IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11mc/D4.0 (SBmc1) | | | | |
| Date: 2015-07-31 | | | | |
| 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 CIDs 5062, 6075, 6214, 6215, 6216, 6305, 6306, 6308, 6375, 6376, 6377, 6389, 6390, 6404, 6482, 6496, 6506, 6562, 6563, 6573, 6576, 6582, 6583, 6625, 6661, 6716, 6754, 6771, 6795, 6820, 6824 on 11mc/D4.0. Green indicates material agreed to in the group, yellow material to be discussed, red material rejected by the group and cyan material not to be overlooked. The “Final” view should be selected in Word.

r1: changes made before and during BRC meeting on 2015-06-17.

r2: changes made before and during BRC meeting on 2015-06-18. CID 6482 has been left mid-way through major surgery.

r3: changes made before and during BRC meeting on 2015-06-19. Added CIDs 6625, 6824.

r4: changes made before and during BRC meeting in Waikoloa and on 2015-07-31. Added CIDs 5062, 6573, 6576, 6582, 6661, 6716, 6754, 6771, 6795, 6820.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6562  Mark RISON | The exception for the PM bit in Probe Responses sent in response to unicast Probe Requests in an IBSS makes no sense | Get rid of this special case (in 3.2, 8.2.4.1.7 and 10.2.2.4) |
| CID 6563 Mark RISON  10  1529 | Lots of things are ambiguous/unclear in relation to power-saving signalling and mechanisms | I will propose text (not possible to give here) |
| CID 6075  Mark Hamilton  8.2.4.1.7  566.52 | The details of when the PM subfield is valid are still a bit murky. (This is a follow-on comment to changes already made which improved things, but left a bit of work to do.) Also, PM should be discussed as a field/subfield, not a "bit". | A submission will be made by Mark Rison/Mark Hamilton with specific proposed changes. |

Discussion:

[Work in progress!]

*1) IBSS issue 1*

10.2.3.4 [IBSS] STA power state transitions says:

A STA shall set the Power Management subfield in the Frame Control field of frames containing all or part of a BU or individually addressed Probe Request frame that it transmits using the rules in 8.2.4.1.7 (Power Management field).

8.2.4.1.7 says:

In an IBSS, the Power Management field is valid only in frame exchanges as described in 10.2.3.4 (STA power state transitions).

This is circular.

*2) IBSS issue 2*

10.2.3.5 ATIM frame and frame transmission says:

l) A non-DMG STA may transmit individually addressed or group addressed Null Data frames within the ATIM window to indicate the STA’s intent to change power management modes. The STA may transition into PS mode after acknowledgments have been successfully received for all individually addressed Null Data frames or after the STA has transmitted group addressed Null Data frames at least dot11BSSBroadcastNullCount times.

The problem with using individually-addressed frames is that you never really know who’s in the IBSS. It would be far more robust (and simpler and faster too) to just spam out group-addressed frames.

Furthermore, the wording appears to allow the STA to indicate PS mode but not transition to it, and does not address transitioning back to AM.

*3) IBSS issue 3*

10.2.3.4 [IBSS] STA power state transitions says a STA’s PM mode is indicated in frames containing all/part of a BU, and in certain Probe Request frames (see excerpt above). 10.2.3.5 ATIM frame and frame transmission, though, says that the STA signals changes to PM mode in (QoS) Null frames. Such frames do not contain all/part of a BU (and are not Probe Request frames, obviously).

Note the definition of BU is:

**bufferable unit (BU)**: An MSDU, A-MSDU (HT STAs and DMG STAs only) or bufferable MMPDU that is buffered to operate the power saving protocol.

Proposed changes:

Make the following changes in the indicated subclauses:

**8.2.4.1.7 Power Management field**

In an IBSS, the Power Management field is valid only in certain frame ~~exchange~~s as described in 10.2.3.4 (STA power state transitions). In such ~~exchanges~~frames, 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.

**10.2.3.4 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. ***<paragraph break>***

A STA shall indicate its power management mode in~~set~~ the Power Management subfield ~~in~~of the Frame Control field of frames containing all or part of a BU or individually addressed Probe Request frame, or (QoS) Null frames, that it transmits ~~using the rules in 8.2.4.1.7 (Power Management field)~~.

**10.2.3.5 ATIM frame and frame transmission**

To change power management mode, a~~A~~ non-DMG [where are the rules of DMG IBSSen, then?] STA shall transmit (QoS) Null frames within the ATIM window. The STA should transmit group addressed (QoS) Null frames, and may transmit ~~individually addressed or group addressed~~ (QoS) Null ~~Data~~ frames individually addressed to all other STAs in the IBSS ~~within the ATIM window to indicate the STA’s intent to change power management modes~~. The STA ~~may~~shall not transition into or out of PS mode ~~after~~unless it has ~~acknowledgments have been successfully~~ received acknowledgements from all other STAs in the IBSS ~~for all individually addressed Null Data frames~~ or ~~after the STA~~it has transmitted group addressed (QoS) Null ~~Data~~ frames at least dot11BSSBroadcastNullCount times.

**C.3 MIB Detail**

dot11BSSBroadcastNullCount OBJECT-TYPE

SYNTAX Unsigned32 (~~1~~0..64)

*[…]*

This attribute specifies the number of group addressed (QoS) Null ~~Data~~ frames an IBSS STA ~~may~~ transmits before it changes power management mode. The value 0 indicates the STA uses individually addressed (QoS) Null frames to change power management mode."

Proposed resolution:

[Work in progress!]

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6390  Mark RISON | As regards the listen interval (CID 3363), there are three formulations, which generally seem to follow the following rules:  - ListenInterval: the parameter in the MLME-(RE)ASSOCIATE.request, which the non-AP STA sets  - Listen Interval: the field in the (Re)Association Request, which the AP gets  - listen interval: the general notion (mostly used by security handshake timeout descriptions)  However, the wording is not always consistent. | I will propose text (not possible to give here) |

Discussion:

As the commenter says, one should distinguish the MLME SAP parameter from the MMPDU field from the general notion.

Proposed changes:

Make the following changes:

* 177.12 and 190.50 to "listen interval ~~value~~"
* 651.27 to "The value of this ~~parameter~~field is the ListenInterval parameter of the MLME-ASSOCIATE.request or MLME‑REASSOCIATE.request primitive" [note deletion of the space in “Listen Interval”, not hyphen]
* 651.42 to "An AP uses the ~~L~~listen ~~I~~interval ~~information~~ in determining the lifetime of frames that it buffers for a STA.".
* 657.37 to "Association denied because the ~~L~~listen ~~I~~interval is too large"
* 1549.4 to "A STA operating in PS mode that is not in WNM-sleep mode shall periodically listen for Beacon frames, as determined by the ~~STA’s~~ ListenInterval parameter of the MLME-ASSOCIATE.request or MLME‑REASSOCIATE.request primitive and the ReceiveDTIMs parameter ~~in~~of the MLME‑POWERMGT.request primitive"
* 1557.53 to "The AP may base the aging function on the ~~L~~listen ~~I~~interval ~~specifi~~indicated by the STA in ~~the~~its (Re)Association Request frame"
* 1559.20 to "The STA shall wake up early enough to be able to receive the first Beacon frame scheduled for transmission at the time corresponding to the last TBTT for which the STA was awake plus the time interval indicated by the ListenInterval parameter of the MLME-ASSOCIATE.request or MLME‑REASSOCIATE.request primitive."
* 1561.10 to "Any AP aging function shall not cause the buffered BU to be discarded after any period that is shorter than ~~the Listen Interval of~~ that indicated by the STA for which BUs are buffered, in the Listen Interval field of its (Re)Association Request frame."

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6390 in <this document>, which distinguish the MLME SAP parameter from the MMPDU field from the general notion.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6404  Mark RISON  8.2.5.2  591.37 | The first para of 8.2.5.2 is full of horrors | I will propose text (not possible to give here) |

Discussion:

591.37 says “Within a frame (excluding [what does this mean? How is a class of duration settings present within a frame anyway?] Data frames containing QoS CF-Poll [is this the same thing as “QoS (+)CF-Poll frame”? And why would such a frame be “transmitted under EDCA” rather than HCCA?], PSMP frames [but including the frames polled by the PSMP? And isn't PSMP a non-EDCA exchange (cf. 8.2.5.6, 594.40)? This contradicts the sentence “PSMP frames always use multiple protection.” below, anyway], and frames that have the RDG/More PPDU subfield equal to 1 [this contradicts the sentence “Frames that have the RDG/More PPDU subfield equal to 1 always use multiple protection” below] [There’s no Duration in a PS-Poll; doesn’t this potentially “initiate a TXOP” too?]) transmitted under EDCA by a STA that initiates a TXOP, there are two classes of duration settings”.

Proposed changes:

Change from 591.37 as follows

~~Within a frame (excluding Data frames containing QoS CF-Poll, PSMP frames, and frames that have the RDG/More PPDU subfield equal to 1)~~ In transmi~~tted~~ssions under EDCA by a STA that initiates a TXOP, there are two classes of duration settings: single protection and multiple protection. In single protection, the value of the Duration/ID field of the frame can set a NAV value at receiving STAs that protects up to the end of any following Data, Management, or response frame plus any additional overhead frames as described below. In multiple protection, the value of the Duration/ID field of the frame can set a NAV that protects up to the estimated end of a sequence of multiple frames. ~~Frames that have the RDG/More PPDU subfield equal to 1 always use multiple protection. PSMP frames always use multiple protection.~~***<paragraph break>***

The STA selects between single and multiple protection when it transmits the first frame of a TXOP. All subsequent frames transmitted by the STA in the same TXOP use the same class of duration settings. A STA always uses multiple protection in a TXOP that includes:

* Frames that have the RDG/More PPDU subfield equal to 1
* PSMP frames
* VHT NDP Announcement frames ~~and~~or Beamforming Report Poll frames ~~always use multiple protection settings.~~

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6404 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6389  Mark RISON  10.42  1847.31 | The requirement for an AP to notify (re)associating STAs that it is operating with reduced max NSS is not clearly expressed. Part of the problem is that the text talks of "changes in" max NSS, but from the perspective of a (re)associating STA (except special case of reassociating to the same AP) this is meaningless.  [The OMN element appears in Beacons, Probe Responses, (Re)Association Requests/Responses, TDLS Setup Responses, TDLS Setup Confirms, Mesh Peering Opens, Mesh Peering Confirms, and of course OMN frames.] | I will propose text (not possible to give here) |

Discussion:

As it says in the comment. OMN applies to both sides of a link, so the wording should be general enough to reflect this.

Proposed changes:

Make the following changes at 1847.39:

A STA that is operating mode notification capable and that transmits a Beacon or group addressed Probe Response frame or that transmits a~~n~~ Probe Response, Association Request, Association Response, Reassociation Request, Reassociation Response, TDLS Setup Response, TDLS Setup Confirm, Mesh Peering Open, or Mesh Peering Confirm frame to a STA that is operating mode notification capable should ~~notify the recipient STA of a change in its operating mode~~ signal that the maximum number of spatial streams it is able to receive is less than that indicated in the HT Capabilities element in the frame and, if present, the VHT Capabilities element in the frame by including the Operating Mode Notification element in the frame.

A first STA that is operating mode notification capable should notify a second STA that is operating mode notification capable of a change in its operating mode by transmitting an Operating Mode Notification frame to the second STA if the first STA has established any of the following with a second STA:

— An association ~~with an AP~~ in an infrastructure BSS

— A TDLS link

— A DLS link

— A Mesh Peer relationship

NOTE 1—Notify Channel Width frames and elements are used to signal STA operating channel width changes to and from STAs that are not operating mode notification capable.

Make the following changes at 1849.4:

An AP shall not include the Operating Mode Notification element in Beacon, Probe Response, Association Response, and Reassociation Response frames when ~~not changing~~ the maximum number of spatial streams the AP is able to receive is the same as that indicated in the HT Capabilities element and, if present, the VHT Capabilities element.

A STA shall not transmit in an individually addressed frame an Operating Mode field with the value of the Rx NSS subfield indicating a number of spatial streams not supported by the recipient STA. ***<paragraph break>***

***<smaller font>***NOTE 2—The number of spatial streams supported by the recipient HT STA is reported in the ~~Supported Rates element, Extended Supported Rates element,~~ Supported MCS Set field in the HT Capabilities element~~, or~~ and the Supported VHT-MCS and NSS Set field in any VHT Capabilities element transmitted ~~in Management frames~~ by the ~~recipient~~ STA.

