IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some MAC, PICS and security comments on 11mc/D3.0 (LB202) | | | | |
| Date: 2015-01-14 | | | | |
| 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, 3211, 3212, 3213, 3226, 3313, 3314, 3318, 3323, 3324, 3345, 3355, 3359, 3360, 3365, 3368, 3369, 3370, 3374, 3377, 3382, 3386, 3390, 3393, 3430, 3431, 3440, 3462, 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-lxen” 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.

r8: Updated prior to Atlanta F2F. Added MAC CID 3211.

r9: Updated prior to Atlanta F2F.

r10: Updated prior to and during Atlanta F2F. Added MAC CIDs 3226, 3393, 3430, 3462, 3523.

r11: Updated during Atlanta F2F.

|  |  |  |
| --- | --- | --- |
| 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 (note to the editor: format the two NOTEs to be distinctive):

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

1. for an uplink TS, it

* is included in dot11SupportedDataRatesTxTable and in the AP’s operational rate set, or
* corresponds to an HT MCS included in dot11HTSupportedMCSTxTable, if present, and in the AP’s operational HT MCS set, if defined, at a bandwidth and guard interval supported by the non-AP STA on transmission and permitted in the BSS, or
* corresponds to a VHT-MCS and NSS for which support is indicated in the Tx VHT-MCS Map subfield in the VHT Operation parameter of the MLME-(RE)ASSOCIATE.request primitive, if present, and in the AP’s operational VHT-MCS and NSS set, if defined, at a bandwidth and guard interval supported by the non-AP STA on transmission and permitted in the BSS~~, for an uplink TS.~~

1. for a downlink TS, it

* is ~~in the non-AP STA’s operational rate set~~included in the OperationalRateSet parameter of the MLME-JOIN.request primitive and supported by the AP on transmission, or

NOTE—How a non-AP STA determines an AP’s non-HT rate transmission support is implementation dependent. The non-AP STA might conservatively use the BSS basic rate set, or it might use knowledge of past transmissions by the AP, or it might use other means.

* corresponds to an HT MCS included in dot11HTSupportedMCSRxTable, if present, and supported by the AP on transmission, at a bandwidth and guard interval supported by the non-AP STA on reception and permitted in the BSS, or

NOTE—How a non-AP STA determines an AP’s HT MCS transmission support, if the Tx MCS Set subfield in the HT Capabilities element advertised by the AP is equal to 0 or if the Tx Rx MCS Set Not Equal subfield in that element is equal to 1, is implementation dependent. The non-AP STA might conservatively use the BSS basic HT MCS set, or it might use knowledge of past transmissions by the AP, or it might use other means.

* corresponds to a VHT-MCS and NSS for which support is indicated in the Rx VHT-MCS Map subfield in the VHT Operation parameter of the MLME-(RE)ASSOCIATE.request primitive, if present, and in the Tx VHT-MCS Map subfield of the VHT Operation element advertised by the AP, if present, at a bandwidth and guard interval supported by the non-AP STA on reception and permitted in the BSS~~, for a downlink TS.~~

1. for a bidirectional TS, it satisfies both a) and b) above~~it is in both the AP’s operational rate set and non-AP STA’s operational rate set, for a bidirectional TS.~~

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

Change 2823.19 as follows: “This attribute specifies the set of non-HT data rates at which the station ~~may transmit~~is able to receive data.”

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 that 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 Table 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 (“implies”) for TXOP Limit 0 in QoS (+)CF-Polls
* There is a bogus spelling: “dot11EDCAQAPTableTXOPLimit” (should be QAPEDCA)
* The units in the MIB are not clear (µs or 32 μs?)
* 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)
* Numbers in the MIB are likely to rot (see e.g. CID 3776); a cross-reference would be more robust

Proposed changes:

Change 580.58 as follows:

*TTXOP* is the ~~value of~~duration given by dot11EDCATableTXOPLimit (dot11~~EDCA~~QAPEDCATableTXOPLimit for the AP) for that AC

Change 3145.11 as follows (note deletion of “QAP”; make the Table reference a cross-reference which will update if the table numbers change; ditto the Subclause reference):

dot11EDCATableTXOPLimit OBJECT-TYPE

SYNTAX Unsigned32 (0..65535)

UNITS "32 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~~ element.

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum ~~number of microseconds~~duration of an EDCA

TXOP for a given AC, for a non-AP non-OCB STA. The default value for this attribute is given (in different units) in Table 8-144.

~~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.~~"

REFERENCE "IEEE Std 802.11-<year>, 8.4.2.28 (EDCA Parameter Set element)"

::= { dot11EDCAEntry 5 }

Change 3147.59 as follows (make the Table reference a cross-reference which will update if the table numbers change; ditto the Subclause reference):

dot11QAPEDCATableTXOPLimit OBJECT-TYPE

SYNTAX Unsigned32 (0..65535)

UNITS "32 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~~duration of an EDCA

TXOP for a given AC ~~at the~~, for an AP. The default value for this attribute is given (in different units) in Table 8-144.

~~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.~~"

REFERENCE "IEEE Std 802.11-<year>, 8.4.2.28 (EDCA Parameter Set element)"

::= { dot11QAPEDCAEntry 5 }

Also:

* 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 “dot11QAPEDCACWmin and dot11QAPEDCACWmax” to “dot11QAPEDCATableCWmin and dot11QAPEDCATableCWmax” at 1226.24
* change “dot11QAPEDCATXOPLimit” to “dot11QAPEDCATableTXOPLimit” at 1226.38
* 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.”

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, which address the issue raised by the commenter.

Proposed resolution for CID 3433:

REVISED

Rather than deleting “irretrievably”, replace “destroyed” with “deleted”.

|  |  |  |
| --- | --- | --- |
| 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 [but subsequently superseded by a resolution in 14/1345]

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.

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 or dot11ExtendedSpectrumManagementImplemented is true;

Change 616.47 as follows:

The Channel Switch Wrapper element is optionally present if dot11VHTOptionImplemented 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 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 is false, and sets it to 0 otherwise.  Editor’s note: The <ANA+1> flag will be replaced by a number assigned by the 802.11 ANA. |

Insert at 1304.58:

The following, and only the following, are extended spectrum management capable: a VHT STA and a STA that has dot11ExtendedSpectrumManagementImplemented true. A non-VHT 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 indicate 80+80 bandwidth and the same center frequency of segment 0 as the Operating Class and Channel Number fields); 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. [actually, I don’t think after all that this is restricted to dot11OperatingClassesImplemented being true, since it is not part of the list introduced by “When dot11OperatingClassesImplemented is true, the following statements apply:”, so I think that’s 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 only the VHT Transmit Power Envelope element ~~only~~, not the Power Constraint element, 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.

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 station implementation is capable of supporting extended spectrum management. The capability is disabled at the non-VHT station otherwise."

DEFVAL { false }

::= { dot11StationConfigEntry 24 }

For reference, here is a PICS CF key:

|  |  |
| --- | --- |
| CF1 | AP |
| CF2.1 | Non-AP STA in infrastructure BSS |
| CF2.2 | IBSS STA |
| CF10 | Spectrum management |
| CF15 | 3.65–3.70 GHz band |
| CF29 | VHT |
| CF30 | TVWS |

Add the following entry to the PICS:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \*CF32 | Extended spectrum management | 9.21.3 | O  CF29 OR CF30:M | Yes  No  |

Make the following changes in the PICS

SM20.4 Transmission of Wide Bandwidth Channel Switch element in Channel Announcement frame and transmission of Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated channel switching procedure by an AP

~~(CF1 AND CF10 AND CF29):M~~

(CF1 AND CF10 AND CF3~~0~~2):M

SM20.5 Transmission of Wide Bandwidth Channel Switch element in Channel Announcement frame and transmission of Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated channel switching procedure by a STA.

~~(CF2.2 AND CF10 AND CF29):M~~

(CF2.2 AND CF10 AND CF3~~0~~2):M

SM20.6 Reception of Wide Bandwidth Channel Switch element in Channel Announcement frame and reception of Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated channel switching procedure by a STA.

~~(CF10 AND CF29):M~~

(CF10 AND CF3~~0~~2):M

SM20.7 Transmission of New VHT Transmit Power Envelope element in Channel Announcement frame and transmission of New VHT Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and

associated channel switching procedure by an AP.

~~(CF1 AND CF10 AND CF29):M~~

(CF1 AND CF10 AND CF3~~0~~2):M

SM20.8 Transmission of New VHT Transmit Power Envelope element in Channel Announcement frame and transmission of New VHT Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and

associated channel switching procedure by a STA.

~~(CF2.2 AND CF10 AND CF29):M~~

(CF2.2 AND CF10 AND CF3~~0~~2):M

SM20.9 Reception of New VHT Transmit Power Envelope element in Channel Announcement frame and reception of New VHT

Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated channel switching procedure by a STA.

~~(CF10 AND CF29):M~~

(CF10 AND CF3~~0~~2):M

DSE5 STA association procedure

Transmission of Association Request frame with Supported Operating Classes element by a STA

(CF15 AND CF2.1):M

Transmission of Association Response frame with Supported Operating Classes element by an AP

(CF15 AND CF1):M

DSE6 STA reassociation procedure

Transmission of Reassociation Request frame with Supported Operating Classes element by a STA

(CF15 AND CF2.1):M

Transmission of Reassociation Response frame with Supported Operating Classes element by an AP

(CF15 AND CF1):M

DSE9.4 Transmission of Wide Bandwidth Channel Switch element in Extended Channel Announcement frame and transmission of Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by an AP.

~~(CF1 AND CF29):M~~

(CF1 AND CF3~~0~~2):M

DSE9.5 Transmission of Wide Bandwidth Channel Switch element in Extended Channel Announcement frame and transmission of Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by a STA.

~~(CF2.2 AND CF29):M~~

(CF2.2 AND CF3~~0~~2):M

DSE9.6 Reception of Wide Bandwidth Channel Switch element in Extended Channel Announcement frame and reception of

Wide Bandwidth Channel Switch subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by a STA.

