined in Clause 21 (Directional multi-gigabit (DMG) PHY specification)~~The DMG PHY operates”.

Change “conforming to”/“conformant to” to “compliant with” at 28.30, 32.9, 34.57, 1259.9, 1886.44.

Change “conform to”/“conform with” to “comply with” at 1259.12, 1331.50, 1446.14, 2058.19, 2130.51, 2131.46, 2146.31, 2146.44, 2168.57, 2170.51, 2202.24, 2236.25, 2238.27, 2261.26, 2339.26, 2341.52, 2622.19. 2622.27, 2624.44, 2626.54, 3303.58.

Is “Protocol Implementation Conformance Statement” some kind of standard term, or can we change it to “Protocol Implementation Compliance Statement”?

Change “conforms with” to “complies with” at 2227.50.

Change “conformance” to “compliance” at 843.45, 2622.39, 2665.37, 2665.61, 2694.50, 2695.14, 3252.56, 3258.31.

Change “Conformance” to “Compliance” at 3252.47.

Change “Conformance to” to “Compliance with” at 2175.36, 2206.45.

Change “conforms” to “shall comply with” at 2199.35.

Delete “conformant” at 62.44, 95.52 (and add “the” before “SS” afterwards), 1857.3.

Change “conformant OFDM signal” to “signal compliant with the OFDM PHY” at 2242.27, 2242.35, 2243.8, 2243.16.

Change “a conformant OFDM PHY” to “an OFDM PHY” at 2242.28.

Change “a conformed OFDM PHY” to “an OFDM PHY” at 2243.9.

Change “conformant OFDM signal” to “signal compliant with the ERP” at 2263.4.

Change “an OFDM PHY” to “an ERP” at 2263.6.

Change “OFDM PHY” to “HT PHY” at 2339.26.

Change “conformant OFDM signal” to “signal compliant with the HT PHY” at 2346.41, 2347.4.

Change “a conforming OFDM PHY” to “an HT PHY” at 2346.42, 2347.5.

Change “conformant OFDM signal” to “signal compliant with the VHT PHY” at 2530.1, 2531.10.

Change “a conforming OFDM PHY” to “a VHT PHY” at 2530.2, 2531.11.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3370, which address the issue raised by the commenter. See also the resolution of CID 3159.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3390  Mark RISON  9.22.2.8  1315.57 | "3) A VHT MU PPDU carrying A-MPDUs to different users" -- wording is unclear | Change to "3) A VHT MU PPDU carrying single A-MPDUs to different users", matching 2) above |

Discussion:

The commenter proposes changing bullet 3) of:

1. One of the following at any rate, subject to the rules in 9.7 (Multirate support)
   1. SU PPDUs carrying fragments of a single MSDU or MMPDU
   2. An SU PPDU or a VHT MU PPDU carrying a single MSDU, a single MMPDU, a single A-MSDU, or a single A-MPDU
   3. A VHT MU PPDU carrying A-MPDUs to different users
   4. A QoS Null frame or PS-Poll frame

to:

1. One of the following at any rate, subject to the rules in 9.7 (Multirate support)
   1. SU PPDUs carrying fragments of a single MSDU or MMPDU
   2. An SU PPDU or a VHT MU PPDU carrying a single MSDU, a single MMPDU, a single A-MSDU, or a single A-MPDU
   3. A VHT MU PPDU carrying single A-MPDUs to different users
   4. A QoS Null frame or PS-Poll frame

by analogy with the “a single A-MPDU” in the line above, and to avoid any suggestion that a given A‑MPDU can be to different users. There is a possible question about whether VHT single MPDU might be mis-understood, but “a single A-MPDU” already appears in 2) and in 2 other locations, so this is probably an unwarranted concern.

Proposed resolution:

ACCEPTED

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3483  Mark RISON  8.4.2.26  823.6 | "Max Number Of MSDUs In A-MSDU" only applies to VHT STAs | Add "VHT" before (also at 1295.42) |

Discussion:

In general, new features need to be restricted to new devices. It has been suggested that the intention might have been to permit its use by pre-VHT devices, on the basis that otherwise this field would most likely have been defined in the VHT Capabilities element. However, it could only be used by pre-VHT devices if there were signalling to indicate whether a given pre-VHT device supports restricting its A‑MSDU transmissions, which there isn’t. The best one can do is an earnest plea to HT transmitters. What about DMG transmitters?

Proposed changes:

Change 823.6 as follows:

Indicates the maximum number of MSDUs in an A-MSDU that the STA is able to receive from a VHT STA:

Change 823.12 as follows:

Reserved~~,~~ if A-MSDU is not supported or if the STA is not an HT STA.

Change 1295.41 as follows:

A VHT STA shall not transmit ~~to a recipient VHT STA~~ an A-MSDU that includes a number of MSDUs greater than the value indicated by the Max Number ~~o~~Of MSDUs ~~i~~In A-MSDU field in ~~the~~any Extended Capabilities element ~~received from~~sent by the recipient STA. An HT STA should not transmit an A-MSDU that includes a number of MSDUs greater than the value indicated by the Max Number Of MSDUs In A-MSDU field in any Extended Capabilities element sent by the recipient STA.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3483, which allow opportunistic use of this feature by HT STAs.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3444  Mark RISON | "N\_KEY" (4 instances) | "X" or "Z" is the preferred form |

Discussion:

The output length of a KDF invocation is sometimes dependent on the context. In this case a “variable” is used to refer to it:

1858.47: *pwd*-*value* = KDF-z(*pwd*-*seed*, “SAE Hunting and Pecking”, *p*)

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

1937.58: R0-Key-Data = KDF-Hash-Z(XXKey, "FT-R0", SSIDlength || SSID || MDID || R0KHlength ||

1938.54: PMK-R1 = KDF-Hash-Z(PMK-R0, "FT-R1", R1KH-ID || S1KH-ID)

1939.23: PTK = KDF-Hash-PTKLen(PMK-R1, "FT-PTK", SNonce || ANonce || BSSID || STA-ADDR)

1975.40: TPK = KDF-N\_KEY(TPK-Key-Input, "TDLS PMK", min (MAC\_I, MAC\_R)

2082.7: MTK ← KDF-X(PMK, “Temporal Key Derivation”, min(localNonce, peerNonce) ||

The “–X” form is also used for various PRF invocations.

It would be desirable to consistently use one name for the “variable”. “X” seems a reasonable choice, given there is no clear winner for KDFs and there is for PRFs. The alternative would be “Length”, per 1937.28.

Note there is a separate issue that a KDF invocation needs a hash to be specified as well as an output length, so the instances of “KDF-z”, “KDF-N\_KEY” and “KDF-X” shown above (which all become “KDF-X”) are underspecified (this also applies to instances of “KDF-256” and “KDF-512”). This is outside the scope of this comment and its resolution, however.

Proposed resolution:

Change “*z*” to “X” (not italic) at 1858.42, 1858.47, 1861.4, 1861.9.

Change “Z” to “X” at 1937.58 and on page 1938 (all 9 instances).

Change “PTKLen” to “X” at 1939.23, 1939.27, 1939.28, 1940.10.

Change “PTKlen” to “X” at 1939.41.

Change “N\_KEY” to “X” at 1975.40, 1975.45, 1975.48, 1976.7.

**References:**

802.11mc/D3.0