A STA shall not transmit in an individually addressed frame an Operating Mode field with the value of the Channel Width subfield indicating a bandwidth not supported by the recipient STA~~, as~~. ***<paragraph break>***

***<smaller font>***NOTE 3—The bandwidth supported by the recipient HT STA is reported in the Supported Channel Width Set subfield in the HT Capability Information field in the HT Capabilities element ~~or the~~ and the Supported Channel Width Set subfield of the VHT Capabilities Info field of any VHT Capabilities element ~~in Management frames~~ transmitted by the STA.

A STA that is operating mode notification capable shall not transmit a PPDU to a STA that uses a bandwidth that is greater than the channel width indicated in the most recently received Operating Mode Notification element or Operating Mode Notification frame from that STA. A STA that is operating mode notification capable shall not transmit a PPDU to a STA that uses a greater number of spatial streams than indicated in the most recently received Operating Mode Notification element or Operating Mode Notification frame ~~received~~ from that STA.

Increment by 2 the number of NOTEs 2 onwards.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6389 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6214  Mark RISON | There are references to "physical carrier sense", "virtual carrier sense" and "physical CS" and "virtual CS" but the terms are never defined | Define the terms. Arguably, virtual CS is defined at 1247.61 (though why it is "referred to as the NAV" is unclear -- or maybe virtual CS also includes considering the medium busy for the duration indicated in a received PPDU header?), but physical CS is not well-defined. 1247.57 says each PHY provides the details, but the term is only used at 2280.45 and merely reflects back to the PHY. Something needs to tie "physical CS" with the zoo of CS/CCA/energy detect/ED/blahblahblahPHYwibblings terminology used in each PHY |
| CID 6215  Mark RISON | Use "CS" rather than "carrier sense" except when defined etc. | Use "CS" rather than "carrier sense" at 74.14, 833.8, 1239.15, 1664.39, 1664.40, 3187.59 (2x), 860.43, 864.52, 1378.5, 1679.57, 2184.52, 2437.59 |
| CID 6216  Mark RISON | The terms PHYCS and PHYED are defined but barely used | Delete them from subclause 3.4 and replace them in the other locations with their full-fat equivalents, i.e. physical CS and physical ED (4 instances each) |
| CID 6305  Mark RISON | There is a zoo of inconsistent terminology for "carrier sense", whch makes it hard to understand exactly what is meant where and how the various PHYs compare: CS, CCA, CS/CCA, energy detect, ED, PHYED, CCA-ED, CCA Mode 1-5 | First rename CCA-ED to PHYRED (regulatory ED). Then call the ED which everybody uses PHYED, and the preamble detect PHYPD. Call the combination of things which yield the PHY part of "carrier sense" PHYCS. Kill the terms CS, CCA, CS/CCA, CCA Mode, ED. Make it clear how "I'm currently transmitting" fits into "carrier sense", and whether "I've received the PPDU header so I know how long to consider the medium busy even though the energy has gone away" is considered part of PHYCS or part of MACCS/virtual CS |
| CID 6306  Mark RISON | "CCA-ED" just confuses everyone, because everyone thinks it means CCA using ED, when in fact it means some wacko mode of operation in wacky regulatory domains/bands | Rename CCA-ED to something more obscure, so that people can use this term for the CCA-ED which is actually used in practice |

Discussion:

[Work in progress!]

Whereas:

1. CS (as in “CSMA/CA”) consists of the following, where any causes the medium to be considered busy (1248.9: “The CS mechanism combines the NAV state and the STA’s transmitter status with physical CS to determine the busy/idle state of the medium”):
   1. NAV
      1. The network allocation vector, set by Duration fields (1247.61: “A virtual CS mechanism shall be provided by the MAC. This mechanism is referred to as the NAV.”)
   2. Local tx in progress
      1. Delineated by PHY-TXSTART.request and PHY-TXEND.request
   3. CCA
      1. Delineated by PHY-CCA.indication (BUSY) and PHY-CCA.indication (IDLE) (1247.56: “A physical CS mechanism shall be provided by the PHY. See Clause 7 (PHY service specification) for how this information is conveyed to the MAC. The details of physical CS are provided in the individual PHY specifications.”)
2. CCA consists of one or more of the following (depending on the PHY and in some cases on the CCA mode), where any causes the medium to be indicated as busy (via PHY-CCA.indication):
   1. CCA-ED is energy detect
      1. This is typically at 20 dB above the sensitivity
   2. CCA-PD is PPDU detect (which holds CCA busy for the duration indicated in the PPDU header)
      1. L-SIG TXOP protection relies on this
      2. Note PHY-RXSTART.indication and PHY-RXEND.indication are independent of this (e.g. carrier might be lost before the end of the PPDU as indicated in the PPDU header)
   3. CCA-SD is signal detect (i.e. detection of symbols generated by a particular PHY)
      1. Note some modes (e.g. “CCA mode 3” for DSSS) have an energy threshold too
      2. Note some modes (e.g. “CCA mode 4” for HR/DSSS) have a timer too
   4. CCA-RED is regulatory energy detect (only applicable to the 3G6 band in the FCC regulatory domain)
   5. CCA-SCSD is signal detect on a non-primary channel (only applicable to the VHT and TVHT PHYs)

This is illustrated graphically in the following figure (I am grateful to Guido HIERTZ for the starting design):



Here is the zoo of existing terminology, and how it maps to the terminology above:

|  |  |  |
| --- | --- | --- |
| Term | Location | Meaning |
| virtual CS mechanism  virtual carrier sense mechanism  virtual carrier sense (CS) mechanism  virtual carrier sense  virtual CS  virtual CS indication  virtual CS condition | 25.8, 74.14, 1239.15 (obsolete – PCF), 1243.14, 1243.17, 1246.24, 1247.5, 1247.33, 1247.61, 1248.11, 1248.14, 1252.39, 1270.34, 1271.32, 1358.25, 1358.28, 1665.14, 2276.35, 2977.53 | NAV [only] |
| physical or virtual carrier sense  (CS) mechanism  physical or virtual CS mechanism  physical or virtual CS  PHY and virtual CS mechanisms  the virtual carrier sense mechanism or  the physical carrier sense mechanism  Physical and virtual CS functions  the CS function provided by the PHY, the virtual CS function provided by the MAC via the NAV  the NAV and physical CS | 833.8, 1247.52, 1252.48, 1268.8, 1323.24, 1327.36, 1358.24, 1358.30, 1664.39, 1700.43, 3187.59 | CS mechanism [including “local tx”] |
| physical CS mechanism  physical carrier sense mechanism  physical CS | 1247.56, 1247.57, 1248.9, 1271.4, 1271.13, 1324.54, 2280.45 | CCA |
| carrier sense mechanism  carrier-sense mechanism [hyphen sic]  “CS mechanism” [quotes sic] | 860.43, 864.52, 1378.5, 1679.57, 2280.44 | CS mechanism |
| PHYCS  PHY carrier sense (PHYCS) | 56.64, 2184.52, 2184.56, 2211.28, 2211.30 | CCA-PD |
| PHYED  PHY energy detection (PHYED) | 57.1, 2184.53, 2184.56, 2211.28, 2211.30 | CCA-ED |
| PHY CS/CCA  CS/CCA  carrier sense/clear channel assessment (CS/CCA) | 551.36, 2185.13, 2212.7, 2264.32 (better to reword to include next sentence too, i.e. say something like “including CCA-RED, for operating classes requiring this”), 2264.39, 2264.44, 2264.45, 2264.47, 2269.10, 2271.4, 2373.13, 2374.1, 2375.4, 2375.37, 2376.53, 2445.7, 2562.2, 2563.3, 3353.22, 3355.16 | CCA |
| CS/CCA | 3351.57 (delete the item immediately above) | CCA including CCA-RED |
| code lock | 2176.8 (2x) | CCA-SD? |
| IEEE Std 802.11 DSSS correlation | 2687.60 | DSSS PPDU detection |
| CS  high rate CS | 2717.24, 2717.26 | DSSS and HR/DSSS PPDU detection |
| CS | 2722.36 | DSSS, HR/DSSS and ERP PPDU detection |
| carrier sense | 3197.37, 3197.38, 3197.61, 3197.62, 3197.63, 3197.64, 3206.59, 3206.60, 3206.61, 3206.62 | PPDU detection |
| energy detection (ED) and/or code lock  ED and/or code lock | 2183.61, 2209.61 | CCA-ED and/or CCA-SD? |
| energy detect  energy  Energy  Energy Detection  CCA-ED energy | 2190.18, 2220.47, 2265.4, 2554.3, 2628.56, 2687.58, 2697.23, 2717.22, 2717.26, 2722.35, 3198.11 (also lowercase “Threshold”), 3205.35 (ditto) | ED |
| energy detect | 3197.36, 3197.38, 3197.60, 3197.62, 3197.64, 3206.58, 3206.60, 3206.62 | energy detection |
| energy detect or CS | 2196.18, 2227.19 | energy or signal detection |
| CCA-Energy Detect (CCA-ED)  CCA-ED [sometimes followed without space “Behavior” appended; this should be preserved]  CCA-Energy Detect  CCA-EnergyDetect | 2264.33 (+many others in this subclause), 2265.5, 2368.25 (+5 in next para), 2253.48 (+in subclause heading and many others in the subclause), 2627.59 (+in subclause heading and many others in the subclause), 2697.19, 3205.7 (also rename MIB variable + change “that” to “whether”), 3205.20 (ditto; also either delete “PHY” or prepend “OFDM”), 3205.35, 3332.13, 3336.5, 3336.8, 3339.36, 3339.38, 3339.40, 3347.11, 3347.12, 3347.15, 3351.56, 3351.63 | CCA-RED |

MIB changes also required:

dot11EDThreshold: should be stated to be in dBm with a UNITS, have a sensible range.

dot11TIThreshold: should be deleted (no apparent connection to anything (TI?)).

dot11OFDMEDThreshold: should be renamed to be dot11OFDMREDThreshold, be stated to be in dBm with a UNITS, have a sensible range, and have a DEFVAL of -72.

2227.5/6: “a high rate PHY signal”; 2227.22: “a valid high rate signal”; 2227.10: “a high rate PPDU” – all these include a DSSS signal, right? Note also 2227.37: “an equivalent High-Rate signal” [sic]

Make “The 3.65 ms timeout is the duration of the longest possible 5.5 Mb/s PSDU” in 17.3.8.5 a NOTE. Make the CCA wording consistent (at least for DSSS, HR/DSSS and ERP). What does the “only” in “report a medium busy condition only upon the detection of a high rate PHY signal” mean? Either have “at the antenna” everywhere or nowhere, and if present, make it say “at the antenna connector”. What does the “true” in “The CCA shall indicate true” mean? Is dot11EDThreshold needed (only present for DSSS and HR/DSSS)? Make sure everywhere includes aCCATime. “IDLE medium” should be “medium idle condition”. “is present at the start of the PHY slot” – the PHY does not have slots, and the only requirement is to detect within aCCATime.

Proposed resolution:

[Work in progress!]

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6482  Mark RISON  9.3.2.1  1248.21 | "AirDelay is aAirPropagationTime indicated in the Coverage Class field of the Country element received from the AP of the BSS with which the STA is associated or the DO of the IBSS of which the STA is a member or from another mesh STA in the same MBSS, or if no Country element has been received from the AP of the BSS with which the STA is associated, the value of aAirPropagationTime indicated in the PLME-CHARACTERISTICS.confirm primitive." is circular, because the PLME-CHARACTERISTICS.confirm gets info from the PHY characteristics, and the PHYs say "As indicated by the coverage class (see 9.21.4 (Operation with coverage classes))." | This would probably best be fixed in 9.21.4. Perhaps "The default PHY parameters are based on aAirPropagationTime having a value of 0 us" could be changed to something like "When dot11OperatingClassesRequired is false, or the aAirPropagationTime is not available from a Country element, the aAirPropagationTime shall be taken to be 0 us" |

Discussion:

As the commenter notes, aAirPropagationTime in PLME-CHARACTERISTICS.confirm is specified in all the PHYs (except DMG and TVWS) as being dynamic, per 9.21.4, which says you look at the Country element.

Some other issues arise: aAirPropagationTime only applies if dot11OperatingClassesRequired is true, and the situation with DMG and TVWS (which have a specified aAirPropagationTime) is not clear.