~~CF29:M~~

CF3~~0~~2:M

DSE9.7 Transmission of New VHT Transmit Power Envelope element in Extended Channel Announcement frame and transmission of New VHT Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by an AP.

~~(CF1 AND CF29):M~~

(CF1 AND CF3~~0~~2):M

DSE9.8 Transmission of New VHT Transmit Power Envelope element in Extended Channel Announcement frame and transmission of New VHT Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by a STA.

~~(CF2.2 AND CF29):M~~

(CF2.2 AND CF3~~0~~2):M

DSE9.9 Reception of New VHT Transmit Power Envelope element in Extended Channel Announcement frame and reception of New VHT Transmit Power Envelope subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and

associated extended channel switching procedure by a STA.

~~CF29:M~~

CF3~~0~~2:M

DSE9.10 Transmission of New Country element in Extended Channel Announcement frame and transmission of New

Country subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by an AP.

~~(CF1 AND CF29):M~~

(CF1 AND CF3~~0~~2):M

DSE9.11 Transmission of New Country element in Extended Channel Announcement frame and transmission of New

Country subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated

extended channel switching procedure by a STA.

~~(CF2.2 AND CF29):M~~

(CF2.2 AND CF3~~0~~2):M

DSE9.12 Reception of New Country element in Extended Channel Announcement frame and reception of New Country

subelement in Channel Switch Wrapper element in Beacon/Probe Response frames, and associated extended channel switching procedure by a STA.

~~CF29:M~~

CF3~~0~~2:M

SM1.1 VHT Transmit Envelope element(s) in Beacon and Probe Response frames

~~CF10 AND CF29:M~~

CF10 AND CF3~~0~~2:M

MD13 Reserved First Channel Number

CF15:M

MD14 Reserved Operating Class

CF15:M

MD15 Operation with operating classes

Multiple classes in Country element

CF15:M

Multiple classes in Association and Reassociation frames

CF15:M

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 (0.002%). 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:

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: “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.”.

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~~ *~~T~~~~space~~* ~~= 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*

)

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. Change “Standard” to “standard” at 3.1 and 63.32.

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.

Note the following should in principle be done, but they are in deprecated material (TKIP):

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.”

Proposed changes:

At 2.51 change “Mathematical usage” to “Terminology for mathematical, logical and bit operations”.

*C Boolean 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/C Boolean OR (||)*

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.”

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 on x and y being numbers 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 1767.21 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*, *N*) is bits *F* to *F*+*N*–1 of the bit string *S* starting from the left, using the IEEE Std 802.11 bit conventions from 8.2.2 (Conventions).”

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 deleted.”.

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

***[Note to editor: the resolution for CID 3432 et al.includes changes which move Truncate-128() around; that part should be ignored and the changes indicated here for Truncate-128() should be effected.]***

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CIDs 3431 and 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):

*My suggestion is to explicitly state that the units in each case are Hz (or MHz if you prefer). I say this because, as you know, many people informally use "bandwidth" to refer to the number of bits/second, bytes/second, or packets/second consumed. That's not a correct usage of bandwidth, but including an explicit statement that these definitions are measured in Hz might help.*

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.

Alternative terminology: “PPDU channel width”, “BSS channel width”, “mask width”?

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 that 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.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3386.

|  |  |  |
| --- | --- | --- |
| 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~~can 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 to the editor: 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."

::= { 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: not only mesh STAs operate in “active mode”.

Furthermore, it is abundantly clear from examination of the standard that awake/doze states are states of the STA as a whole, not of the relationship of the STA to another STA, so talking of operating in a given power state towards a peer does not make sense. The definitions of the two mesh sleep modes are similarly afflicted:

**deep sleep mode**: A mesh power mode in which the mesh station (STA) operates either in the Awake state or in the Doze state toward a neighbor mesh STA, and is not expected to receive beacons from this neighbor mesh STA.

**light sleep mode**: A mesh power mode in which the mesh station (STA) operates either in the Awake state or in the Doze state toward a neighbor mesh STA, and is expected to receive beacons from this neighbor peer mesh STA.

However these definitions can be fixed simply by rewording so that “toward a neighbor mesh STA” pertains to the mode not the state. A mesh STA in active mode is in awake state and hence can receive any frame from a peer mesh STA, while a mesh STA in deep sleep mode might be in doze state and hence not be able to receive a frame from a peer mesh STA. A mesh STA in light sleep mode is similar to one in deep sleep mode, except that it undertakes to be in awake state when a beacon is expected from a peer mesh STA, so that it can receive that.

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

For reference, here are the definitions of the power states and modes for various flavours of network:

**10.2.2 Power management in a non-DMG infrastructure network**

A STA may be in one of two different power states:

— *Awake*: STA is fully powered.

— *Doze*: STA is not able to transmit or receive and consumes very low power.

|  |  |
| --- | --- |
| Active mode or AM | STA receives and transmits frames at any time. The STA remains in the Awake state. |
| Power save mode or PS | STA enters the Awake state to receive or transmit frames. The STA remains in the Doze state otherwise. STA and AP procedures for power-save are described in 10.2.2 (Power management in a non-DMG infrastructure network). |

**10.2.6 Power management in a PBSS and DMG infrastructure BSS**

A STA may operate in one of two power states:

— Awake: STA is fully powered.

— Doze: STA is not able to transmit or receive and consumes very low power.

The manner in which a STA transitions between these two power states shall be determined by the STA’s Power Management mode:

— Active mode: A STA is in the Awake state, except that the STA can switch to Doze state in an Awake BI when the STA is allowed to doze as indicated in Table 10-3 (Power management states for an Awake BI).

— Power Save (PS) mode: A STA alternates between the Awake and the Doze states, as determined by the rules defined in this subclause.

**13.14.2.2 Peer-specific mesh power modes**

The peer-specific mesh power modes are defined as follows:

— *Active mode*: The mesh STA shall be in Awake state all the time.

— *Light sleep mode*: The mesh STA alternates between Awake and Doze states, as specified in 13.14.8.4 (Operation in light sleep mode for a mesh peering). The mesh STA shall listen to all the Beacon frames from the corresponding peer mesh STA.

— *Deep sleep mode*: The mesh STA alternates between Awake and Doze states, as specified in 13.14.8.5 (Operation in deep sleep mode for a mesh peering). The mesh STA may choose not to listen to the Beacon frames from the corresponding peer mesh STA.

Proposed changes:

Change 24.34 as follows:

**active mode**: A power management mode in which a non-mesh station (STA) remains in the awake state, and a mesh power mode with respect to a neighbor peer mesh STA in which ~~the~~a mesh station ~~(STA)~~ ~~operates~~remains in the ~~A~~awake state ~~toward a neighbor mesh STA~~ and is expected to receive frames from this neighbour peer mesh STA.

Change 26.26 as follows:

**deep sleep mode**: A mesh power mode with respect to a neighbor peer mesh STA in which ~~the~~a mesh station (STA) ~~operates either in the Awake state or in the Doze state~~ alternates between awake and doze states ~~toward a neighbor mesh STA,~~ and is not expected to receive beacons from this neighbor peer mesh STA.

Change 32.38 as follows:

**light sleep mode**: A mesh power mode with respect to a neighbor peer mesh STA in which ~~the~~a mesh station (STA) ~~operates either in the Awake state or in the Doze state~~ alternates between awake and doze states ~~toward a neighbor mesh STA,~~ and is expected to receive beacons from this neighbor peer mesh STA.

Add at 38.43 the following:

**power save (PS) mode**: A power management mode in which a non-mesh station (STA) alternates between awake and doze states.

Change “VHT TXOP Power Save Mode” to “VHT TXOP power save mode” at 1031.12.

Change “TXOP Power Save Mode” to “VHT TXOP power save mode” (note addition of “VHT”) at 1031.11, 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.

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).

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

Globally replace “SUCCESS\_STA\_IN\_DOZE\_MODE” with “SUCCESS\_STA\_IN\_PS\_MODE” (5 instances).

Globally replace “doze mode” with “doze state” (4 instances).

Change “Doze State” to “doze state” at 1538.41.

Globally replace “Doze state” with “doze state” and “Awake state” with “awake state” (about 67 instances of each, including cross-references; note to editor: I have not found any locations where this would not be valid, e.g. at the start of a sentence or cell, but worth being on the lookout just in case!).

Change “Awake” to “awake” at 1024.38, 1559.25, 1562.34, 2141.40, 2141.44.

Change “awake” to “in awake state” at 1446.32.

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~~ receives ~~like-PHY IEEE Std 802.11~~ traffic that is within range and ~~can~~ transmits to any other ~~IEEE Std 802.11~~ STA within range.”

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.”

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 to the editor: 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.

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 OFDM PHY” at 2263.4.

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

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

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.

However, this is still not clear enough.

Proposed resolution:

REVISED

Add after “carrying A-MPDUs to different users” “(a single A-MPDU to each user)”.

|  |  |  |
| --- | --- | --- |
| 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 or PRF 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*)

1931.11: PRF - X(PMK, “Pairwise key expansion”,

1931.62: PTK ← PRF-X(PMK, “Pairwise key expansion”, Min(AA,SPA) || Max(AA,SPA) ||

1933.29: PRF -X(GMK, “Group key expansion”, AA || GNonce)

1933.54: GTK ← PRF-X(GMK, “Group key expansion” || AA || GNonce)

1934.35: PRF-X(SMK, “Peer key expansion”,

1934.61: STK ← PRF-X(SMK, "Peer key expansion", Min(MAC\_I,MAC\_P) || Max(MAC\_I,MAC\_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)

1961.6: PTK ← PRF-X(PMK, “Pairwise key expansion” || Min(AA,SPA) || Max(AA,SPA) ||

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) ||

It would be desirable to consistently use one name for the “variable”. “Length” seems a reasonable choice, 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-Length”) 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:

REVISED

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

Change “X” to “Length” at 1931.11, 1931.19, 1931.62, 1932.1, 1933.29, 1933.37, 1933.54, 1933.56, 1934.35, 1934.41, 1934.61, 1935.1, 1961.6, 2082.7, 2082.13.

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

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

Change “PTKlen” to “Length” at 1939.41.

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

Remove the spaces in “PRF - X” at 1931.11 and in “PRF -X” at 1933.29.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3211  George Vlantis  20.4.4  2361.16 | aMPDUMaxLength is not defined in Table 20-25 (nor wasn't it defined in the 802.11n amendment). So what is the maximum length of an un-aggregated MPDU for the HT PHY? In Clause 16, 17, 18, and 19 this parameter is defined in the PHY characteristics table. For 802.11a and 802.11g the value is 4096 octets. However, the dot11FragmentationThreshold MIB variable limits the longest transmission to be 2346, originally for both PHYs, under the rules of Clause 9, but this was later changed to be 3000 octets in 802.11REVmb, and changed again in 802.11n to 8000 octets. With this last increase to dot11FragmentationThreshold, aMPDUMaxLength = 4096 octets became the effective limit for these two PHYs.  Now, in 802.11n, aMPUDMaxLength was not defined in the HT PHY parameters, although it is still required as one of the parameters in the initialization of the PHY primitive. aPSDUMaxLength = 65536, and the aPPDUMaxTime = 10ms were added, and the configurable dot11MaxAMSDUlength MIB variable = either 7935 or 3839 (default) was added. These 3 parameters, together, do limit the PHY transmission in both the aggregated and unaggregated cases, but then the default value for dot11FragmentationThreshold, which becomes the limit of an unaggregate packet, is ill-defined because aMPDUMaxLength is undefined for the Clause 20 HT PHY. All that is really known is that 8000 octets is the upper limit for dot11Fragmentation Threshold. (See the last sentence of the description of dot11FragmentationThreshold on page 3120, line 57, which gives the equation for calculating dot11FragmentationThreshold as a function of aMPDUMaxLength.) | Define aMPDUMaxLength for the HT PHY. In this way, the length of the maximum unaggregated MPDU (and the default maximum fragment as defined by the value of dot11FragmentationThreshold in the MIB) will be well-defined, as well as the parameter to the PHY initialization.  (Sorry for not finding this in REVmb or earlier ballots of REVmc.) |

Discussion:

It is true that aMPDUMaxLength is not defined in Clause 20. Nor is it defined in subsequent clauses, in fact.

However, as Table 8-19 in Subclause 8.2.4.7.1 shows at 575.30, the maximum MPDU size for HT PPDUs is indirectly constrained by the maximum A-MSDU size, which as the commenter observes, is advertised in dot11MaxAMSDULength (it is not configurable; it’s a capability variable; note it actually only gives the max rx length when in an HT PPDU (though it should also apply when in a pre-HT PPDU, and there are restrictions in A-MPDUs, I think)).

It is important to understand that dot11FragmentationThreshold does not define the MTU, as it is generally understood in Internet terms, i.e. the maximum packet size which will get through the network. It merely defines the size beyond which certain packets will in some circumstances (there is a large list of exceptions, one of which (no fragmentation of A-MSDUs) has been forgotten) be fragmented. The MTU is probably best thought of as being defined by the maximum MSDU size, which is 2304 octets for all PHYs except DMG (ibid.). This value is not exposed through the MIB. Perhaps it should be, modelled on dot11MaxAMSDULength (i.e. a capability variable, the allowed values being for 7920 octets (for DMG) and 2304 octets (for everything else))?

[dot11FragmentationThreshold does not define the MinTU either, since might have to fragment apparently small enough MSDUs, e.g. to meet a TXOP Limit constraint. It ends up just saying “if it gets this big, you must fragment (err, except in this big list of cases where you don't)”. The default value, 11500, effectively means “no requirement to fragment”, since it is greater than the maximum MPDU size for any PHY.]

In any case, aMPDUMaxLength isn’t something which a PHY should be defining. A PHY should define things within its domain, e.g. aPSDUMaxLength. (See also the explicit special justification for aMACProcessingDelay at 522.58.)

Proposed changes:

Change 3120.38 as follows (ignore the colouring, which is merely there to show how some things have just been moved around/deduplicated, but not changed/added):

dot11FragmentationThreshold OBJECT-TYPE

SYNTAX Unsigned32 (256..~~11500~~65535)

UNITS "octets"

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 ~~current~~ maximum size~~, in octets,~~ of ~~the~~an individually addressed MPDU

~~that may be delivered to the security encapsulation~~ beyond which the corresponding MSDU or MMPDU is fragmented, except ~~. This maximum size~~

~~does not apply~~ when an MSDU is transmitted ~~using~~under an HT-immediate or HT-delayed block ack agreement, or when an MSDU is carried in an A-MSDU, or when an MSDU or MMPDU is carried in

an A-MPDU that does not contain a VHT single MPDU. Fields added to

the ~~frame~~MPDU by security encapsulation are not counted against the limit

specified by this attribute. An MSDU or MMPDU might be fragmented even

if it is smaller. ~~Except as described above, an MSDU or MMPDU~~

~~is fragmented when the resulting frame has an individual address in the~~

~~Address 1 field, and the length of the frame is larger than this~~

~~threshold, excluding security encapsulation fields. The default value for~~

~~this attribute is the lesser of 11500 or aMPDUMaxLength and the~~

~~value never exceeds the lesser of 11500 or aMPDUMaxLength.~~"

DEFVAL { 65535 }

::= { dot11OperationEntry 5 }

Delete aMPDUMaxLength from 6.5.4.2 (1 line at 521.34) and 6.5.4.3 (1 table row at 523.29).

Delete “(16 to 216–1 as defined by aMPDUMaxLength)” at 2158.3.

Rename aMPDUMaxLength to aPSDUMaxLength in Table 16-5, Table 17-4, Table 18-21, Table 19-6 (1 instance in each).

Make the following changes in Annex C.3:

dot11MaxAMSDULength OBJECT-TYPE

SYNTAX INTEGER { short(3839), long(7935) }

UNITS "octets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the ~~supported~~ maximum supported size of an A-MSDU

received in an HT PPDU."

DEFVAL { short }

::= { dot11HTStationConfigEntry 4 }

dot11MaxMPDULength OBJECT-TYPE

SYNTAX INTEGER { short(3895), medium(7991), long(11454) }

UNITS "octets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the ~~supported~~ maximum supported size of an MPDU ~~size~~received in a VHT PPDU."

DEFVAL { short }

::= { dot11VHTStationConfigEntry 1 }

dot11TVHTMaxMPDULength OBJECT-TYPE

SYNTAX INTEGER { short(3895), medium(7991), long(11454) }

UNITS "octets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

This attribute indicates the ~~supported~~ maximum supported size of an MPDU ~~size~~received in a TVHT PPDU.

DEFVAL { short }

::= { dot11TVHTStationConfigEntry 1 }

dot11MaxMSDULength OBJECT-TYPE

SYNTAX INTEGER { normal(2304), long(7920) }

UNITS "octets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

This attribute indicates the maximum supported MSDU size.

This is 7920 octets for a DMG STA and 2304 octets for a non-DMG STA."

::= { dot11StationConfigEntry <ANA> }

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3211, which clarify the usage of dot11FragmentationThreshold, aMPDUMaxLength and aPSDUMaxLength, and introduce a MIB variable to give the maximum MSDU size (i.e. MTU).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3226  Qi Wang  10.33.2.2  1805.23 | Consider using PPDU | "... any other individually addressed PPDUA-MPDU, MPDU, or MMPDU to the responder ..." |

Discussion:

The text at the cited location reads:

c) The initiator shall send an FST Ack Request frame or may send any other individually addressed A-MPDU, MPDU, or MMPDU to the responder.

This text is an instance of the common confusion between DUs. MMPDUs (and MSDUs) are sent in one or more MPDUs (where one or more MSDUs can be sent in an A-MSDU, itself sent in an MPDU). One or more MPDUs can be sent in an A-MPDU. The things which are individually addressed are MMPDUs, MSDUs and MPDUs (where as just stated the first two of these are carried in one or more of the last of these); A-MPDUs and A-MSDUs are not individually addressed per se, though the rules on their contents may result in all MPDUs/MSDUs they contain being addressed to the same device(s). The cited text is therefore inappropriately mixing DUs.

The proposed change is inappropriate too, though, since PPDUs are not addressed at all; they merely carry PSDUs which are addressed.

Proposed resolution:

REVISED

Delete “A-MPDU,” and “, or MMPDU” at 1805.23.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3430  Mark RISON  11.3.5.4  1862.56 | Having more than one thing (e.g. "KCK || PMK") on the left of an equals sign is somewhat confusing | Use L() as in 11.6.1.3 |

Discussion:

By analogy with 1932.14, 1935.10, 1939.51, 1979.59, it seems that the intent is that the KCK is the first KCK\_bits bits of the thing on the right. KCK\_bits is 256 here (1862.51: “both the KCK and PMK shall be 256-bits in length”).

Proposed resolution:

REVISED

Change “*KCK || PMK*” to “*kck\_and\_pmk*” at 1862.56.

Add “KCK = L(*kck\_and\_pmk*, 0, 256)” after the equation at 1862.56.

Add “PMK = L(*kck\_and\_pmk*, 256, 256)” after the equation at 1862.56.

In all cases, italicise “kck\_and\_pmk”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3462  Mark RISON | "Alternate Preferred" -- actually it's not a mere preference, it's an override | Change to "Overridden" throughout (10 instances in 8.4.2.76, 10.2.2.16.3, 10.2.2.16.4 and 10.24.8) |

Discussion:

The uses of “Alternate Preferred” are the following:

Table 8-203—FMS Element Status and TFS Response Status definition [6 of the values, all of the form “Alternate Preferred, due to …”.]

If the AP selects an alternate delivery interval or alternate maximum delivery interval from the value specified in the FMS Request, the FMS Status subelement shall be set to Alternate Preferred, and the FMS subelement shall indicate the AP selected value(s).