Proposed changes:

Change 1248.19 as follows:

At aRxTxTurnaroundTime + aAirPropagationTime~~Delay~~ + aRxPHYDelay + 10% of aSlotTime after each MAC slot boundary as defined in 9.3.7 (DCF timing relations) and 9.22.2.4 (Obtaining an EDCA TXOP), the MAC shall issue a PHY-CCARESET.request primitive to the PHY, where aAirPropagationTime is determined as described in 9.21.4 ~~AirDelay is aAirPropagationTime indicated in the Coverage Class field of the Country element received from the AP of the BSS with which the STA is associated or the DO of the IBSS of which the STA is a member or from another mesh STA in the same MBSS, or if no Country element has been received from the AP of the BSS with which the STA is associated, the value of aAirPropagationTime indicated in the PLME-CHARACTERISTICS.confirm primitive~~.

Change 1275.49 as follows (aSlotTime equation):

aAirPropagationTime is determined as described in 9.21.4~~the value indicated in the Coverage Class field of the Country element received from the AP of the BSS with which the STA is associated or the DO of the IBSS of which the STA is a member or from another mesh STA in the same MBSS, otherwise, the value indicated in the PLME-CHARACTERISTICS.confirm primitive~~

Change 1320.53 as follows:

~~The default PHY parameters are based on aAirPropagationTime having a value of 0 μs, and~~ aSlotTime and other MAC timings are based on the PHY timing parameters, as specified in 9.3.2.3 (IFS) and 9.3.7 (DCF timing relations), and in particular on aAirPropagationTime. ~~When~~If dot11OperatingClassesRequired is true, it is possible to manage the MAC timings of STAs ~~that can receive Beacon frames, DMG Beacon frames, or Probe Response frames that contain the Country element (8.4.2.9 (Country element)),~~ to increase fairness in contending for the medium. Radio waves propagate at ~300 m/μs in free space, and, for example, 3 μs would be the ceiling for BSS maximum one-way distance of ~450 m (~900 m round trip). The Coverage Class field of the Country element indicates ~~the~~a ~~new~~ value of aAirPropagationTime (see Table 8-76 (Coverage Class field parameters)), and the MAC can use the ~~new~~ value to calculate aSlotTime (as specified in the relevant PHY clause) and other timings. ***<paragraph break>***

~~When~~ If dot11OperatingClassesRequired is true and a Country element~~s~~ containing a ~~value for the~~ ~~c~~Coverage ~~c~~Class field has~~ve~~ been received ~~in Beacon frames, DMG Beacon frames, or Probe Response frames~~ from the AP of the BSS with which a STA is associated or from the DO of the IBSS of which a STA is a member or from another mesh STA in the same MBSS, an associated STA, or a dependent STA, or member of an IBSS, or member of an MBSS shall, if the relevant PHY clause specifies that aAirPropagationTime is indicated by the coverage class, use MAC timings that correspond~~s~~ to the ~~new~~ value of aAirPropagationTime indicated (as specified in the relevant PHY clause).

NOTE 1—Some PHYs do not specify a dependency of aSlotTime on aAirPropagationTime.

NOTE 2—Operation over larger BSS diameters is facilitated by relaxing some PHY timing parameters, while maintaining compatibility with existing implementations in small BSS diameters.

aAirPropagationTime is 0 μs if:

* the relevant PHY clause specifies that aAirPropagationTime is indicated by the coverage class, and
* at least one of the following applies:
* dot11OperatingClassesRequired is false
* no Country element containing a Coverage Class field has been received from the AP of the BSS with which a STA is associated or from the DO of the IBSS of which a STA is a member or from another mesh STA in the same MBSS

Using the Country element, an AP ~~or PCP~~, IBSS STA or MBSS STA can change ~~coverage class and~~ maximum transmit power level to enhance operation. ~~When~~If dot11OperatingClassesRequired and dot11ExtendedChannelSwitchActivated are true and the maximum transmit power level [which limit is this one referring to?] is different from the transmit power limit indicated by the operating class [OCs don’t indicate power limits; subband triplets do], the associated STA, or dependent STA, or member of an IBSS, or member of an MBSS shall operate at a transmit power at or below that indicated by the lesser of the two limits.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6482 in <this document>, which address the comment along the lines suggested.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6496  Mark RISON  9.3.2.3.3  1250.16 | Does the SIFS 10% of aSlotTime include aAirPropagationTime too? Seems large. There is no need to allow for 10% of the aAirPropagationTime as a STA's timing accuracy is independent of the aAirPropagationTime | Change to 10% of aSlotTime - aAirPropagationTime (2x in this subclause). See also 9.3.2.1's 10% and the 10%s in 9.3.2.3.10 and 9.3.2.3.11 |

Discussion:

The error on SIFS is to allow for timing inaccuracy at the STA responding after SIFS. This inaccuracy has no dependency on the BSS diameter, since it is purely local (note that an increased aAirPropagationTime increases aSlotTime but not aSIFSTime).

Note that the DMG and TVHT situation is less significant than the non-DMG non-TVHT situation, because for DMG aAirPropagationTime is < 0.1 μs and aSlotTime is 5 μs and for TVHT aAirPropagationTime is 3 μs and aSlotTime is 20 or 24 μs, while for other PHYs aAirPropagationTime can be up to 93 μs compared with an unadulterated aSlotTime of 9 or 20 μs.

Proposed changes:

Change 1248.19 as follows:

At aRxTxTurnaroundTime + AirDelay + aRxPHYDelay + 10% ~~of~~× (aSlotTime – aAirPropagationTime) after each MAC slot boundary

Change 1250.14 as follows:

non-DMG STA shall not allow the space between frames that are defined to be separated by a SIFS, as measured on the medium, to vary from the nominal SIFS by more than ±10% ~~of~~× (aSlotTime – aAirPropagationTime)

Change 1250.17 as follows:

DMG STA shall not allow the space between frames that are defined to be separated by a SIFS time, as measured on the medium, to vary from the nominal SIFS value by more than –0% or +10% ~~of~~× (aSlotTime – aAirPropagationTime).

Change 1253.17 as follows:

DMG STA shall not allow the space between frames that are separated by MBIFS time, as measured on the medium, to vary from the nominal MBIFS value by more than –0% or +10% ~~of~~× (aSlotTime – aAirPropagationTime).

Change 1253.27 as follows:

DMG STA shall not allow the space between frames that are separated by LBIFS time, as measured on the medium, to vary from the nominal LBIFS value by more than –0% or +10% ~~of~~× (aSlotTime – aAirPropagationTime).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6496 in <this document>, which address the comment in the manner suggested.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6308  Mark RISON | 18.3.10.6 CCA requirements says: "For improved spectrum sharing, CCA-ED is required in some bands. The behavior class indicating CCA-ED is given in Table D-2 (Behavior limits sets). The operating classes requiring the corresponding CCA-ED behavior class are given in E.1 (Country information and operating classes). A STA that is operating within an operating class that requires CCA-ED shall operate with CCA-ED. Unless required by regulation, the CCA-ED shall not be required for license-exempt operation.  CCA-ED shall indicate a channel busy condition when the received signal strength exceeds the CCA-ED threshold as given by dot11OFDMEDThreshold. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold)."  D.2.5 CCA-ED threshold says: "CCA-ED thresholds for operation in specific bands are given in E.2 (Band-specific operating requirements) where they differ from the values in PHY clauses."  So the OFDM PHY refers you to D.2.5 which refers you to E.2 except where the answer is the same as in the PHY clause ... but that's where you started! | Break the infinite loop. Define the CCA-ED thresholds in one place only |

Discussion:

10 REM PHY clauses

20 PRINT "The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5"

30 GOTO 1325

1325 REM D.2.5

1330 PRINT "CCA-ED thresholds for operation in specific bands are given in E.2 where they differ from the values in PHY clauses"

1340 IF NOT (differ) THEN GOTO 10

1350 GOTO 1402

1402 REM E.2

1410 PRINT “Here are the CCA-ED thresholds.”

The solution is to delete line 1340 above.

Proposed resolution:

REVISED

Delete “where they differ from the values in PHY clauses” at 3336.9.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6506  Mark RISON  20.3.20.5.1  2368.25 | This subclause starts "For the operating classes requiring CCA-Energy Detect (CCA-ED)" but examination of Annex E shows that the only operating classes requiring CCA-ED are in the 3G band and the maximum channel width is 20 MHz, so this subclause seems otiose at best and misleading at worst; ditto for TVHT | Delete this subclause; consider doing the same for TVHT since although 4.3.12 suggests VHT might be used in the 3G band this is not actually the case in practice |

Discussion:

This was discussed in Vancouver and the outcome was:

REVISED (GEN: 2015-05-12 00:34:20Z) - At 2368.32, add "NOTE--The CCA-ED is not required for license-exempt operation in any band." and at 2264.57, 2553.57, 2628.44 change similar statements to NOTEs.

However, there are other inconsistencies among the PHYs which (potentially) use CCA-ED (OFDM, HT, VHT, TVHT).

Proposed changes:

Change 18.3.10.6 CCA requirements as follows:

The PHY shall indicate a medium busy condition by issuing a PHY-CCA.indication primitive when the carrier sense/clear channel assessment (CS/CCA) mechanism detects a channel busy condition. ***<paragraph break>***

For the operating classes requiring CCA-Energy Detect (CCA-ED), the PHY shall also indicate a medium busy condition when CCA-ED detects a channel busy condition

[…]

For improved spectrum sharing, CCA-ED is required in some bands. The behavior class indicating CCA-ED is given in Table D-2 (Behavior limits sets). The operating classes requiring the corresponding CCA-ED behavior class are given in E.1 (Country information and operating classes). ~~A~~The PHY of a STA that is operating within an operating class that requires CCA-ED shall operate with CCA-ED. ***<paragraph break>***

~~Unless required by regulation, the~~ ***<smaller font>***NOTE 2—CCA-ED ~~shall not be~~ is not required for license-exempt operation in any band.

CCA-ED shall indicate a channel busy condition when the received signal strength exceeds the CCA-ED threshold as given by dot11OFDMEDThreshold. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold).

NOTE ~~2~~3—The requirement to indicate a channel busy condition for any signal 20 dB above the minimum modulation and coding rate sensitivity (minimum modulation and coding rate sensitivity + 20 dB resulting in –62 dBm for 20 MHz channel spacing, –65 dBm for 10 MHz channel spacing, and –68 dBm for 5 MHz channel spacing) is a mandatory energy detect requirement on all Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification) receivers. Support for CCA-ED is an additional requirement that relates specifically to the sensitivities described in D.2.5 (CCA-ED threshold).

Change 20.3.20.5.1 CCA-Energy Detect (CCA-ED) as follows:

For the operating classes requiring CCA-Energy Detect (CCA-ED), the PHY shall also indicate a medium busy condition when CCA-ED detects a channel busy condition.

For improved spectrum sharing, CCA-ED is required in some bands. The behavior class indicating CCA-ED is given in Table D-2 (Behavior limits sets). The operating classes requiring the corresponding CCA-ED behavior class are given in E.1 (Country information and operating classes). ~~An HT~~The PHY of a STA that is operating within an operating class that requires CCA-ED shall operate with CCA-ED ~~as defined in 18.3.10.6 (CCA requirements)~~.

NOTE 1—CCA-ED is not required for license-exempt operation in any band.

CCA-ED shall indicate a channel busy condition when the received signal strength exceeds the CCA-ED threshold as given by dot11OFDMEDThreshold for the primary 20 MHz channel and dot11OFDMEDThreshold for the secondary 20 MHz channel. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold).

NOTE 2—The requirement to indicate a channel busy condition as stated in 20.3.20.5.2, 20.3.20.5.3 and 20.3.20.5.4 is a mandatory energy detect requirement on all Clause 20 receivers. Support for CCA-ED is an additional requirement that relates specifically to the sensitivities described in D.2.5 (CCA-ED threshold).

Change 22.3.18.5.2 CCA sensitivity for operating classes requiring CCA-ED as follows:

For the operating classes requiring CCA-Energy Detect (CCA-ED), ~~CCA~~the PHY shall also ~~detect~~indicate a medium busy condition when CCA-ED detects a channel busy condition.

For improved spectrum sharing, CCA-ED is required in some bands. The behavior class indicating CCA-ED is given in Table D-2 (Behavior limits sets). The operating classes requiring the corresponding CCA-ED behavior class are given in ~~Annex~~ E.1. ~~A~~The PHY of a STA that is operating within an operating class that requires CCA-ED shall operate with CCA-ED. ***<paragraph break>***

~~The~~ ***<smaller font>***NOTE 1—CCA-ED is not required for license-exempt operation in any band.