If the Element Status value in FMS Status subelement is Alternate Preferred due to AP changed the maximum delivery interval:

— The AP does not deliver the requested streams at the delivery interval as specified by the non-AP STA in the FMS Request element. The delivery interval specified in the FMS Status subelement specifies a delivery interval that the AP is willing to accept for the specified streams if the non-AP STA sends another FMS Request with that delivery interval specified.

— The non-AP STA may submit a new FMS Request that includes the delivery interval value received from the AP. If the AP accepts this new FMS Request, it shall respond as described in 10.2.2.16.2 (FMS general procedures).

If the Element Status value in FMS Status subelement is Alternate Preferred due to AP unable to provide requested TCLAS-based classifiers:

— The AP does not deliver the requested streams at the delivery interval as specified by the non-AP STA in the FMS Request element. The TCLAS element(s) or TCLAS Processing element in the TCLAS Status subelement contains one or more fields or subfields whose values have been modified by the AP. The AP may include fewer TCLAS elements in the FMS Response element than were present in the request; when the AP’s response includes a single TCLAS element, it does not include a TCLAS processing element. If the AP changes a TCLAS element’s Classifier Type field in the FMS Response element but is unable to suggest a value for the Classifier Mask field, it shall set that field to 0. If the AP changes a TCLAS element’s Classifier Type field or Classifier Mask field in the FMS Response element but is unable to suggest values for one or more Classifier Parameter subfields, it shall set those fields to 0.

— A non-AP STA receiving a modified TCLAS element having a Classifier Mask field equal to 0 or Classifier Parameter subfields equal to 0 shall interpret these values as meaning that no suggested value has been provided by the AP.

The AP may send an FMS Response frame to the STA to change the STA’s multicast rate. When the AP sends an FMS Response frame to the STA with an Element Status field value of 8, indicating “Alternate Preferred, due to AP multicast rate policy,” the STA shall not send further FMS Request frames to request a change in the multicast rate while the STA is associated to the AP.

It seems that “Alternate Preferred due to AP changed the maximum delivery interval” and “Alternate Preferred due to AP unable to provide requested TCLAS-based classifiers” are not overrides as the commenter suggested, since in both cases “The AP does not deliver the requested streams” (the subsequent “at the delivery interval as specified by the non-AP STA in the FMS Request element” is confusing, though, as it suggests the AP might still deliver the requested streams, just at a different interval). The situation is not clear for “Alternate Preferred due to AP changed the delivery interval” and “Alternate Preferred, due to AP multicast rate policy” (the first might be the same as “due to AP changed the maximum delivery interval” by analogy (but see CID 3459), while the latter seems to be more of an override-and-don’t-ever-dare-ask-again). The last two are completely undefined (see CID 3460).

Proposed changes:

Err, dunno. Maybe it should be “Alternate Required”? Delete the “at the delivery interval as specified by the non-AP STA in the FMS Request element”s?

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3393  Mark RISON | References to "Clause <n> frames" (n = 16, 17, etc.) make no sense as frames are a MAC concept. "rates" is suspect too because a given rate may be used by more than one PHY (e.g. 11g and 11a, and probably some variants of 11a and 11n). Other forms like "Clause <n> waveforms" or "PPDUs" or "formats" make sense but should be consistent | Pick one valid term (I suggest PPDU) and use it consistently |

Discussion:

For most PHYs (exceptions are DSSS and DMG) we need to distinguish between formats introduced by that PHY, and formats supported by that PHY. For example, 11n introduces two new formats (MF and GF) and supports various earlier formats (non-HT: ERP, OFDM, HR/DSSS, DSSS).

The definitions in Subclause 3.2 make it clear that “Clause n PPDU” includes those sent in earlier formats supported by the PHY in question. “Clause n format” is ambiguous because it would appear to indicate a specific format, but doesn’t (see e.g. Figure 20-1 which shows three HT PPDU formats: non-HT, MF and GF; a notable exception is “Clause 18 format” since this doesn’t recurse to any earlier formats). “<name> format” seems less ambiguous (see e.g. Subclause 20.3.2 which for HT states that “Two formats are defined for the PPDU: HT-mixed format and HT-greenfield format. These two formats are

called *HT formats*.”), and in turn “<name> PPDU” seems OK too.

So the proposed convention is:

* Use “<name> PHY” for a PHY compliant with the clause defining the <name> PHY (so a VHT PHY is also an HT PHY and an OFDM PHY)
* Use “<name> STA” for a STA using a <name> PHY (so a VHT STA is also an HT STA and an OFDM STA)
* Use “<name> format”/“<name> PPDU” for everything introduced by the <name> PHY (i.e. not inherited from its ancestors, so an HT PPDU is **not** also a VHT PPDU)
* Do not use “Clause n format” or “Clause n PPDU”

Make sure that in the glossary:

* Each type of PHY, PPDU and STA has an entry
* Each type of PPDU is orthogonal to all others, and covers all PHYs which can generate it
* The type of STA which generates each PPDU is indicated
* The TXVECTOR parameters are spelt out sufficiently to uniquely identify a PPDU format
* Things are consistent

Proposed changes:

**20 MHz high throughput (HT):** A ~~Clause 20 (High Throughput (HT) PHY specification)~~ transmission

by an HT [or VHT?] STA with TXVECTOR parameter FORMAT equal to HT\_MF or HT\_GF and TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20. [CH\_OFFSET parameter doesn’t have to be equal to CH\_OFF\_20?]

**20 MHz mask physical layer (PHY) protocol data unit (PPDU):** One of the following PPDUs:

a) A ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification)~~n orthogonal frequency division multiplexing (OFDM) PPDU [the omission of “20 MHz channel spacing” is intentional, i.e. 10 and 5 MHz channel spacing PPDUs count as 20 MHz mask PPDUs? Compare with 20 MHz PPDUs below] transmitted by an OFDM STA using the transmit spectral mask for 20 MHz channel spacing [or the mask for the channel spacing in question?] defined in Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification).

b) A ~~Clause 19 (Extended Rate PHY (ERP) specification) orthogonal frequency division multiplexing~~

~~(OFDM)~~n extended rate PHY (ERP) PPDU using OFDM modulation (ERP-OFDM) transmitted by an ERP STA using the transmit spectral mask for ERP-OFDM defined in Clause 19 (Extended Rate PHY (ERP) specification).

c) A high throughput (HT) PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to

HT\_CBW20 and ~~the~~ CH\_OFFSET parameter equal to CH\_OFF\_20 transmitted by an HT STA using the 20 MHz transmit spectral mask defined in Clause 20 (High Throughput (HT) PHY specification). [where is the OFDM PPDU transmitted using the 20 MHz HT mask, like e below for a VHT STA?] [where is the ERP-OFDM PPDU transmitted using the 20 MHz HT mask, like f below for a VHT STA?]

d) A very high throughput (VHT) PPDU with TXVECTOR parameter CH\_BANDWIDTH equal to CBW20 transmitted by a VHT STA using the 20 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

e) A ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification)~~n OFDM PPDU transmitted by a VHT STA using the transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

f) An HT PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20 and ~~the~~ CH\_OFFSET parameter equal to CH\_OFF\_20 transmitted by a VHT STA using the 20 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

***[Editor: swap b and c in the following list.]***

**20 MHz physical layer (PHY) protocol data unit (PPDU):** One of the following PPDUs:

a) A ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications)~~DSSS PPDU~~,~~

b) An ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification)~~OFDM PPDU ~~(when~~ using 20 MHz channel spacing~~),~~

c) An ~~Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~HR/DSSS PPDU~~,~~

d) An ~~Clause 19 (Extended Rate PHY (ERP) specification) orthogonal frequency division multiplexing (OFDM)~~ERP-OFDM PPDU~~,~~

e) An ~~Clause 20 (High Throughput (HT) PHY specification) 20 MHz high throughput (~~HT~~)~~ PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20~~, or~~

f) A ~~Clause 22 (Very High Throughput (VHT) PHY specification) 20 MHz very high throughput (~~VHT~~)~~ PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to CBW20.

**40 MHz high throughput (HT):** A ~~Clause 20 (High Throughput (HT) PHY specification)~~ transmission

by an HT [or VHT?] STA with TXVECTOR parameter FORMAT equal to HT\_MF or HT\_GF and TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW40.

***[Editor: reorder the items below so that they are grouped by STA flavour, i.e. a, b, d, h then f, g, c, e, i.]***

**40 MHz mask physical layer (PHY) protocol data unit (PPDU):** One of the following PPDUs:

a) A ~~40 MHz~~ high throughput (HT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW40~~)~~ transmitted by an HT STA using the 40 MHz transmit spectral mask defined in Clause 20 (High Throughput (HT) PHY specification).

b) A ~~40 MHz~~ non-HT duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to NON\_HT\_CBW40~~)~~ transmitted by a ~~non-very high throughput (non-VHT)~~n HT STA using the 40 MHz transmit spectral mask defined in Clause 20 (High Throughput (HT) PHY specification).

c) A ~~40 MHz~~ non-HT duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW40~~)~~ and TXVECTOR parameter NON\_HT\_MODULATION equal to NON\_HT\_DUP\_OFDM transmitted by a very high throughput (VHT) STA using the 40 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

d) An ~~20 MHz~~ HT PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20 and ~~the~~ CH\_OFFSET parameter equal to ~~either~~ CH\_OFF\_20U or CH\_OFF\_20L transmitted by an HT STA using the 40 MHz transmit spectral mask defined in Clause 20 (High Throughput (HT) PHY specification).

e) A ~~20 MHz~~ VHT PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to CBW20 transmitted by a VHT STA using the 40 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

f) A ~~40 MHz~~ VHT PPDU with ~~the~~ TXVECTOR parameter CH\_BANDWIDTH equal to CBW40 transmitted by a VHT STA using the 40 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

g) An ~~40 MHz~~ HT PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW40~~)~~ transmitted by a VHT STA using the 40 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification). [where is 20 MHz HT transmitted by a VHT STA?]

h) A ~~20 MHz~~ non-HT PPDU ~~(~~with TXVECTOR parameter ~~CH\_BANDWIDTH equal to NON\_HT\_CBW20)~~ CH\_OFFSET equal to CH\_OFF\_20U or CH\_OFF\_20L transmitted by an HT STA using the 40 MHz transmit spectral mask defined in Clause 20 (High Throughput (HT) PHY specification).

i) An ~~20 MHz non-HT~~OFDM PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW20~~)~~ transmitted by a VHT STA using the 40 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification).

**40 MHz physical layer (PHY) protocol data unit (PPDU):** One of the following PPDUs:

a) A ~~40 MHz~~ high throughput (HT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW40~~) or~~

b) ~~a~~A ~~40 MHz~~ non-HT duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to NON\_HT\_CBW40 (HT STA) or ~~TXVECTOR parameter CH\_BANDWIDTH equal to~~ CBW40 (VHT STA)~~, or~~

c) ~~a~~A ~~40 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW40~~)~~.

**80 MHz mask physical layer (PHY) protocol data unit (PPDU):** A PPDU that is transmitted by a VHT STA using the 80 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification) and that is one of the following:

a) A~~n~~ ~~80 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW20, CBW 40 or CBW80~~)~~

b) A~~n~~ ~~80 MHz~~ non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW40 or CBW80~~)~~

c) A ~~20 MHz~~ non-HT PPDU~~,~~

d) A high throughput (HT) PPDU with TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20 or HT\_CBW40

~~, or VHT PPDU (TXVECTOR parameter CH\_BANDWIDTH equal to CBW20)~~

~~d) A 40 MHz non-HT duplicate, HT, or VHT PPDU (with TXVECTOR parameter CH\_BANDWIDTH equal to CBW40)~~

**80 MHz physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 22 (Very High Throughput (VHT)~~

~~PHY specification) 80 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter

CH\_BANDWIDTH equal to CBW80~~)~~ or a ~~Clause 22 (Very High Throughput (VHT) PHY specification) 80 MHz~~ non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal toCBW80~~)~~.

**160 MHz mask physical layer (PHY) protocol data unit (PPDU):** A PPDU that is transmitted by a VHT STA using the 160 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification) and that is one of the following:

a) A ~~160 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW20, CBW40, CBW80 or CBW160~~)~~

b) A ~~160 MHz~~ non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter

CH\_BANDWIDTH equal to CBW40, CBW80 or CBW160~~)~~

c) A ~~20 MHz~~ non-HT PPDU~~,~~

d) A high throughput (HT) PPDU with TXVECTOR parameter CH\_BANDWIDTH equal to HT\_CBW20 or HT\_CBW40

~~, or VHT PPDU (TXVECTOR parameter CH\_BANDWIDTH equal to CBW20)~~

~~d) A 40 MHz non-HT duplicate, HT, or VHT PPDU (TXVECTOR parameter CH\_BANDWIDTH~~

~~equal to CBW40)~~

~~e) An 80 MHz non-HT duplicate or VHT PPDU (TXVECTOR parameter CH\_BANDWIDTH equal to~~

~~CBW80)~~

**160 MHz physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 22 (Very High Throughput (VHT) PHY specification) 160 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter

CH\_BANDWIDTH equal to CBW160~~)~~ or a ~~Clause 22 (Very High Throughput (VHT) PHY specification) 160 MHz~~ non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW160~~)~~.

**80+80 MHz mask physical layer (PHY) protocol data unit (PPDU):** A PPDU that is transmitted by a VHT STA using the 80+80 MHz transmit spectral mask defined in Clause 22 (Very High Throughput (VHT) PHY specification) and that is one of the following:

a) A~~n~~ ~~80+80 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW80+80~~)~~

b) An 80+80 MHz non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter CH\_BANDWIDTH equal to CBW80+80~~)~~

[why not also all the combinations where only the primary segment is used?]

**80+80 MHz physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 22 (Very High Throughput~~

~~(VHT) PHY specification) 80+80 MHz~~ very high throughput (VHT) PPDU ~~(~~with TXVECTOR parameter

CH\_BANDWIDTH equal to CBW80+80~~)~~ or a ~~Clause 22 (Very High Throughput (VHT) PHY~~

~~specification) 80+80 MHz~~ non-high throughput (non-HT) duplicate PPDU ~~(~~with TXVECTOR parameter

CH\_BANDWIDTH equal to CBW80+80~~)~~.

**direct sequence spread spectrum (DSSS) physical layer (PHY):** A physical layer (PHY) compliant with Clause 16.

**direct sequence spread spectrum (DSSS) physical layer (PHY) protocol data unit (PPDU):** A PPDU transmitted by a DSSS STA, or by an HR/DSSS STA with TXVECTOR parameter DATARATE equal to 1 or 2 Mb/s and TXVECTOR parameter PREAMBLE\_TYPE equal to LONGPREAMBLE, or by an ERP STA with TXVECTOR parameter MODULATION equal to ERP-DSSS and TXVECTOR parameter PREAMBLE\_TYPE equal to LONGPREAMBLE, or by an HT STA with TXVECTOR parameter NON\_HT\_MODULATION equal to ERP-DSSS and TXVECTOR parameter PREAMBLE\_TYPE equal to LONGPREAMBLE.

**direct sequence spread spectrum (DSSS) station (STA):** A STA that uses a DSSS physical layer (PHY).

***[Note to editor: move the following to the correct place in alphabetical order.]***

**high throughput (HT) physical layer (PHY) using direct sequence spread spectrum/complementary code keying (HT-DSSS/CCK):** A ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) transmission~~mode of operation of an HT PHY using the DSSS modulation defined in Clause 16 or the CCK modulation defined in Clause 17.

**directional multi-gigabit (DMG)**: Pertaining to operation in a frequency band containing a channel with

the Channel starting frequency above 45 GHz.

**directional multi-gigabit (DMG) physical layer (PHY):** A physical layer (PHY) compliant with Clause 21.

**directional multi-gigabit (DMG) physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 21~~

~~(Directional multi-gigabit (DMG) PHY specification)~~ PPDU transmitted ~~or received using the Clause 21~~

~~(Directional multi-gigabit (DMG) PHY specification) physical layer (PHY)~~ by a DMG STA.

**directional multi-gigabit (DMG) station (STA):** A STA ~~whose radio transmitter is capable of transmitting and receiving DMG physical layer (PHY) protocol data units (PPDUs)~~ that uses a Clause 21 physical layer (PHY).

**extended rate physical layer (ERP):** A physical layer (PHY) conforming to Clause 19 (Extended Rate PHY (ERP) specification).

**extended rate physical layer (~~PHY~~ERP) using CCK modulation (ERP-CCK):** A mode of operation of an ERP ~~PHY operating under Clause 19 (Extended Rate PHY (ERP) specification) rules~~, ~~where MODULATION=ERP-CCK~~using the CCK modulation defined in Clause 17.

**extended rate physical layer (~~PHY~~ERP) using DSSS modulation (ERP-DSSS):** A mode of operation of an ERP~~PHY operating under Clause 19 (Extended Rate PHY (ERP) specification) rules~~, ~~where MODULATION=ERP-DSSS~~using the DSSS modulation defined in Clause 16.

**extended rate physical layer (~~PHY~~ERP) using DSSS or CCK modulation (ERP-DSSS/CCK):** A mode of operation of an ERP~~PHY operating under Clause 19 (Extended Rate PHY (ERP) specification) rules~~, ~~where MODULATION=ERP-CCK or MODULATION=ERP-DSSS~~using the DSSS modulation defined in Clause 16 or the CCK modulation defined in Clause 17.

**extended rate physical layer (~~PHY~~ERP) using OFDM modulation (ERP-OFDM):** A mode of operation of an ERP~~PHY operating under Clause 19 (Extended Rate PHY (ERP) specification) rules~~, using the OFDM modulation defined in Clause 18.

**extended rate physical layer (ERP) using OFDM modulation (ERP-OFDM) physical layer (PHY) protocol data unit (PPDU)**: A PPDU transmitted by an ERP STA with TXVECTOR parameter MODULATION equal to ERP-OFDM, or by an HT STA with TXVECTOR parameter NON\_HT\_MODULATION equal to ERP-OFDM.

**extended rate physical layer (ERP) station (STA):** A STA that uses a Clause 19 physical layer (PHY).

**high rate direct sequence spread spectrum (HR/DSSS) physical layer (PHY):** A physical layer (PHY) compliant with Clause 17.

**high rate direct sequence spread spectrum (HR/DSSS) physical layer (PHY) protocol data unit (PPDU):** A PPDU transmitted by an HR/DSSS STA with TXVECTOR parameter DATARATE equal to 5.5 or 11 Mb/s or TXVECTOR parameter PREAMBLE\_TYPE equal to SHORTPREAMBLE, or by an ERP STA with TXVECTOR parameter MODULATION equal to ERP-CCK or TXVECTOR parameter PREAMBLE\_TYPE equal to SHORTPREAMBLE, or by an HT STA with TXVECTOR parameter NON\_HT\_MODULATION equal to ERP-CCK or TXVECTOR parameter PREAMBLE\_TYPE equal to SHORTPREAMBLE.

**high rate direct sequence spread spectrum (HR/DSSS) station (STA):** A STA that uses a DSSS physical layer (PHY).

**high throughput greenfield (HT-greenfield) format:** A physical layer (PHY) protocol data unit (PPDU) format of the HT physical layer ~~(PHY)~~ using the HT-greenfield format preamble. This format is represented at the PHY data service access point (SAP) by the TXVECTOR/RXVECTOR FORMAT parameter being equal to HT\_GF.

**high throughput mixed (HT-mixed) format:** A physical layer (PHY) protocol data unit (PPDU) format of the HT physical layer ~~(PHY)~~ using the HT-mixed format preamble. This format is represented at the PHY data service access point (SAP) by the TXVECTOR/RXVECTOR FORMAT parameter being equal to HT\_MF.