CCA-ED shall indicate a channel busy condition when the received signal strength exceeds the CCA-ED threshold as given by dot11OFDMEDThreshold for the primary 20 MHz channel ~~and~~, dot11OFDMEDThreshold for the secondary 20 MHz channel, dot11OFDMEDThreshold + 3 dB for the secondary 40 MHz channel, and dot11OFDMEDThreshold + 6 dB for the secondary 80 MHz channel. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold).

NOTE 2—The requirement to ~~issue~~indicate a ~~CCA signal~~channel busy condition as stated in 22.3.18.5.3 (CCA sensitivity for signals occupying the primary 20 MHz channel) and 22.3.18.5.4 (CCA sensitivity for signals not occupying the primary 20 MHz channel) is a mandatory energy detect requirement on all Clause 22 (Very High Throughput (VHT) PHY specification) receivers. Support for CCA-ED is an additional requirement that relates specifically to the sensitivities described in D.2.5 (CCA-ED threshold).

Change 23.3.18.6.2 CCA sensitivity for operating classes requiring CCA-ED as follows:

For the operating classes requiring CCA-Energy Detect (CCA-ED), ~~CCA~~the PHY shall also ~~detect~~indicate a medium busy condition when CCA-ED detects a channel busy condition.

For improved spectrum sharing, CCA-ED is required in some bands. The behavior class indicating CCA-ED is given in Table D-2 (Behavior limits sets). The operating classes requiring the corresponding CCA-ED behavior class are given in E.1 (Country information and operating classes). ~~A~~The PHY of a STA that is operating within an operating class that requires CCA-ED shall operate with CCA-ED. ***<paragraph break>***

~~The~~ ***<smaller font>***NOTE 1—CCA-ED is not required for license-exempt operation in any band.

CCA-ED shall indicate a channel busy condition when the received signal strength exceeds the CCA-ED threshold as given by dot11OFDMEDThreshold for the primary TVHT\_W channel ~~and~~, dot11OFDMEDThreshold for the secondary TVHT\_W channel and dot11OFDMEDThreshold + 3 dB for the secondary TVHT\_2W channel [no secondary TVHT\_4W?]. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold).

NOTE 2—The requirement to ~~issue~~indicate a ~~CCA signal~~channel busy condition as stated in 23.3.18.6.3 (CCA sensitivity for signals occupying the primary channel) and 23.3.18.6.4 (CCA sensitivity for signals not occupying the primary channel) is a mandatory energy detect requirement on all Clause 23 (Television Very High Throughput (TVHT) PHY specification) receivers. Support for CCA-ED is an additional requirement that relates specifically to the sensitivities defined in D.2.5.

Change 3332.13 as follows: “CCA shall also ~~detect~~indicate a medium busy condition when CCA-EnergyDetect detects a channel busy condition.”

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6506 in <this document>, which reject the thrust of the comment but harmonise the wording for the OFDM, HT, VHT and TVHT PHYs (which are the only PHYs subject to regulatory energy detection).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6583  Mark RISON | "All other bits are reserved, and are set to 0 on transmission and ignored on reception."; "the WEP Key ID subfield in the MPDU shall be set to 0 on transmit and ignored on receive."; "Bits 5 to 7 of the Nonce Flags field are reserved and shall be set to 0 on transmission."; "The reserved bits shall be set to 0 and shall be ignored on reception."; "If the value of Key Type (bit 3) is 0, then this bit shall be 0 on transmit and ignored on receive. "; "It shall be set to 0 on transmit and ignored on receive." | Simplifiy all of these to a statement of the form to "x is reserved", except the one which just says to set reserved bits to 0 on tx and ignore on rx, which can just be deleted.  Note, however, that the statement that reserved bits are set to 0 on tx and ignored on rx is only made within the scope of clause 8, so this needs to be widened to cover other clauses |

Discussion:

OK, so we need to extend the Clause 8 convention to other MAC clauses. Leave the last one alone, as it’s in the PHY and PHY people are a bit odd (e.g. often their reserved bits are set to 1!).

Proposed changes:

Change 561.46 as follows: “Reserved fields and subfields are set to 0 upon transmission and are ignored upon reception (this includes reserved fields and subfields in the security encapsulation in protected frame bodies, nonces and EAPOL-Key frames (see Clause 11)).”

Change 872.35 as follows: “~~set to 0 on transmit and is not used at the receiver~~reserved”.

Change 937.54 as follows: “~~0 on transmission and ignored upon reception~~reserved”.

Change 943.6 as follows: “~~An AP always sets Bits 4–6 to 0. A non-AP STA ignores Bits 4–6 on reception.~~Bits 4-6 are reserved.”

Change 963.53 as follows: “~~The requesting STA sets the Query Response Length Limit to 0 on transmission and the responding STA ignores it upon reception~~In this case, the Query Response Length Limit is reserved.” [lots of missing “field”s around here!]

Change 1001.14 as follows: “~~value of the~~ AID field is ~~ignored~~reserved”.

Change 1011.37 as follows: “~~value of the~~ PCP Active subfield is ~~ignored~~reserved”.

Change 1185.28 as follows: “~~0~~reserved for all BSSIDs ~~and ignored upon reception~~”.

Change 1870.34 as follows: “field ~~value~~ is ~~ignored~~reserved”.

Change 1870.52 as follows: “~~shall be set to 0 on transmit and ignored on receive~~is reserved”.

Delete 1912.3 (“The reserved bits shall be set to 0 and shall be ignored on reception.”).

Change 1914.50 as follows: “are reserved ~~and shall be set to 0 on transmission~~”.

Change 1964.14 as follows: “~~shall be 0 on transmit and ignored on receive~~is reserved”.

Change 1966.30 as follows: “~~value~~field ~~shall be set to 0 on transmit and shall not be used at the receive~~is reserved”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6583 in <this document>, which address the comment (including some missing instances of reserved quanta) as far as it pertains to MAC clauses.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6375 Mark RISON  10.3.5.3  1596.24 | "and an earlier, timed out SA Query procedure with the non-AP and non-PCP STA has not allowed a new association process to be started without an additional SA Query procedure," is extremely ambiguous: does the earlier procedure allow the new process, or disallow it? In fact, it allows it! The issue is that the precedence is not clear: "(an earlier SA) (has not) (allowed association)" v. "(an earlier SA) (has) (not allowed association)" | Reword to be clear; ditto in reassoc. Text like: "and there has been no earlier, timed out SA Query procedure with the STA (which would have allowed a new reassociation process to be started, without an additional SA Query procedure)" |
| CID 6376  Mark RISON  10.3.5  1593 | There are numerous editorial and consistency issues with the description of the AP/PCP (re)assoc receipt procedures | I will propose text (not possible to give here) |
| CID 6377  Mark RISON  10.3.5  1593 | There are numerous technical issues with the description of the AP/PCP (re)assoc receipt procedures, including deletion of the PTKSA, the point of the Disassociation frame, the situation with PCPs, the distinction between SME and MLME, the behaviour if the result is not success and MFP is not in use and the reassoc is part of FT, the situation with DMG STAs | I will propose text (not possible to give here) |

Discussion:

Part of PMF is the handling of (re)association. It is necessary for an AP (or PCP, implied throughout this discussion) to be able to distinguish between a genuine (re)association request to the same AP, including the case where a STA has reset and lost its state, and a forged one. Similarly, it is necessary to distinguish between a genuine deauthentication/disassociation, including the case where an AP has reset and lost its state, and a forged one.

This is done through the SA Query procedure. The querying STA sends an encrypted frame with a unique identifier, and the queried STA, if it is still associated, sends an encrypted frame back with that identifier. If the queried STA does not respond in this way, the querying STA can, after a suitable number of attempts, conclude that the queried STA is no longer associated (e.g. it has reset).

The procedure for a genuine reassociation proceeds as follows:

1. (non-AP) STA deletes PTKSA
2. STA sends reassociation request
3. AP says “please try later” and starts SA Query procedure
4. STA does not respond (since it no longer has the PTKSA)
5. STA sends reassociation request again
6. AP accedes to the request and sends reassociation response
7. AP sends protected Disassociation frame (ignored by STA since it no longer has the PTKSA to decrypt it)
8. AP deletes PTKSA

Similarly, the procedure for a genuine association after the non-AP STA has reset proceeds as follows:

1. STA sends association request
2. AP says “please try later” and starts SA Query procedure
3. STA does not respond
4. STA sends association request again
5. AP accedes to the request and sends association response
6. AP sends protected Disassociation frame (ignored by STA since it no longer has the PTKSA to decrypt it)
7. AP deletes PTKSA

In contrast, the procedure for a forged reassociation proceeds as follows:

1. attacking STA sends reassociation request
2. AP says “please try later” and starts SA Query procedure
3. genuine STA does respond
4. AP determines the reassociation request was a forgery

There is a special case where for whatever reason the genuine STA does not respond to the SA Queries:

1. attacking STA sends reassociation request
2. AP says “please try later” and starts SA Query procedure
3. genuine STA does not respond for some reason
4. attacking STA sends reassociation request again
5. AP accedes to the request and sends reassociation response
6. AP sends protected Disassociation frame. This might be picked up by the genuine STA since it still has the PTKSA to decrypt it, though why the STA would miss all the SA Query frames but not this one, and what the genuine STA is supposed to do at this point (call the cops?) are unclear
7. genuine STA deletes PTKSA
8. AP deletes PTKSA

Unfortunately 11mc/D4.0 doesn’t quite say this (in particular the deletion of the PTKSA at the AP is missing, and the point of the Disassociation frame is unclear), and what it does say is in many places ambiguous or inconsistent (most egregiously, “an earlier SA Query procedure has not allowed a new association process to be started” has two possible and nearly opposite interpretations: “an earlier SA Query procedure has {not allowed [i.e. disallowed] {a new association process to be started}}” and “an earlier SA Query procedure has not {allowed {a new association process to be started}}”).

PCPs have not always been covered in all this, and it is not always clear that the state is maintained at both the SME and the MLME. The behaviour if the ResultCode is not SUCCESS and management frame protection is not in use and the reassociation is part of a fast BSS transition is not clearly stated.

Finally, as noted in the comments, there are a lot of editorial accuracy and consistency issues.

Proposed changes:

Change “Association request rejected temporarily; try again later” to “REFUSED\_TEMPORARILY” at 173.14, 187.20, 194.24.

Change ““Association request rejected temporarily; try again later.”” to “REFUSED\_TEMPORARILY.” (note no double quotes in the final text, but full stop yes) at 174.58, 181.53, 188.55, 195.56.

Change the indicated subclauses as follows (small changes which might be missed highlighted in turquoise), relettering steps as necessary:

**10.3.5.5 AP or PCP reassociation receipt procedures**

~~Upon receipt of an Reassociation Request frame from a non-AP STA for which the state is State 1, the AP’s MLME shall transmit an Reassociation Response frame with an appropriate status code.~~

Upon receipt of a Reassociation Request frame from a STA ~~for which the state is State 2, State 3, or State 4,~~ the AP or PCP~~’s MLME~~ shall ~~reassociate with the STA using~~use the following procedure:

1. The MLME shall issue an MLME-REASSOCIATE.indication primitive to inform the SME of the reassociation request. The SME shall issue an MLME-REASSOCIATE.response primitive addressed to the STA identified by the PeerSTAAddress parameter of the MLME-REASSOCIATE.indication primitive. If the reassociation is not successful, the SME shall indicate a specific reason for the failure to reassociate in the ResultCode parameter. Upon receipt of the MLME-REASSOCIATE.response primitive, the MLME shall transmit a Reassociation Response frame.
2. [New step] If the state for the STA is 1, the SME shall refuse the reassociation request by issuing an MLME‑REASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED. [not for DMG if the DMG STA doesn’t use 802.11 open system auth, though – does this need to be NOTEd?]
3. ~~At an~~ AP ~~having~~with dot11InterworkingServiceActivated ~~equal to~~ true only: If ~~, subsequent to receiving an~~ the MLME-REASSOCIATE.indication primitive ~~with~~has the EmergencyServices parameter set to true ~~that~~ and the RSN parameter does not include an RSNE ~~parameter~~, the SME shall ~~accept~~not reject the reassociation request ~~even if~~on the basis that dot11RSNAActivated is true and dot11PrivacyInvoked is true, thereby granting access, using unprotected frames (see 8.2.4.1.9 (Protected Frame field)), to the network for emergency services purposes.
4. Otherwise, i~~I~~n an RSNA~~,~~ the SME shall check the values received in the RSN~~E~~ parameter to see whether the values received match the ~~AP or PCP’s~~ security policy. If they do not, the SME shall refuse the reassociation ~~shall not be accepted~~ by issuing an MLME-REASSOCIATE.response primitive with a ResultCode indicating the security policy mismatch.
5. Otherwise, i~~I~~f the ~~AP or PCP’s~~ state for the ~~non-AP and non-PCP~~ STA is 4, the ~~non-AP and non-PCP~~ STA has a valid security association, the ~~non-AP and non-PCP~~ STA has negotiated management frame protection, ~~and~~ the reassociation is not a part of a fast BSS transition, and ~~an~~ there has been no earlier, timed out SA Query procedure with the ~~non-AP and non-PCP~~ STA ~~has not~~ (which would have allowed a new reassociation process to be started, without an additional SA Query procedure):
   1. The SME shall ~~reject~~refuse the reassociation request by ~~generat~~issuing an MLME‑REASSOCIATE.response primitive with ResultCode ~~“Association request rejected temporarily; Try again later.”~~REFUSED\_TEMPORARILY ~~The SME shall not modify any association state for the non-AP and non-PCP STA, and shall include in the MLME-REASSOCIATE.response primitive~~ and TimeoutInterval containing a Timeout Interval element with the Timeout Interval Type field set to 3 (Association Comeback time)~~, specifying a comeback time when the AP or PCP would be ready to accept an association with this STA~~. If the SME is in an ongoing SA Query with the STA, the Timeout Interval Value field shall be set to the remaining SA Query period, otherwise it shall be set to dot11AssociationSAQueryMaximumTimeout.
   2. The state for the STA shall be left unchanged.
   3. Following this, if the SME is not in an ongoing SA Query with the STA, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA every dot11AssociationSAQueryRetryTimeout TUs until an ~~matching~~ MLME-SA-QUERY.confirm primitive for the STA and with a matching TransactionIdentifier is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. [joined to next bullet] The SME shall ~~insert the TransactionIdentifier in MLME-SA-QUERY.request primitive,~~ increment ~~this~~ the TransactionIdentifier by 1 for each ~~subsequent~~ MLME-SA-QUERY.request primitive, ~~and~~ rolling it over to 0 after the maximum allowed value ~~in this field~~is reached.
   4. ~~An MLME may interpret reception of a valid protected frame as an indication of a successfully completed SA Query and thereby generate an MLME-SA-QUERY.confirm primitive.~~
   5. If ~~an~~no MLME-SA-QUERY.confirm primitive with a~~n~~ ~~outstanding~~ ~~t~~Transaction~~i~~Identifier matching a TransactionIdentifier in an MLME-SA-QUERY.request issued in this SA Query procedure is ~~not~~ received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall allow ~~the~~a subsequent reassociation process with the STA to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent reassociation process with the STA if an MSDU was received from the STA within this period.
6. The SME shall refuse a reassociation request from a STA that does not support all the rates in the BSSBasicRateSet parameter in the MLME-START.request primitive.
7. The SME shall refuse a reassociation request from an HT STA that does not support all the MCSs in the Basic MCS Set field of the HT Operation parameter ~~of~~in the MLME-START.request primitive.
8. The SME shall refuse a reassociation request from a VHT STA that does not support all the <VHT‑MCS, NSS> tuples indicated by the Basic VHT-MCS and NSS Set field of the VHT Operation parameter in the MLME-START.request primitive.
9. ~~The SME shall generate an MLME-REASSOCIATE.response primitive addressed to the non-AP and non-PCP STA. If the reassociation is not successful, the SME shall indicate a specific reason for the failure to reassociate in the ResultCode parameter as defined in 6.3.7.5.2 (Semantics of the service primitive).~~
10. If the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS, and the SME has an existing SA with the ~~non-AP and non-PCP~~ STA, and an SA Query procedure with that ~~non-AP and non-PCP~~ STA has failed to receive a valid response, ~~then~~ the SME shall issue an MLME-DISASSOCIATE.request primitive addressed to the STA with ReasonCode INVALID\_AUTHENTICATION.

NOTE—This MLME-DISASSOCIATE.request generates a protected Disassociation frame ~~addressed to the STA~~. If the reassociation request was genuine, the STA has deleted the PTKSA by this point and so the protected Disassociation frame is ignored. The purpose is to inform a STA which has for some reason failed to respond to an SA Query procedure triggered by a forged reassociation request.

1. If the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS~~, the association identifier assigned to the STA shall be included in this primitive. If~~ and the reassociation is not part of a fast BSS transition ~~and management frame protection is not in use~~, the SME shall delete any PTKSA and temporal keys held for communication with the STA by using the MLME-DELETEKEYS.request primitive (see 11.5.18 (RSNA security association termination)). In the case of a DMG AP or PCP, the association identifier shall be in the range of 1 to 254.
2. If the MLME-REASSOCIATE.indication primitive includes an MMS parameter, the AP or PCP shall ~~generate the MLME-REASSOCIATE.response primitive directed to the MLME of the STA identified by the PeerSTAAddress parameter of the MLME-REASSOCIATE.request primitive and~~ take the following additional action, as appropriate:
   1. If the Single AID field in the MMS parameter of the MLME-REASSOCIATE.indication primitive is equal to 1, the AP or PCP may allocate a single AID for all the STAs included in the MMS element. If the AP or PCP allocates the same AID to all STAs whose MAC address was included in the MMS element, it shall include the MMS element received from the MMS-ME coordinated STA in the MLME-REASSOCIATE.response primitive.
   2. If the Single AID field is 0, the AP or PCP shall allocate a distinct AID for each STA specified in the MMS element.
3. ~~Upon receipt of an MLME-REASSOCIATE.response primitive, the MLME shall transmit a Reassociation Response frame to the STA.~~
4. ~~When~~If ~~the~~a Reassociation Response frame with a status ~~value~~code of ~~Successful~~SUCCESS is acknowledged by the STA [how does the SME find out?], the state ~~variable~~ for the STA shall be set to State 4, or to State 3 if RSNA establishment is required [how does the MLME know?] ~~on the new AP or PCP~~ and ~~the FT Protocol is not used on the new AP or PCP~~ the reassociation is not part of a fast BSS transition.
5. ~~When~~If the ResultCode ~~of the reassociation~~ in the MLME-REASSOCIATE.response primitive is not SUCCESS and ~~if~~ management frame protection is in use the state for the STA shall be left unchanged ~~on the AP or PCP the Reassociation Request frame was sent to~~. If the ResultCode is not SUCCESS and management frame protection is not in use and the reassociation is part of a fast BSS transition, the state for the STA shall be left unchanged. ~~When~~If the ResultCode is not SUCCESS and management frame protection is not in use and the reassociation is not part of a fast BSS transition, the state for the STA ~~is~~shall be set to State 3 if it was ~~in~~ State 4.
6. If the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS,~~If~~ RSNA establishment is required and ~~FT is not in use~~ the reassociation is not part of a fast BSS transition, the SME shall attempt a 4-way handshake. Upon a successful completion of a 4-way handshake, the SME shall enable protection by invoking MLME-SETPROTECTION.request(Rx\_Tx)~~. Upon receipt of the MLME‑SETPROTECTION.request(Rx\_Tx), the MLME shall set~~ and the state for the STA shall be set to State 4.
7. AP only: The SME shall inform the DS of any changes in the ~~association~~ state for the STA.

**10.3.5.3 AP or PCP association receipt procedures**

~~Upon receipt of an Association Request frame from a non-AP STA for which the state is State 1, the AP’s MLME shall transmit an Association Response frame with an appropriate status code.~~

Upon receipt of an Association Request frame from a ~~non-AP and non-PCP~~ STA ~~for which the state is State 2, State 3, or State 4,~~ the AP or PCP~~’s MLME~~ shall ~~associate with the non-AP and non-PCP STA using~~use the following procedure:

1. The MLME shall issue an MLME-ASSOCIATE.indication primitive to inform the SME of the association request. The SME shall issue an MLME-ASSOCIATE.response primitive addressed to the STA identified by the PeerSTAAddress parameter of the MLME-ASSOCIATE.indication primitive. If the association is not successful, the SME shall indicate a specific reason for the failure to associate in the ResultCode parameter. Upon receipt of the MLME-ASSOCIATE.response primitive, the MLME shall transmit an Association Response frame.
2. [New step] If the state for the STA is 1, the SME shall refuse the association request by issuing an MLME‑ASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED. [not for DMG if the DMG STA doesn’t use 802.11 open system auth, though – does this need to be NOTEd?]
3. ~~At an~~ AP ~~having~~with dot11InterworkingServiceActivated ~~equal to~~ true only: If~~, subsequent to receiving an~~the MLME-ASSOCIATE.indication primitive ~~with~~has the EmergencyServices parameter set to true ~~that~~ and the RSN parameter does not include an RSNE, the SME shall ~~accept~~not reject the association request ~~even if~~on the basis that dot11RSNAActivated is true and dot11PrivacyInvoked is true, thereby granting access, using unprotected frames (see 8.2.4.1.9 (Protected Frame field)), to the network for emergency services purposes.
4. Upon receiving an MLME-ASSOCIATE.indication primitive, when management frame protection is not in use, the SME shall delete any PTKSA and temporal keys held for communication with the STA by using the MLME-DELETEKEYS.request primitive (see 11.5.18 (RSNA security association termination)) – CHECK, not in reassoc and appears to be duplicated in step k) below
5. Otherwise, i~~I~~n an RSNA~~,~~ the ~~AP or PCP~~SME shall check the values received in the RSN~~E~~ parameter to see whether the values received match the ~~AP or PCP’s~~ security policy. If they do not, the SME shall refuse the association ~~shall not be accepted~~by issuing an MLME-ASSOCIATE.response primitive with a ResultCode indicating the security policy mismatch.
6. Otherwise, i~~I~~f the ~~AP or PCP’s~~ state for the ~~non-AP and non-PCP~~ STA is 4, ~~and~~ the ~~AP or PCP~~STA has a valid security association ~~for the non-AP and non-PCP STA~~, ~~and~~the STA has negotiated management frame protection ~~with the non-AP and non-PCP STA~~, and ~~an~~ there has been no earlier, timed out SA Query procedure with the ~~non-AP and non-PCP~~ STA ~~has not~~ (which would have allowed a new association process to be started, without an additional SA Query procedure~~,~~):
   1. ~~t~~The SME shall ~~reject~~refuse the association request by ~~generat~~issuing an MLME-ASSOCIATE.response primitive with ResultCode ~~“Association request rejected temporarily; try again later.”~~REFUSED\_TEMPORARILY ~~The SME shall not modify any association state for the non-AP and non-PCP STA, and shall include in the MLME-ASSOCIATE.response primitive~~and TimeoutInterval containing a Timeout Interval element with the Timeout ~~i~~Interval ~~t~~Type field set to 3 (Association Comeback time)~~, specifying a comeback time when the AP or PCP would be ready to accept an association with this STA~~. If the SME is in an ongoing SA Query with the STA, the Timeout Interval Value field shall be set to the remaining SA Query period, otherwise it shall be set to dot11AssociationSAQueryMaximumTimeout.
   2. The state for the STA shall be left unchanged.
   3. Following this, if the SME is not ~~already engaging~~ in an ongoing SA Query with the STA, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA every dot11AssociationSAQueryRetryTimeout TUs until an ~~matching~~ MLME-SA-QUERY.confirm primitive for the STA and with a matching TransactionIdentifier is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. [joined to next bullet] The SME shall ~~specify a TransactionIdentifier parameter value in the MLME-SA-QUERY.request primitive, and~~ increment the ~~value~~TransactionIdentifier by 1 for each ~~subsequent~~ MLME-SA-QUERY.request primitive, rolling it over the value to 0 after the maximum allowed value is reached.
   4. ~~The MLME may interpret reception of a valid protected frame as an indication of a successfully completed SA Query, and thereby generate an MLME-SA-QUERY.confirm primitive.~~
   5. If ~~an~~no MLME-SA-QUERY.confirm primitive with a~~n outstanding~~ ~~t~~Transaction ~~i~~Identifier matching a TransactionIdentifier in an MLME-SA-QUERY.request issued in this SA Query procedure is ~~not~~ received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall allow ~~the~~a subsequent association process with the STA to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent association process with the STA if an MSDU was received from the STA within this period.
7. The SME shall refuse an association request from a STA that does not support all the rates in the BSSBasicRateSet parameter in the MLME-START.request primitive.
8. The SME shall refuse an association request from an HT STA that does not support all the MCSs in the Basic MCS Set field of the HT Operation parameter ~~of~~in the MLME-START.request primitive.
9. The SME shall refuse an association request from a VHT STA that does not support all the <VHT-MCS, NSS> tuples indicated by the Basic VHT-MCS and NSS Set field of the VHT Operation parameter in the MLME-START.request primitive.
10. ~~The SME shall generate an MLME-ASSOCIATE.response primitive addressed to the non-AP and non-PCP STA. When the association is not successful, the SME shall indicate a specific reason for the failure to associate in the ResultCode parameter as defined in 6.3.7.5.2 (Semantics of the service primitive).~~ If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS, and the SME has an existing SA with the ~~non-AP and non-PCP~~ STA, and an SA Query procedure with that ~~non-AP and non-PCP~~ STA has failed to receive a valid response, ~~then~~ the SME shall ~~send~~issue an MLME-DISASSOCIATE.request primitive addressed to the STA with ReasonCode INVALID\_AUTHENTICATION.~~46~~

***[Note to the editor: replace footnote 46 with a NOTE as follows]***

NOTE—This MLME-DISASSOCIATE.request generates a protected Disassociation frame ~~addressed to the STA~~. If the association request was genuine, the STA has deleted the PTKSA by this point and so the protected Disassociation frame is ignored. The purpose is to inform a STA which has for some reason failed to respond to an SA Query procedure triggered by a forged association request.