**high throughput (HT) physical layer (PHY):** A physical layer (PHY) compliant with Clause 20.

**high throughput (HT) physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 20 (High Throughput (HT) PHY specification)~~ PPDU transmitted by an HT or VHT STA with ~~the~~ TXVECTOR FORMAT parameter equal to HT\_MF or HT\_GF.

**high throughput (HT) station (STA):** A STA that uses an HT physical layer (PHY).

**nonextended rate physical layer (NonERP):** A physical layer (PHY) conforming to Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), but not to Clause 19 (Extended Rate PHY (ERP) specification).

**non-high throughput (non-HT):** A modifier meaning neither high throughput (HT) nor very high

throughput (VHT).

**non-high throughput (non-HT) duplicate:** A transmission format of the HT or VHT physical layer (PHY) that duplicates a 20 MHz non-HT transmission in two or more 20 MHz channels and allows a station (STA) in a non-HT basic service set (BSS) on any one of the 20 MHz channels to receive the transmission. A non-HT duplicate format is one of the following:

a) 40 MHz non-HT duplicate: A transmission format of the PHY that replicates a 20 MHz non-HT

transmission in two adjacent 20 MHz channels.

b) 80 MHz non-HT duplicate: A transmission format of the PHY that replicates a 20 MHz non-HT

transmission in four adjacent 20 MHz channels.

c) 160 MHz non-HT duplicate: A transmission format of the PHY that replicates a 20 MHz non-HT

transmission in eight adjacent 20 MHz channels.

d) 80+80 MHz non-HT duplicate: A transmission format of the PHY that replicates a 20 MHz non-HT

transmission in two frequency segments of four adjacent 20 MHz channels where the two frequency

segments of channels are not adjacent.

**non-high throughput (non-HT) duplicate frame:** A frame transmitted in a non-HT duplicate physical

layer (PHY) protocol data unit (PPDU).

**non-high throughput (non-HT) duplicate physical layer (PHY) protocol data unit (PPDU):** A PPDU

transmitted by ~~a Clause 20 (High Throughput (HT) PHY specification) or Clause 22 (Very High Throughput (VHT) PHY specification) PHY~~ an HT or VHT STA with ~~the~~ TXVECTOR FORMAT parameter equal to NON\_HT and ~~the~~ CH\_BANDWIDTH parameter equal to NON\_HT\_CBW40 (HT STA), CBW40, CBW80, CBW160, or CBW80+80 (VHT STA).

**non-high throughput (non-HT) physical layer (PHY) protocol data unit (PPDU):** A ~~Clause 20 (High~~

~~Throughput (HT) PHY specification) physical layer (PHY) PPDU with the TXVECTOR FORMAT~~

~~parameter equal to NON\_HT~~ PPDU other than one transmitted by an HT or VHT STA with TXVECTOR parameter FORMAT equal to HT\_MF or HT\_GF or by a VHT STA with TXVECTOR parameter FORMAT equal to VHT.

**orthogonal frequency domain multiplexing (OFDM) physical layer (PHY):** A physical layer (PHY) compliant with Clause 18.

**orthogonal frequency domain multiplexing (OFDM) physical layer (PHY) protocol data unit (PPDU):** A PPDU transmitted by an OFDM STA, or by an HT or VHT STA with TXVECTOR parameter NON\_HT\_MODULATION equal to OFDM.

**orthogonal frequency domain multiplexing (OFDM) station (STA):** A STA that uses an OFDM physical layer (PHY).

**very high throughput (VHT) physical layer (PHY):** A physical layer (PHY) compliant with Clause 22.

**very high throughput (VHT) physical layer (PHY) protocol data unit (PPDU):** A PPDU transmitted by a VHT STA with ~~the~~ TXVECTOR parameter FORMAT equal to VHT.

**very high throughput (VHT) station (STA):** A STA that uses a VHT physical layer (PHY).

Change 613.15 as follows: “The DSSS Parameter Set element is present within Beacon frames generated by DSSS, HR/DSSS and ERP STAs ~~using Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY~~

~~specification), and Clause 19 (Extended Rate PHY (ERP) specification) PHYs~~.

The DSSS Parameter Set element is present within Beacon frames generated by HT STAs ~~using a Clause 20 (High Throughput (HT) PHY specification) PHY~~ in the 2.4 GHz band.”

Change 625.17 as follows: “The DSSS Parameter Set element is present within Probe Request

frames generated by DSSS, HR/DSSS and ERP STAs ~~using Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), or Clause 19 (Extended Rate PHY (ERP) specification) PHYs~~ if dot11RadioMeasurementActivated is true.

The DSSS Parameter Set element is present within Probe Request frames generated by HT STAs ~~using a Clause 20 (High Throughput (HT) PHY specification) PHY~~ in the 2.4 GHz band if dot11RadioMeasurementActivated is true.

The DSSS Parameter Set element is optionally present within Probe Request frames generated by DSSS, HR/DSSS and ERP STAs ~~using Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), or Clause 19 (Extended Rate PHY (ERP) specification) PHYs~~ if dot11RadioMeasurementActivated is false.

The DSSS Parameter Set element is optionally present within Probe Request frames generated by HT STAs ~~using a Clause 20 (High Throughput (HT) PHY specification) PHY~~ in the 2.4 GHz band if dot11RadioMeasurementActivated is false.”

Change 626.43 as follows: “The DSSS Parameter Set element is present within Probe Response frames generated by DSSS, HR/DSSS and ERP STAs ~~using Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) PHYs~~.

The DSSS Parameter Set element is present within Probe Response frames generated by HT STAs ~~using a Clause 20 (High Throughput (HT) PHY specification) PHY~~ in the 2.4 GHz band.”

Change 719.3 as follows: “The ERP element contains information on the presence of ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications)~~DSSS or ~~Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~HR/DSSS STAs in the BSS ~~that~~; these are not capable of ~~Clause 19 (Extended Rate PHY (ERP) specification) (ERP-OFDM) data rates~~ ERP formats.”

Change the headings at 826.29 to say “For DSSS and HR/DSSS STAs”, “For OFDM, ERP, HT and VHT STAs”, “For TVHT STAs” and “For other STAs”.

Change 1043.17 as follows: “Non-HT, excluding DSSS and HR/DSSS~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) and Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~”.

Change 1262.55 as follows: “Transmissions of ERP-OFDM PPDUs, of ~~frame~~PPDUs with TXVECTOR parameter FORMAT ~~of type~~value NON\_HT ~~with~~and NON\_HT\_MODULATION value~~s of~~ ERP-OFDM ~~and~~or NON\_HT\_DUP\_OFDM by HT STAs, and ~~transmissions~~ of ~~frame~~HT PPDUs ~~with TXVECTOR parameter FORMAT with values of HT\_MF and HT\_GF~~ include a period of no transmission of duration aSignalExtension, except for RIFS transmissions. The purpose of this signal extension is to enable the NAV value of ~~Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~ DSSS and HR/DSSS STAs to be set correctly.”

Change “ERP PPDU” to “ERP-OFDM PPDU” at 1367.20.

Change 1367.27 as follows: “The intent of a protection mechanism is to cause a STA to not transmit a~~n MPDU of type Data or an MMPDU~~PPDU with an ERP-OFDM preamble and header unless it has attempted to update the NAV of receiving NonERP STAs. The updated NAV period shall be longer than or equal to the total time required to send the Data and any required response frames. An ERP STA shall use protection mechanisms (such as RTS/CTS or CTS-to-self) for ERP-OFDM ~~MPDUs of type Data or an MMPDU~~PPDUs when the Use\_Protection field of the ERP element is equal to 1 (see the requirements of 9.7 (Multirate support)). Protection mechanism~~s~~ frames shall be sent using one of the mandatory Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) rates and using one of the mandatory Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) ~~waveforms~~formats, so all STAs in the BSA are able to learn the duration of the exchange even if they cannot detect the ERP-OFDM signals using their CCA function.”

Change 1369.36 as follows: “An ERP STA shall use long preambles when transmitting ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) frames~~DSSS or HR/DSSS PPDUs after transmission or reception of an ERP element with a Barker\_Preamble\_Mode value of 1 in an MMPDU to or from the BSS that the ERP STA has joined or started, regardless of the value of the short preamble capability bit from the same received or transmitted MMPDU that contained the ERP element. An ERP STA may additionally use long preambles when transmitting ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) frames~~DSSS or HR/DSSS PPDUs at other times. An ERP STA may use short preambles when transmitting ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) frames~~DSSS or HR/DSSS PPDUs after transmission or reception of an ERP element with a Barker\_Preamble\_Mode value of 0 in an MMPDU to or from the BSS that the ERP STA has joined or started, regardless of the value of the short preamble capability bit from the same received or transmitted MMPDU. A NonERP STA may also follow the rules given in this paragraph.

An ERP mesh STA shall use long preambles when transmitting ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) frames~~DSSS or HR/DSSS PPDUs after transmission or reception of an ERP element with a Barker\_Preamble\_Mode value of 1 in an MMPDU to or from the MBSS to which the ERP mesh STA belongs. A Mesh STA may additionally use long preambles when transmitting ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), and Clause 19 (Extended Rate PHY (ERP) specification) frames~~DSSS or HR/DSSS PPDUs at other times.”

Change 1371.21 as follows: “The frames that are used for providing the protection shall be sent ~~at a Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) rate~~ using DSSS or HR/DSSS PPDUs.”

Change 1553.19 as follows: “For ~~Clause 19 (Extended Rate PHY (ERP) specification) and Clause 20 (High Throughput (HT) PHY specification) PHYs~~ERP and HT APs, if the Beacon frame is transmitted using ERP-DSSS/CCK, the AP shall transmit the high data rate TIM frame and shall transmit it using ERP-OFDM.”

Change 1661.52 as follows: “NOTE 2—For efficient use of the medium, it is recommended that Measurement Pilots not be sent ~~using a PHY specified in Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~ in DSSS or HR/DSSS PPDUs.”

Change 1721.32 as follows: “The responding STA shall not transmit Fine Timing Measurement frames ~~using Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) formats~~ in DSSS or HR/DSSS PPDUs.”

Change “HR/DSSS” to “HR/DSSS/long” at 54.23, 2177.22, 2177.35.

Change 2254.34 as follows: “~~The~~An ERP ~~has the capability to decode~~is capable of receiving all ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) and Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) PHYs~~DSSS and HR/DSSS PPDUs and all ERP-OFDM ~~PHYs~~PPDUs [err, not all rates are mandatory, are they?]. An ERP ~~shall be~~is capable of sending and receiving the short preamble that is ~~(and remains)~~ optional for ~~Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~HR/DSSS PHYs.”

Change 2255.27 as follows: “The 2.4 GHz ISM band is a shared medium, and coexistence with other devices such as ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) and Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~  DSSS and HR/DSSS STAs is an important issue for maintaining high performance in ~~Clause 19 (Extended Rate PHY (ERP) specification) (~~ERP~~)~~ STAs. The ERP modulation (ERP-OFDM) has been designed to coexist with existing ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) and Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification)~~ DSSS and HR/DSSS STAs.”.

Change “ERP-DSSS” to “a” at 2256.52.

Delete “PHY” at 2258.62 and 2261.1.

Change 2259.49 as follows: “For ERP-OFDM ~~frame~~PPDUs, this includes the length extension. For ERP-OFDM ~~frame~~PPDUs”.

Change 2260.10 as follows: “for the ERP-OFDM ~~frame~~PPDU format”.

Change 2260.41 as follows: “An ERP receiver shall be capable of receiving 1, 2, 5.5, and 11 Mb/s PPDUs using either the long or short preamble formats described in Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) and shall be capable of receiving 6, 12, and 24 Mb/s PPDUs using the modulation and preamble described in Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification). The PHY may also ~~implement the ERP-OFDM modulations at rates of~~ be capable of receiving 9, 18, 36, 48, and 54 Mb/s PPDUs using these.”

Change “ERP-DSSS” to “ERP-DSSS/CCK” at 2262.14, 2262.57, 2263.13.

Delete “format” at 2262.34.

Change 2265.24 as follows: “The value of the TXTIME parameter returned by the PLME\_TXTIME.confirm primitive for an ERP-OFDM PPDU shall be calculated using ~~the ERP-OFDM TXTIME calculation as shown in~~ Equation (19-1).”

Delete “-OFDM” at 2265.42.

Change 2267.51 as follows: “these STAs support a mixture of DSSS, HR/DSSS, OFDM, ERP and HT ~~PHY and Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), or Clause 19 (Extended Rate PHY (ERP) specification)~~ PHYs.”

Change 2278.60 as follows: “~~Non-HT format PPDUs structured according to Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), or Clause 19 (Extended Rate PHY (ERP) specification)~~ DSSS, HR/DSSS, OFDM and ERP PPDUs are transmitted”.

Change 2434.11 as follows: “these STAs support a mixture of OFDM, HT and VHT~~: Clause 20 (High Throughput (HT) PHY specification) and Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification)~~ PHYs.”

Change 2445.6 as follows: “A VHT STA logically contains ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification), Clause 20 (High Throughput (HT) PHY specification), and Clause 22 (Very High Throughput (VHT) PHY specification)~~ OFDM and HT PHYs. The MAC interfaces to the PHYs via the ~~Clause 22 (Very High Throughput (VHT) PHY specification)~~ VHT PHY service interface, which in turn interacts with the ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification) and Clause 20 (High Throughput (HT) PHY specification)~~ OFDM and HT PHY service interfaces as shown in Figure 22-1 (PHY interaction on transmit for various PPDU formats), Figure 22-2 (PHY interaction on receive for various PPDU formats), and Figure 22-3 (PHY-CONFIG and CCA interaction with ~~Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification), Clause 20 (High Throughput (HT) PHY specification), and Clause 22 (Very High Throughput (VHT) PHY specification)~~ OFDM, HT and VHT PHYs).”

Change 2699.16 as follows: “Use ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) or Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) rates~~ DSSS or HR/DSSS PPDUs when using protection mechanisms”.

Change 2904.13 as follows: “This attribute, when true, indicates that the station implementation is capable of supporting Time Of Departure for ~~Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications) transmitted frames, Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification) transmitted frames, Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) transmitted frames, Clause 19 (Extended Rate PHY (ERP) specification) transmitted frames and Clause 20 (High Throughput (HT) PHY specification) transmitted frames~~DSSS, HR/DSSS, OFDM, ERP and HT PPDUs [not VHT?] when the dot11WirelessManagementImplemented is set to true.”.

Change 2904.33 as follows: “This attribute, when true, indicates that the capability to support Time Of Departure ~~frames~~ for ~~transmitted Clause 16 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification), Clause 17 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), Clause 19 (Extended Rate PHY (ERP) specification) and Clause 20 (High Throughput (HT) PHY specification) frames~~DSSS, HR/DSSS, OFDM, ERP and HT PPDUs [not VHT?] is enabled.”.

Add the following between 54.29 and 54.30: “HT-DSSS/CCK HT PHY using DSSS or CCK modulation”.

Add “HT-” before “DSSS/CCK” at 870.45, 872.5 (twice), 872.6, 872.7, 872.10, 872.11, 1680.58, 1680.60 (twice), 1681.1, 1681.2, 1681.4, 1681.5, 1681.8, 1681.11, 1681.13, 1681.16, 3009.10 (second instance), 3009.11, 3009.12.

Change “HT DSSS/CCK” to “HT-DSSS/CCK” at 3009.10.

TVHT?

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3393.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3523  Mark Hamilton  8.2.4.1.7  554.54 | The rules in 8.2.4.1.7 are not consistent with 10.2.2.2.  The concepts "MMDU is bufferable" and "PM bit is reserved" need to be separated. It makes no sense to say that an Action MMDU sent by a non-AP STA is bufferable, for example, just because you want to be able to say that the PM is valid in the MPDUs used to send it.  The exception for the PM bit in Probe Responses sent in response to unicast Probe Requests in an IBSS makes no sense  It's not clear enough which Control MPDUs have non-reserved PM bits and when. Note for example that 8.2.4.1.7 implies the PM bit in ACKs sent by a non-AP STA are not reserved. | Consider documents 11-12/1199 and 11-13/0131 |

Discussion:

Hear, hear.

Summary of changes:

* Tighten up the language about which frames the PMsf is valid
* Remove duplication and break infinite loops between 8.2.4.1.7 and 10.2
* Move format stuff to clause 8
* Give more examples and put them together
* Change “PM” to “Power Management” and “field”/ “bit” to “subfield” (except in clause 8, where it is endemic and will need to be done in one go under a separate change, and in clause 11, where it is similarly wider)
* Restrict “may be set to any value” to “when not reserved”, in the context of WNM-sleep mode
* Editorial fixes

Proposed changes:

**8.2.4.1.7 Power Management field**

The Power Management field is 1 bit in length and is used to indicate the power management mode of a STA. The value of this field is either reserved (as defined below) or remains constant in each frame from a particular STA within a frame exchange sequence (see Annex G)~~. The value~~, in which case it indicates the mode of the STA after the successful completion of the frame exchange sequence.

NOTE 1—This means the Power Management field is the same for all MPDUs in an A-MPDU.

In an infrastructure BSS or an IBSS, the following applies:

— The Power Management field is valid only in certain frames transmitted in an infrastructure BSS by a non-AP STA in certain frame exchanges, as described in 10.2.2.2 (STA Power Management modes), and in certain frames transmitted in an IBSS, as described in 10.2.3.4 (STA power state transitions).

— When the Power Management field is valid~~In such exchanges~~, a value of 1 indicates that the STA will be in PS mode. A value of 0 indicates that the STA will be in active mode.

— When the Power Management field is not valid, t~~T~~he ~~Power Management~~ field is reserved ~~in all~~.

NOTE 2—Examples of frames where the Power Management field is reserved are Management frames transmitted by a STA to an AP with which it is not associated, PS-Poll frames, and~~.~~

~~— The Power Management field is reserved in all~~ frames transmitted by ~~the~~an AP.

NOTE 3—A non-AP STA might set the Power Management field to 1 in frames such as PS-Poll frames to maximise interoperability with existing implementations. However, since this field is reserved, an AP ought not to consider a PS-Poll frame with a Power Management field equal to 0 as indicating that the STA will be in active mode if it is currently in PS mode.

~~In an IBSS, the Power Management field is valid only in frame exchanges as described in 10.2.3.4 (STA power state transitions). In such exchanges, a value of 1 indicates that the STA will be in PS mode. A value of 0 indicates that the STA will be in active mode.~~

**10.2.2 Power management in a non-DMG infrastructure network**

**10.2.2.1 General**

~~A STA that is associated with an AP and that~~ In order to change~~s~~ Power Management mode, a STA that is associated with an AP shall inform the AP of this fact using the Power Management subfield~~bits~~ within the Frame Control field of transmitted frames. The STA shall remain in its current Power Management mode until it successfully informs the AP of ~~a~~the Power Management mode change ~~via a frame exchange that includes an acknowledgment from the AP. Power Management mode shall not change during any single frame exchange sequence, as described in Annex G~~.

~~NOTE—This means the Power Management bit is the same for all MPDUs in an A-MPDU.~~

A STA may use both WNM-Sleep mode and PS mode or active mode simultaneously. Prefer “use WNM-sleep mode simultaneously with PS mode or active mode” to lessen possible precedence confusion? Or “may simultaneously use WNM-sleep mode and PS mode, or WNM-sleep mode and active mode”? Or two sentences?

~~The PM bit of the Frame Control field may be set to 0 or 1 within a frame sent by a STA in WNM-Sleep mode.~~

**10.2.2.2 STA Power Management modes**

To change Power Management mode~~s~~, a STA shall inform the AP through a ~~successful~~ frame exchange ~~as described in~~ (see Annex G)~~,~~ that:

* is initiated by the STA, ~~and that~~
* includes a Management, Extension or Data frame, and ~~that~~
* necessarily includes an Ack or a BlockAck frame from the AP.