1. [new step break] If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS, ~~the association identifier assigned to the STA shall be included in the MLME-ASSOCIATE.response primitive, and~~ the SME shall delete any PTKSA and temporal keys held for communication with the STA by using the MLME-DELETEKEYS.request primitive (see 11.5.18 (RSNA security association termination)). In the case of a DMG AP or PCP, the association identifier shall be in the range of 1 to 254.
2. If the MLME-ASSOCIATE.indication primitive includes an MMS parameter, the AP or PCP shall ~~generate the MLME-ASSOCIATE.response primitive directed to the MLME of the STA identified by the PeerSTAAddress parameter of the MLME-ASSOCIATE.request primitive and~~ take the following additional action, as appropriate:
   1. If the Single AID field in the MMS parameter of the MLME-ASSOCIATE.indication primitive is equal to 1, the AP or PCP may allocate a single AID for all the STAs included in the MMS element. If the AP or PCP allocates the same AID to each STA whose MAC address was included in the MMS element, it shall include the MMS element received from the MM-SME coordinated STA in the MLME-ASSOCIATION.response primitive.
   2. If the Single AID field is 0, the AP or PCP shall allocate a distinct AID for each STA specified in the MMS element.
3. ~~Upon receipt of an MLME-ASSOCIATE.response primitive, the MLME shall transmit an Association Response frame) to the STA.~~
4. ~~When~~If the ResultCode ~~of~~in the MLME-ASSOCIATE.response primitive is not SUCCESS~~,~~ ~~if~~and management frame protection is in use the state for the STA shall be left unchanged. If the ResultCode is not SUCCESS and ~~if~~ management frame protection is not in use the state for the STA shall be set to State 3 if it was ~~in~~ State 4. ***[Editor: swap this and the next step.]***

1. ~~When~~If ~~the~~an Association Response frame with a status code of ~~Successful~~SUCCESS is acknowledged by the STA [how does the SME find out?], the state for the STA shall be set to State 4, or to State 3 if RSNA establishment is required [how does the MLME know?].
2. If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS and~~If~~ RSNA establishment is required, the SME shall attempt a 4-way handshake. Upon a successful completion of a 4-way handshake, the SME shall enable protection by invoking MLME-SETPROTECTION.request(Rx\_Tx)~~. Upon receipt of the MLME-SETPROTECTION.request(Rx\_Tx), the MLME shall set~~ and the state for the STA shall be set to State 4.
3. AP only: The SME shall inform the DS of any changes in the ~~association~~ state for the STA.

An AP may provide neighbor report information to a STA that requests authentication or association by responding with an Authentication or (Re)Association Response frame that includes the Reason Code field set to REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION and that includes one or more Neighbor Report elements. [what is this doing here? and why is this not in the auth or reassoc subclauses too?]

**10.14 SA Query procedures**

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

To send an SA Query Request frame to a peer STA, the SME shall issue an MLME-SA-QUERY.request primitive. A STA that supports the SA Query procedure and receives an SA Query Request frame shall respond with an SA Query Response frame ~~when~~if all of the following are true and shall not respond otherwise: the receiving STA is currently associated to the sending STA, and no pending MLME-ASSOCIATE.request or MLME‑REASSOCIATE.request primitives are outstanding for the receiving STA ~~that receives the SA Query indication~~.

NOTE—A non-AP and non-PCP STA does not respond if it is trying to reassociate with the AP or PCP that sent the SA Query Request frame (since it no longer has the PTKSA) or to another AP or PCP (it could maintain the old association and PTKSA until the reassociation is completed). There is no such restriction for an AP or PCP.

If a non-AP and non-PCP STA that has an SA with its AP or PCP for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the AP or PCP, the non-AP and non-PCP STA may use this as an indication that there may be a mismatch in the association state between itself and the AP or PCP. In such a case, the non-AP and non-PCP STA’s SME may initiate the SA Query procedure with the AP or PCP to verify the validity of the SA by issuing one MLME-SA-QUERY.request primitive every dot11AssociationSAQueryRetryTimeout TUs until a matching MLME-SA-QUERY.confirm primitive is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure has passed. [Shouldn’t this stuff be moved to Subclause 10.3.5.7?] If the AP or PCP ~~repliesr~~esponds to the SA Query request with a valid SA Query response that has a matching transaction identifier, the non-AP STA ~~may~~should continue to use the SA. If no valid SA Query response is received, the non-AP STA’s SME may destroy the SA using the MLME-DELETEKEYS.request primitive and the non-AP STA may move into State 1 [or optionally State 2 for DMG?] with the AP.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CIDs 6375, 6376, 6377 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6625  Mark RISON  11  1865.1 | The security flowcharts use "!", which is not defined | Either change to NOT, or add the terminology to Subclause 1.5 |

Discussion:

! is a C-ism. While it is convenient, it needs to be defined, like all the others.

Proposed resolution:

REVISED

Add at 3.35 “!*x* is the Boolean NOT.”, where the x is italic.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6824  Mark RISON  11  1865.1 | There are about 30 references to "temporal keys" but the derivations only show a single temporal key. If the idea is that you can have one per key ID, then fine, but (a) make this clear and (b) only use the plural in the contexts where you have more than one (e.g. talking about deleting any temporal keys). | As it says in the comment |

Discussion:

There are 33 hits for “temporal keys” and 154 hits for “temporal key” in the singular (some of these pertain to TKIP).

A TK is defined at 44.17 as “The combination of temporal encryption key and temporal message integrity code (MIC) key.” Note that PTK != Pairwise Temporal Key (rather, == Pairwise Transient Key).

The instances of “temporal keys” are as follows:

37.48: definition of PTK (allegedly contains one or more TKs)

224.35: deletion of multiple TKs using MLME-DELETEKEYS.request

1591.46, 1592.26, 1593.16, 1593.45, 1594.51, 1596.15, 1597.10, 1597.55, 1600.64, 1601.59, 1602.17, 1602.58, 1603.21: “the SME shall delete any PTKSA and temporal keys held”

1866.8, 1866.37, 1867.24: establishing temporal keys in an ESS, and with 802.1X in IBSS

1867.1: establishing temporal keys with PSK in IBSS

1933.1, 1945.30, 1946.10: using MLME-DELETEKEYS.request to delete a PTKSA/GTKSA/IGTKSA

1940.30: “A Supplicant may initiate preauthentication when it has completed the 4-Way Handshake and configured the required temporal keys.”

1942.12: “This process keeps the pair of STAs in a consistent state with respect to derivation of fresh temporal keys upon an IEEE Std 802.1X reauthentication.”

1943.50: “Synchronize the installation of temporal keys into the MAC.” as a purpose of the 4WH

1953.8: “The PTK is partitioned into KCK, KEK, and temporal keys”

1955.22: “The GTK is partitioned into temporal keys” [sic]

1956.29: “The STK is partitioned into SKCK, SKEK, and temporal keys”

1982.6: “The Authenticator sends an EAPOL-Key frame containing ANonce, the RSNE from its Beacon or Probe Response frames, MIC, whether to install the temporal keys, the encapsulated GTK, and if management frame protection is negotiated, the IGTK.”

1982.10: “The Supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.” [but previous step said they might not be]

1997.46: “The Temporal keys (TK) shall be computed as […] TPK-TK = L(TPK, 128, Length – 128)”

2017.18: “STAs transmit protected MSDUs, A-MSDUs, and robust Management frames to an RA when temporal keys are configured […]STAs expect to receive protected MSDUs, A-MSDUs, and robust Management frames from a TA when temporal keys are configured”

As can be seen on page 1954 (and also 1961), a PTK actually only contains a single TK. You only have more than one TK if this is in the context of more than one SA (e.g. a PTKSA and a GTKSA).

Proposed resolution:

Make the following changes:

At 37.45: “**pairwise transient key (PTK):** A concatenation of session keys derived from the pairwise master key

(PMK) or from the PMK-R1. Its components include a key confirmation key (KCK), a key encryption key

(KEK), and ~~one or more~~a temporal key~~s~~ (TK) ~~that are~~, which is used to protect information exchanged over the link.”

At 224.34: “Receipt of this primitive causes the MAC to delete the temporal keys identified by the ~~Keylist Address, including Group, Pairwise and PeerKey~~ DeleteKeyDescriptors in the Keylist, and to cease using them.”

At 1591.45, 1592.26, 1593.14, 1593.45, 1594.50, 1596.15, 1597.10, 1597.55, 1600.64, 1601.58, 1602.16, 1602.57, 1603.20: “any PTKSA, GTKSA, IGTKSA and temporal keys held”

At 1866.8, 1866.36, 1867.1, 1867.24, 1943.50: “one or more temporal keys”

At 1933.1, 1940.30: “temporal key(s)”

At 1942.13: “one or more fresh temporal keys”

At 1953.8, 1956.28: “a temporal key~~s~~, which ~~are~~is used”

At 1955.21: “The GTK ~~is partitioned into~~is a temporal key~~s~~, which is used ~~by the MAC~~ to protect group addressed communication”

At 1982.6:

1. The Authenticator sends an EAPOL-Key frame containing ANonce, the RSNE from its Beacon or

Probe Response frames, MIC, whether to install the temporal keys, the encapsulated GTK, and if management frame protection is negotiated, the IGTK.

1. The Supplicant sends an EAPOL-Key frame to confirm ~~that~~whether the temporal keys ~~are~~were installed.

At 1997.46: “The ~~T~~temporal key~~s~~ (TK) shall be computed as the remaining bits”

At 2017.17:

STAs transmit protected MSDUs, A-MSDUs, and robust Management frames to an RA when a temporal key~~s are~~ has been configured with a MLME-SETKEYS.request primitive and an MLME-SETPROTECTION.request primitive has been invoked with ProtectType parameter Tx or Rx\_Tx to that RA. STAs expect to receive protected MSDUs, A-MSDUs, and robust Management frames from a TA when a temporal key~~s are~~ has been configured with a MLME-SETKEYS.request primitive and an MLME-SETPROTECTION.request primitive has been invoked with ProtectType parameter Rx or Rx\_Tx from that TA. MSDUs, A-MSDUs, and robust Management frames that do not match these conditions are sent in the clear and are received in the clear.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 6824 in <this document>, which align the wording throughout the document so that there is one TK per SA.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6576  Mark RISON  11.5.1.1.10  1930.12 | It says "Since the Key ID 0 is reserved for individually addressed frame transmission, there are only three available Key IDs" -- this is not true when "Extended Key ID for Individually Addressed Frames" is in effect | Amend the wording accordingly |

Discussion:

Originally, unicast transmissions only used Key ID 0. However, with the introduction of the “Extended Key ID for Individually Addressed Frames” mechanism, Key ID 1 can also be used for them.

Proposed changes:

Change 1930.12 as follows:

Since ~~the~~ Key ID 0 is reserved for individually addressed frame transmission, there are ~~only~~at most three available Key IDs (only two if extended Key IDs for individually addressed frames are in use), and the different MGTKs would contend for the single remaining Key ID upon rollover.