NOTE—Examples of frame exchange sequences that cannot be used by a STA to change Power Management mode include sequences initiated by the AP, BlockAckReq-BlockAck sequences (because these only include Control frames) and sequences starting from a PS-Poll frame (because these do not necessarily result in an Ack frame from the AP, given the possibility of an immediate Data frame response). How about Probe Requests to an associated AP? In 2007 these did not carry a valid PM bit, but now they do? What about Auth/(Re)Assoc/Deauth/Disassoc (PM doesn’t make much sense if not associated)?

The Power Management subfield~~(s)~~ in the Frame Control field of the frame(s) sent by the STA in this exchange indicates the Power Management mode that the STA shall adopt upon reception of the Ack or BlockAck frame from the AP.~~successful completion of the entire frame exchange, except where it is reserved (see 8.2.4.1.7 (Power Management field)). A non-AP~~ The STA shall not change power management mode ~~using a frame exchange that~~ if it does not receive an Ack or BlockAck frame from the AP~~, or using a BlockAckReq frame~~.

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

~~NOTE 2—The Power Management subfield is ignored in frame exchanges initiated by the AP.~~

~~To change Power Management mode,~~ In the case of a STA that is coordinated by an MM-SME ~~shall inform the AP through a successful frame exchange initiated by the STA. The Power Management bit in the Frame Control field of the frame sent by the STA in this exchange indicates the Power Management mode that~~ the change applies to all the STAs coordinated by the MM-SME ~~and advertised in the MMS element sent by the STA shall adopt upon successful completion of the entire frame exchange. To change the Power Management mode of the coordinated STA, the frame may be sent~~ and may be performed using any of the MMSLs within the MMSL cluster established with the AP. Why is this DMG thing in a subclause for “Power management in a non-DMG infrastructure network” anyway?

**10.2.2.5 Power management with APSD**

**10.2.2.5.1 Power Management with APSD procedures**

A QoS STA~~s~~ uses the Power Management subfield in the Frame Control field of a frame to indicate whether it is in active or PS mode. As APSD is a mechanism for the delivery of downlink data and bufferable Management frames to power-saving STAs, the frames transmitted by a STA in PS mode that is using APSD have the Power Management subfield~~bit~~ in the Frame Control field set to 1, when it is not reserved (see 8.2.4.1.7 and 10.2.2.2), thereby causing buffering to take place at the AP.

**10.2.2.14 TDLS Peer Power Save Mode**

After the successful PSM setup, a STA informs its TDLS peer STA that it will enter power save mode per direct link by setting the Power Management subfield to 1 in an MPDU requiring acknowledgment. The STA enters power save mode after successful transmission of the MPDU. The power save status on one direct link is independent of the power save status on other links (direct or with the AP) the STA may have.

**10.2.2.15 TDLS Peer U-APSD**

**10.2.2.15.1 General**

A STA that configured TDLS Peer U-APSD at a TDLS peer STA enters power save mode on a TDLS direct link after the successful transmission to the TDLS peer STA over the direct link of an acknowledged MPDU with the Power Management subfield equal to 1. The STA that transmitted the frame with the Power Management subfield equal to 1 is then referred to as a TPU sleep STA. The STA that received the frame with the Power Management subfield equal to 1 is referred to as a TPU buffer STA. A TPU sleep STA may be a TPU buffer STA at the same time and on the same link, by sending a frame to the TDLS peer STA with the Power Management subfield of the Frame Control field set to 1 (this transmission will be preceded by the transmission of a Peer Traffic Indication frame and the subsequent receipt of a trigger frame that starts a service period). The power save status on one direct link is independent of the power save status on other links (direct or with the AP) the STA may have.

**10.2.3 Power management in an IBSS**

**10.2.3.4 STA power state transitions**

A STA may enter PS mode if the value of the ATIM window in use within the IBSS is greater than 0. A STA shall not enter PS mode if the value of the ATIM window in use within the IBSS is equal to 0. A STA shall indicate its power management mode using~~set~~ the Power Management subfield in the Frame Control field of frames containing all or part of a BU [this seems wrong – BUs are for “downlink”, not “uplink”] or individually addressed Probe Request frame that it transmits ~~using the rules in 8.2.4.1.7 (Power Management field)~~. [no “acknowledgement” stuff?]

**10.2.6 Power management in a PBSS and DMG infrastructure BSS**

**10.2.6.2.2 Power management mode operation of a non-AP and non-PCP STA with no wakeup schedule**

A non-AP and non-PCP STA that has not set up a wakeup schedule with the AP or PCP is in Active mode and every beacon interval is an Awake BI. The non-AP and non-PCP STA shall enter PS mode only after a successful frame exchange as described in Annex G, initiated by the non-AP and non-PCP STA and that includes an acknowledgment from the AP or PCP. The Power Management subfield set to 1 in the Frame Control field of the frame sent by the STA is used to indicate such a transition.

**10.42 Notification of operating mode changes**

NOTE 4—It might take a long time for a STA to change its operating mode following the transmission of the Operating Mode Notification frame and during that time the STA might not be able to receive frames resulting in frame loss. If a non-AP STA cannot tolerate frame loss during that period it can set the Power Management subfield of the Frame Control field of the Operating Mode Notification frame to 1 to indicate that the STA has entered power save. When the non-AP STA has completed its operating mode change, it can send another frame (such as a QoS Null) with the Frame Control Power Management subfield set to 0 to indicate that the STA has exited power save.

**11. Security**

Power Management bit (bit 12) masked to 0 [2 instances] Change the first “bit” to “subfield” for all the subfields.

Also, change “power management modes” to “power management mode” at 1560.57 and 2852.15.

Proposed resolution:

REVISED

Make the changes described in $thisdoc under “Proposed changes:” for CID 3523.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 3392  Mark RISON  9.6  1272.11 | "A STA shall support the concurrent reception of fragments of at least three MSDUs or MMPDUs. [...]  The destination STA shall maintain a Receive Timer for each MSDU or MMPDU being received, for a minimum of three MSDUs or MMPDUs." -- does this always apply (e.g. DMG STAs -- see end of 9.5 and 9.22.2.1; also what about the risk of MSDU/MMPDU reordering caused by concurrent reception causing replay detection to discard MSDUs/MMPDUs)? | If it doesn't apply to all STAs, add suitable caveats |

Discussion:

**9.5 Fragmentation**

Except when using block ack, a DMG STA shall complete the transmission of a fragmented MSDU before

starting transmission of another MSDU with the same TID of the fragmented MSDU.

[“we are quite sure there is text somewhere else that does require this for all STAs. Need to recall that discussion (from the F2F in San Antonio) and find the cite. Will reconsider on the next telecon, and confirm that we've covered all the cases, and determined whether there are any special cases or not (after refreshing the memory of the F2F discussion, as well).” OK, where?]

**9.6 Defragmentation**

A STA shall support the concurrent reception of fragments of at least three MSDUs or MMPDUs. Note that a

STA receiving more than three fragmented MSDUs or MMPDUs concurrently may experience a significant

increase in the number of frames discarded.

The destination STA shall maintain a Receive Timer for each MSDU or MMPDU being received, for a

minimum of three MSDUs or MMPDUs.

[Note: both these fragments appear in 802.11-1999. So this is nothing to do with EDCA reordering.]

**9.8 MSDU transmission restrictions**

To avoid reordering MSDUs between pairs of LLC entities and/or unnecessarily discarding MSDUs, the

following restrictions shall be observed by any STA that is able to concurrently process multiple outstanding

MSDUs for transmission. The term *outstanding* refers to an MPDU containing all or part of an MSDU or

MMPDU for which transmission has been started, and for which delivery of the MSDU or MMPDU has not

yet been completed (i.e., an acknowledgment of the final fragment has not been received and the MSDU or

MMPDU has not been discarded due to retries, lifetime, or for some other reason). A STA may have any

number (greater than or equal to one) of eligible MSDUs outstanding concurrently, subject to the restrictions

below.

A non-QoS STA shall not have more than one MSDU or MMPDU from a particular SA to a particular

individual RA outstanding at a time.

NOTE 1—A simpler, more restrictive alternative to the rule in the above paragraph that may be used is that no more than

one MSDU with a particular individual RA be outstanding at a time.

[The “simpler, more restrictive alternative” seems to ensure that a STA will never have to support concurrent reception of fragments of more than one MSDU/MMPDU. So is all the fuss for non-QoS about the case where you have MSDUs from multiple SAs being sent to/via the same AP?!]

For frames that are not sent within the context of a block ack agreement, a QoS STA shall not have more than

one MSDU or A-MSDU for each TID or MMPDU from a particular SA to a particular individual RA

outstanding at any time.

NOTE 2—A simpler, more restrictive alternative to the rule in the above paragraph that may be used is that no more than

one MSDU or A-MSDU with any particular TID with a particular individual RA be outstanding at any time.

[Ditto, though on a per-TID basis. But as noted above the “three concurrent” thing pre-dates TIDs.]

**9.22.2 HCF contention based channel access (EDCA)**

**9.22.2.1 Reference model**

A DMG STA may implement a single AC. If the STA implements a single AC, all UP and frame types shall

be mapped to AC\_BE.

NOTE—A DMG STA that implements a single AC has only one queue in Figure 9-23 (Reference implementation

model when dot11AlternateEDCAActivated is false or not present).

[Where is the stuff which explains how stuff is taken off queues? Is it just that each queue is a pseudo-STA fed DUs one at a time?]

**11.4.3.4 CCMP decapsulation**

**11.4.3.4.4 PN and replay detection**

h) The receiver shall discard MSDUs and MMPDUs whose constituent MPDU PN values are not

sequential.

[What exactly does “sequential” mean?] [Not in GCMP.]

**References:**

802.11mc/D3.0