Change 1948.9 as follows:

When both ends of the link support ~~the expanded~~extended Key IDs ~~space~~ for individually addressed frames~~traffic~~, it is possible to install the new PTKSA or STKSA without data loss,

Delete “the” in “the Key ID 0” at 1978.24 and 1979.3.

Proposed resolution:

Make the changes shown under “Proposed changes” for CID 6576 in <this document>, which account for extended Key IDs.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6573  Mark RISON  B.4  2647.1 | The PICS abbreviations are not helpful | Come up with some more useful abbreviations for the fundamental stuff, e.g. use "CF-IBSS" instead of "CF2.2" and "CF-HT" instead of "CF16" |

Discussion:

Do you know what “(CF2 OR CF21) AND CF10 AND CF29:M” means? Of course not. Using abbreviations rather than numbers would be much more helpful: “(CFIndepSTA OR CFMBSS) AND CFSM AND CFVHT”. Here is a proposed set of replacements (to be done throughout Annex B):

|  |  |  |
| --- | --- | --- |
| Item (old) | Item (new) | IUT configuration |
| CF1 | CFAP | Access point (AP) |
| CF2 | CFIndepSTA | Independent station (neither an AP, nor a mesh STA, nor a STA operating outside the context of a BSS) |
| CF2.1 | CFSTAofAP | Operation in an infrastructure BSS |
| CF2.2 | CFIBSS | Operation in an independent BSS (IBSS) |
| CF2.4 | CFPBSS | Operation in a PBSS |
| CF2.4.1 | CFPCP | Operation as a PCP |
| CF2.4.2 | CFPBSSnotPCP | Operation *not* as a PCP |
| CF4 | CFDSSS | Direct sequence spread spectrum (DSSS) PHY for the 2.4 GHz band |
| CF6 | CFOFDM | Orthogonal frequency division multiplexing (OFDM) PHY |
| CF7 | CFHRDSSS | High rate direct sequence spread spectrum (HR/DSSS) PHY |
| CF8 | CFMD | Multidomain operation capability implemented |
| CF9 | CFERP | Extended Rate PHY (ERP) |
| CF10 | CFSM | Spectrum management |
| CF11 | CFOC | Operating classes capability implemented |
| CF12 | CFQoS | Quality of service (QoS) |
| CF13 | CFRM | Radio Measurement |
| CF14 | CFInfraSTA | Infrastructure mode |
| CF15 | CF3G6 | 3.65–3.70 GHz band in the United States |
| CF16 | CFHT | High throughput (HT) PHY |
| CF16.1 | CFHT2G4 | HT operation in 2.4 GHz band |
| CF16.2 | CFHT5G | HT operation in 5 GHz band |
| CF17 | CF5G9 | 5.9 GHz band |
| CF18 | CFTDLS | Tunneled direct-link setup supported |
| CF19 | CFWNM | Wireless network management (WNM) |
| CF20 | CFIW | Interworking with external networks service |
| CF21 | CFMBSS | Operation in a mesh BSS (MBSS) |
| CF22 | CFQMF | QoS management frame (QMF) policy |
| CF23 | CFAVT | Robust audio/video transport (AVT) |
| CF25 | CFDMG | Directional multi-gigabit (DMG) PHY |
| CF26 | CFMBO | Multi-band operation |
| CF27 | CFnotDMGSTA | Non-DMG STA |
| CF28 | CFDMGSTA | DMG STA |
| CF29 | CFVHT | Very High Throughput (VHT) Features |
| CF30 | CFTVHT | TVWS Operation |
| CF31 | CFOCB | Operation outside the context of a BSS (OCB) |
| CF32 | CFESM | Extended spectrum management |

Proposed changes:

Proposed resolution:

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6716  Mark RISON | Use Chinese characters or translation, not transliteration (see CID 3302) | As it says in the comment |

Discussion:

Per 14/0955 (not 14/0995; the database is in error), which resolved CID 3302, the name of the 5 GHz directive for 5150-5350 MHz in China is 工信部无函〔2012〕620号. The transliteration (using one of the many possible options) has no place now that Unicode is prevalent.

Proposed changes:

Change the penultimate cell at 3329.40 to:

信部无〔2002〕353号,

信部无〔2002〕277号,

工信部无函〔2012〕620号

Also reduce the font size of the “[B13]” at 3329.45 to match the surrounding text.

Proposed resolution:

Make the changes shown under “Proposed changes” for CID 6716 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6820  Mark RISON | Why was "Gaussian" lowercased? | Restore the uppercase G throughout |

Discussion:

In English, adjectives derived from a proper noun are capitalised (e.g. “French”).

Proposed resolution:

REVISED

Change “gaussian” to “Gaussian” at 12.9, 12.10.

Change “boolean” to “Boolean” on p. 1692 (3x), p. 1695, p. 1696 (5x), p. 1697 (2x), p. 2016, p. 2646.

Change “legendre” to “Legendre” at 55.13, 1881.25.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6582  Mark RISON | The spec uses e.g. >= and the corresponding single glyph, with various degrees of popularity | Replace all uses with a single glyph, or (where impossible, e.g. in ASCII text) settle on one set, e.g. !=, >=, etc. |

Discussion:

We should be consistent. Since Unicode has nice symbols for these things, let’s use them.

Proposed changes:

Change >= to ≥ at 1082.29, 1088.9, 1259.8, 1259.33, 1496.23, 1496.47, 1505.27, 1505.58, 1510.2 (2x), 1510.18, 1511.25 (2x), 1870.13, 1911.42, 1921.5.

Change <= to ≤ at 1463.47, 1496.23, 1496.47, 1505.27, 1505.58, 1510.3 (2x), 1510.19, 1511.25 (2x), 2060.31, 2066.21 (2x).

At 3.42 add:

x == y is Boolean equality.

x != y Boolean inequality.

Change 1692.53 as follows:

~~and where the use of “==” in the above expressions means that the value on the left side of the “==” is to be tested for equality with the value on the right side of the “==” yielding a boolean value of true if the two sides are equal and false if the two sides are unequal.~~ If either side of ~~the equality~~ “==” above is the empty set or has a null value, then the expression is defined to have a boolean value of true.

Change == to = at 1232.13, 1542.8, 1542.11, 1542.12.

Change = to == at 1880.62, 1880.65, 1881.42, 1881.46, 1883.22.

Change != to ≠ at 1733.19, 3566.17.

Change <> to ≠ at 1514.8, 1514.35, 1820.1, 2183.25, 2183.30, 2185.26, 2212.21, 2271.22.

Proposed resolution:

Make the changes shown under “Proposed changes” for CID 6582 in <this document>, which use proper glyphs for ==, !=/<>, >=, <= where not in ASCII text and where not in Boolean contexts.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6661  Mark RISON | "attribute values" in the context of PHY characteristics should be "characteristics". | As it says in the comment |

Discussion:

It seems reasonable to assert that something describing characteristics, in a subclause about characteristics or carried in a CHARACTERISTICS primitive, should be called a characteristic. For MAC characteristics as well as PHY characteristics, in fact.

Proposed resolution:

REVISED

Change “attribute values” to “characteristics” at 1275.55.

Change “sublayer attributes” to “characteristics” at 1840.1, 1840.8.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6754  Mark RISON | Table 9-17 should be moved to clause 8, somewhere near Table 8-34 [these might be D3.0 references] | As it says in the comment |

Discussion:

The table which needs moving is Table 9-17 Valid address field usage for Mesh Data and Multihop Action frames. This is a table showing frame formats. It should be in Clause 8, not Clause 9. It is very similar to Table 8-26 Address field contents.

Proposed resolution:

REVISED

Move Subclause 9.35.3 Frame addressing in an MBSS to a new Subclause 8.3.5, deleting “In this subclause, addressing of the Mesh Data and Multihop Action frames and MSDU/MMPDU forwarding behavior are described.” in the first para.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6771  Mark RISON | A few "retry bit"s | Change all of them to "Retry bit"s |

Discussion:

Adrian opines that some of these references are informal, some formal, and that the formal references should be changed to "Retry subfield", except where its location as a bit is significant (in AAD construction).

However, it is not clear to me how one distinguishes a formal instance from an informal one.

Proposed resolution:

REVISED

Change “retry bits in the MAC headers” to “the Retry subfield in the MAC header” at 1240.58.

Change “the Retry bit” to “the Retry subfield” at 1265.26, 1765.64, 1766.5.

Change “the retry bit” to “the Retry subfield” at 1364.14, 1364.15, 3179.54.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6795  Mark RISON | Per the rejection of CID 3372, add "network" after all instances of "BSS" which do not already have it | As it says in the comment |

Discussion:

Adrian opines that “network” is not necessary in this context, and TGmc has agreed on this in the past.

In that case, it is superfluous, and should be removed to save ink and any doubt as to a difference between a BSS and a “BSS network” etc.

Proposed resolution:

REVISED

Delete “network” in “SS network” at 12.16, 16.38, 66.14, 66.18 (2x), 66.60 (end of line), 66.61, 98.22, 108.37, 110.44, 110.55, 928.46, 1937.13, 2814.49.

Change “IBSS or ESS networks” to “IBSSs or ESSs” at 66.59.

Change “ESS and IBSS networks” to “ESSs and IBSSs” at 102.14.

Change “ESS networks” to “ESSs” at 66.60.

Change “non-IBSS networks” to “BSSs which are not IBSSs” at 1730.45.

Change “non-IBSS network” to “BSSs which is not an IBSS” at 2938.55.

Change “IBSS networks” to “IBSSs” at 1730.52.

Change “TSF for infrastructure and PBSS networks” to “TSF for an infrastructure BSS or a PBSS” at 1529.30.

Change “an infrastructure or PBSS network” to “an infrastructure BSS or a PBSS” at 1535.42.

Change “noninfrastructure networks” to “BSSs which are not infrastructure BSSs” at 80.57, 952.9.

Change “a noninfrastructure network” to “a BSSs which is not an infrastructure BSSs” at 80.59.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6788  Mark RISON | "bufferable" v. "buffered" -- there is confusion in these terms. Probably move to "buffered" for most cases | As it says in the comment |
| CID 6819  Mark RISON  3.2  21.31 | "individually addressed bufferable unit (BU): An individually addressed MSDU, individually addressed A-MSDU (HT STAs only) or individually addressed bufferable MMPDU." needs to say "DMG STAs" as for bufferable unit (BU). | As it says in the comment |
| CID 6298  Mark RISON | People keep confusing MPDUs, MSDUs, MMPDUs, A-MSDUs and A-MPDUs | Say something somewhere like "An MSDU or MMPDU is transmitted in one or more MPDUs. An MSDU may be carried in an A-MSDU. An A-MSDU is transmitted in one MPDU. An MSDU or MMPDU may be carried (in an MPDU) in an A-MPDU." |
| *CID 6561*  *Mark RISON* | *MMPDUs are not MPDUs and hence are not "frame"s* | *Change all places in the document which refer to "frame"s incorrectly to refer to "MMDU"s instead. As a first step, check all "<Management frame subtype> frame"s and change most if not all to "<Management frame subtype> MMDU"s* |
| *CID 6467*  *Mark RISON* | *The word "frame" is used too loosely. Sometimes it refers to a MSDU or MMPDU, rather than an MPDU (which might form just part of a fragmented MSDU or MMPDU). This affects, for example, whether the PM mode can change during a fragmented MSDU or MMPDU.* | *Make sure that "frame" is never used to refer to an MSDU or MMPDU.* |

Discussion:

MPDUs are not bufferable, MSDUs and MMPDUs are. And they are only actually buffered if a power save mechanism requires them to so be.

Proposed changes:

Change 26.1 as follows:

**~~bufferable Management frame~~**~~: A Management frame that is buffered for delivery according to a power-saving protocol. See Table 10-1 (Bufferable/nonbufferable classification of Management frames).~~

**bufferable medium access control (MAC) management protocol data unit (MMPDU)**: An MMPDU that is eligible to be queued for delivery using a power-saving mechanism (see Table 10-1)~~transmitted using one or more bufferable Management frames~~.

**bufferable unit (BU):** An MSDU, A-MSDU (HT STAs and DMG STAs only) or bufferable MMPDU ~~that is buffered to operate the power saving protocol~~.

Change 32.22 as follows:

**individually addressed bufferable unit (BU)**: An individually addressed MSDU, individually addressed A-MSDU (HT STAs and DMG STAs only) or individually addressed bufferable MMPDU.

Change 33.4 as follows:

NOTE 1—The MMPDU occupies a position in the management plane similar to that of the ~~MAC service data unit (~~MSDU~~)~~ in the data plane. ~~The MMPDU can be fragmented (under certain circumstances) and in that case is carried in multiple Management frames. This illustrates the similarity of the MMPDU to the MSDU.~~ An MSDU or MMPDU is transmitted in one or more MPDUs (with the Type field set to Data or Management respectively). An MSDU may be carried in an A-MSDU. An A-MSDU is transmitted in one MPDU. An MSDU, A-MSDU or MMPDU may be carried (in an MPDU) in an A-MPDU.

Change “Management frame” to “MMPDU” at 1548.25, 1548.15, 1548.17, 1548.18, 1548.22, 1548.37.

Change “frame” to “MMPDU” at 1548.31, 1548.33, 1548.35.

Change “Data and bufferable Management frames” to “BUs” at 1551.59.

Change 1557.6 (in AP during CP) as follows [is this all about S-APSD only?]:

The More Data bit ~~of~~equal to 1 in ~~the~~an individually addressed ~~Data or bufferable Management frame~~MPDU containing all or part of BU, using a delivery-enabled AC~~s~~ and destined for that STA indicates that more BUs are buffered for the delivery-enabled ACs. The More Data bit equal to 1 in an individually addressed ~~Data or bufferable Management frames~~MPDU containing all or part of a BU, using a nondelivery-enabled AC~~s~~ and destined for that STA indicates that more BUs are buffered for the nondelivery-enabled ACs.

Change “an individually addressed Data or bufferable Management frame” to “an individually addressed MPDU containing all or part of a BU” at 1557.29.

Change “the received Data or bufferable Management frame” to “the MPDU(s) containing the BU” at 1559.40 (in STA during CP).

Change “the last Data or bufferable Management frame” to “the last MPDU containing all or part of the BU” at 1560.36 (in STA during CFP).

Change 1560.56 (in STA using APSD) as follows:

The STA may send additional PS-Poll frames if the More Data subfield is 1 in a downlink individually addressed ~~Data or bufferable Management frames~~MPDU containing all or part of a BU, that does not use a~~ny~~ delivery-enabled AC~~s~~. The STA may send additional trigger frames if the More Data subfield is 1 in a downlink individually addressed ~~Data or bufferable Management frames~~MPDU containing all or part of a BU, that uses a delivery-enabled AC~~s~~.

Proposed resolution:

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 5062  Adrian Stephens  M.4.2  3489.6 | The invocation of hmac\_sha1 at lines 4-5 includes a superfluous "digest," (the 2nd occurrence). | Change lines 4-5 to read: "hmac\_sha1(digest, ssidlength+4, (unsigned char\*) password, (int) strlen(password), digest1)" |

Discussion:

There does indeed seem to be a superfluous argument, but the situation is obscured by the absence of a prototype for the hmac\_sha1 function. Taking a step back, the following are all issues with the code:

* There is no prototype for the hmac\_sha1 function
* The function should be called hmac\_sha\_1 per Subclause 1.5
* Various magic numbers are used
* Fixed-length returns can and should be passed as such, not as pointers
* The naming of some variables is confusing (in particular, “count” is in fact an index, and the thing which is called c in the function F is “iterations”; RFC 2898 is a good publicly-accessible reference which can and should be followed)
* Various function parameters can and should be marked const
* SHA-1 is referred to as A\_SHA for some reason
* The code is not consistent as to whether it uses assertions or return codes
* Casts are unnecessary after & 0xff
* The code is lax about signedness and width
* The code insists on a password of at least 8 characters but the comments do not

The following diff shows the changes proposed; this compiles without errors or warnings with gcc -c -std=c99 -pedantic -Wall where gcc is v4.9.3:

0a1,21

> #include <string.h>

> #include <assert.h>

>

> #define SHA\_1\_DIGEST\_LEN 20

> #define MAX\_SSID\_LEN 32

>

> /\*

> \* message - message to hash

> \* messagelength - length of message in octets

> \* key - key to use

> \* keylength - length of key in octets (must be less than

> \* output - HMAC-SHA-1 (key, message)

> \*/

> void hmac\_sha\_1(

> const unsigned char \*message,

> size\_t messagelength,

> const unsigned char \*key,

> size\_t keylength,

> unsigned char output[SHA\_1\_DIGEST\_LEN]

> );

>

2,5c23,27

< \* F(P, S, c, i) = U1 xor U2 xor ... Uc

< \* U1 = PRF(P, S || Int(i))

< \* U2 = PRF(P, U1)

< \* Uc = PRF(P, Uc-1)

---

> \* See IETF RFC 2898

> \* F(P, S, c, i) = U\_1 XOR U\_2 XOR ... U\_c

> \* U\_1 = PRF(P, S || INT(i))

> \* U\_2 = PRF(P, U\_1)

> \* U\_c = PRF(P, U\_c-1)

7d28

<

9,14c30,35

< char \*password,

< unsigned char \*ssid,

< int ssidlength,

< int iterations,

< int count,

< unsigned char \*output)

---

> const char \*password, /\* P \*/

> const unsigned char \*salt, /\* S \*/

> unsigned int saltlength,

> unsigned int iterations, /\* c \*/

> unsigned int index, /\* i \*/

> unsigned char output[SHA\_1\_DIGEST\_LEN])

16,17c37,38

< unsigned char digest[36], digest1[A\_SHA\_DIGEST\_LEN];

< int i, j;

---

> unsigned char digest[MAX\_SSID\_LEN+4], digest1[SHA\_1\_DIGEST\_LEN];

> int iteration, j;

19,20c40,42

< for (i = 0; i < strlen(password); i++) {

< assert((password[i] >= 32) && (password[i] <= 126));

---

> assert((saltlength+4) <= sizeof(digest));

> for (j = 0; j < strlen(password); j++) {

> assert((password[j] >= 32) && (password[j] <= 126));

23,39c45,61

< /\* U1 = PRF(P, S || int(i)) \*/

< memcpy(digest, ssid, ssidlength);

< digest[ssidlength] = (unsigned char)((count>>24) & 0xff);

< digest[ssidlength+1] = (unsigned char)((count>>16) & 0xff);

< digest[ssidlength+2] = (unsigned char)((count>>8) & 0xff);

< digest[ssidlength+3] = (unsigned char)(count & 0xff);

< hmac\_sha1(digest, ssidlength+4, (unsigned char\*) password,

< (int) strlen(password), digest, digest1);

<

< /\* output = U1 \*/

< memcpy(output, digest1, A\_SHA\_DIGEST\_LEN);

<

< for (i = 1; i < iterations; i++) {

< /\* Un = PRF(P, Un-1) \*/

< hmac\_sha1(digest1, A\_SHA\_DIGEST\_LEN, (unsigned char\*) password,

< (int) strlen(password), digest);

< memcpy(digest1, digest, A\_SHA\_DIGEST\_LEN);

---

> /\* U\_1 = PRF(P, S || INT\_32\_BE(i)) \*/

> memcpy(digest, salt, saltlength);

> digest[saltlength] = (index>>24) & 0xff;

> digest[saltlength+1] = (index>>16) & 0xff;

> digest[saltlength+2] = (index>>8) & 0xff;

> digest[saltlength+3] = index & 0xff;

> hmac\_sha\_1(digest, saltlength+4, (unsigned char \*) password,

> strlen(password), digest1);

>

> /\* output = U\_1 \*/

> memcpy(output, digest1, SHA\_1\_DIGEST\_LEN);

>

> for (iteration = 1; iteration < iterations; iteration++) {

> /\* U\_n = PRF(P, U\_n-1) \*/

> hmac\_sha\_1(digest1, SHA\_1\_DIGEST\_LEN, (unsigned char \*) password,

> strlen(password), digest);

> memcpy(digest1, digest, SHA\_1\_DIGEST\_LEN);

41,42c63,64

< /\* output = output xor Un \*/

< for (j = 0; j < A\_SHA\_DIGEST\_LEN; j++) {

---

> /\* output = output XOR U\_n \*/

> for (j = 0; j < SHA\_1\_DIGEST\_LEN; j++) {

49c71

< \* password - ascii string up to 63 characters in length

---

> \* password - printable ASCII string between 8 and 63 characters in length

52c74

< \* output must be 40 octets in length and outputs 256 bits of key

---

> \* output - 256 bits of key in output[0..31]

54,58c76,80

< int PasswordHash (

< char \*password,

< unsigned char \*ssid,

< int ssidlength,

< unsigned char \*output)

---

> void PasswordHash(

> const char \*password,

> const unsigned char \*ssid,

> unsigned int ssidlength,

> unsigned char output[SHA\_1\_DIGEST\_LEN\*2])

60,61c82,83

< if ((strlen(password) > 63) || (ssidlength > 32))

< return 0;

---

> assert((strlen(password) >= 8) && (strlen(password) <= 63) &&

> (ssidlength <= MAX\_SSID\_LEN));

65,66c87

< &output[A\_SHA\_DIGEST\_LEN]);

< return 1;

---

> &output[SHA\_1\_DIGEST\_LEN]);

Proposed changes:

Change the code in M.4.2 to:

#include <string.h>

#include <assert.h>

#define SHA\_1\_DIGEST\_LEN 20

#define MAX\_SSID\_LEN 32

/\*

\* message - message to hash

\* messagelength - length of message in octets

\* key - key to use

\* keylength - length of key in octets (must be less than

\* output - HMAC-SHA-1 (key, message)

\*/

void hmac\_sha\_1(

const unsigned char \*message,

size\_t messagelength,

const unsigned char \*key,

size\_t keylength,

unsigned char output[SHA\_1\_DIGEST\_LEN]);

/\*

\* See IETF RFC 2898

\* F(P, S, c, i) = U\_1 XOR U\_2 XOR ... U\_c

\* U\_1 = PRF(P, S || INT(i))

\* U\_2 = PRF(P, U\_1)

\* U\_c = PRF(P, U\_c-1)

\*/

void F(

const char \*password, /\* P \*/

const unsigned char \*salt, /\* S \*/

unsigned int saltlength,

unsigned int iterations, /\* c \*/

unsigned int index, /\* i \*/

unsigned char output[SHA\_1\_DIGEST\_LEN])

{

unsigned char digest[MAX\_SSID\_LEN+4], digest1[SHA\_1\_DIGEST\_LEN];

int iteration, j;

assert((saltlength+4) <= sizeof(digest));

for (j = 0; j < strlen(password); j++) {

assert((password[j] >= 32) && (password[j] <= 126));

}

/\* U\_1 = PRF(P, S || INT\_32\_BE(i)) \*/

memcpy(digest, salt, saltlength);

digest[saltlength] = (index>>24) & 0xff;

digest[saltlength+1] = (index>>16) & 0xff;

digest[saltlength+2] = (index>>8) & 0xff;

digest[saltlength+3] = index & 0xff;

hmac\_sha\_1(digest, saltlength+4, (unsigned char \*) password,

strlen(password), digest1);

/\* output = U\_1 \*/

memcpy(output, digest1, SHA\_1\_DIGEST\_LEN);

for (iteration = 1; iteration < iterations; iteration++) {

/\* U\_n = PRF(P, U\_n-1) \*/

hmac\_sha\_1(digest1, SHA\_1\_DIGEST\_LEN, (unsigned char \*) password,

strlen(password), digest);

memcpy(digest1, digest, SHA\_1\_DIGEST\_LEN);

/\* output = output XOR U\_n \*/

for (j = 0; j < SHA\_1\_DIGEST\_LEN; j++) {

output[j] ^= digest[j];

}

}

}

/\*

\* password - printable ASCII string between 8 and 63 characters in length

\* ssid - octet string up to 32 octets

\* ssidlength - length of ssid in octets

\* output - 256 bits of key in output[0..31]

\*/

void PasswordHash(

const char \*password,

const unsigned char \*ssid,

unsigned int ssidlength,

unsigned char output[SHA\_1\_DIGEST\_LEN\*2])

{

assert((strlen(password) >= 8) && (strlen(password) <= 63) &&

(ssidlength <= MAX\_SSID\_LEN));

F(password, ssid, ssidlength, 4096, 1, output);

F(password, ssid, ssidlength, 4096, 2,

&output[SHA\_1\_DIGEST\_LEN]);

}

Proposed resolution:

Make the changes shown under “Proposed changes” for CID 5062 in <this document>. These clean up the reference code, including the spurious argument.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
|  |  |  |

Discussion:

Proposed changes:

Proposed resolution:

Another missing space: “ignorethe”; “AVHT”.

Font size wacko: 1265.8 “RR5”.

**References:**

802.11mc/D4.0