IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for some comments on 11mc/D4.0 (SBmc1) |
| Date: 2015-09-26 |
| 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, 6235, 6295, 6299, 6308, 6323, 6364, 6365, 6366, 6375, 6376, 6377, 6389, 6390, 6404, 6426, 6452, 6459, 6479, 6480, 6482, 6490, 6496, 6506, 6527, 6529, 6561, 6562, 6563, 6573, 6576, 6582, 6583, 6625, 6661, 6676, 6677, 6684, 6716, 6754, 6771, 6795, 6802, 6803, 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.

r5: changes made during BRC meeting on 2015-08-07 and before BRC meeting on 2015-08-14. Added CID 6480.

r6: changes made during and immediately following the BRC meeting on 2015-08-14.

r7: changes made during and immediately following the BRC meeting in Cambridge. Added CIDs 6295, 6364, 6365, 6366.

r8: changes made before BRC meeting on 2015-08-28. Added CIDs 6323, 6426, 6452, 6459, 6490, 6527, 6529, 6561, 6676, 6677.

r9: changes made during and after BRC meeting on 2015-08-28, before BRC meeting on 2015-09-25. Moved CIDs 6214, 6215, 6216, 6303, 6305, 6306 to 15/1155. Added CIDs 6235, 6299, 6479, 6684, 6802, 6803.

r10: remove yellow stuff from the “Proposed changes” part of CIDs 6375, 6376, 6377.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6562Mark 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 6563Mark RISON101529 | Lots of things are ambiguous/unclear in relation to power-saving signalling and mechanisms | I will propose text (not possible to give here) |
| CID 6075Mark Hamilton8.2.4.1.7566.52 | 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 wording appears to allow the STA to indicate PS mode but not transition to it, and does not address transitioning back to AM. More generally, the choices to be made (unicast v. broadcast, whom to unicast, how many times to broadcast) are not clear.

*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**

1. In order to indicate its intent to change power management modes, a~~A~~ non-DMG [where are the rules of DMG IBSSen, then?] STA ~~may~~shall transmit individually addressed or group addressed (QoS) Null ~~Data~~ frames within the ATIM window ~~to indicate the STA’s intent to change power management modes~~. ***<paragraph break>***

The STA ~~may~~shall not transition into or out of PS mode ~~after~~ unless it has received acknowledgments ~~have been successfully received~~ for all individually addressed (QoS) Null ~~Data~~ frames or after ~~the STA~~it has transmitted a sufficient number of group addressed (QoS) Null ~~Data~~ frames ~~at least dot11BSSBroadcastNullCount times~~.

NOTE—The choice between individually addressed and group addressed transmissions, the peer STAs addressed for individually addressed transmissions, and the number of transmissions for group addressed transmissions are implementation choices outside the scope of the standard. A STA might base its choices on factors such as the number of peer STAs it is aware of in the IBSS, the expected traffic from each of these peer STAs, and the reliability of frame exchanges with these peer STAs.

**C.3 MIB Detail**

dot11BSSBroadcastNullCount OBJECT-TYPE

SYNTAX Unsigned32 (1..64)

MAX-ACCESS read-write

STATUS ~~current~~deprecated

DESCRIPTION

"Deprecated because this variable is not referenced in the standard.

This is a control variable.

*[…]*

This attribute specifies the number of group addressed (QoS) Null ~~Data~~ frames an IBSS STA ~~may~~ transmits before it changes power management mode."

Proposed resolution:

[Work in progress!]

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6390Mark 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 6404Mark RISON8.2.5.2591.37 | 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 6389Mark RISON10.421847.31 | 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 6482Mark RISON9.3.2.11248.21 | "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 (see resolution to CID 6479 for the latter).

The last paragraph in 9.21.4 is deleted per the following discussion:

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? Peter ECCLESINE: the one in the Country element] is different from the transmit power limit indicated by the operating class [OCs don’t indicate power limits; subband triplets do. Peter ECCLESINE: “Global OC 124 and 125, the two operating classes for 5.8 GHz band indicate regulatory classifications with power limits. In Japan 4.9 GHz band, nomadic devices have one tx power limit, CPE have another.”], 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. [Why is this para needed? It’s nothing to do with the subclause title, “Operation with coverage classes”, and the requirement already appears in e.g. 10.8.5 Specification of regulatory and local maximum transmit power levels and 10.8.6 Selection of a transmit power. Maybe change to just “Using the Country element, the maximum transmit power level can be changed to enhance operation too (see xxx).”? But the Country element can only reduce tx power, not increase it, so it doesn’t help when the BSS diameter is increased (which is what coverage classes are all about doing). I think it should just be deleted. Peter ECCLESINE: “considering that in 802.11-2012 we tried to remove all tx power considerations from Operating Classes, I am happy to delete the paragraph, which came from the time when nomadic behavior meant lower transmit power than license-exempt behavior. At that time two classes were used to signal use of two tx power limits. Note that FCC 13-49 U-NII-1 rules changes mean we now have four different tx power limits using Operating Class 1 in USA.”]

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, 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, 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 can change coverage class and maximum transmit power level to enhance operation. When dot11OperatingClassesRequired and dot11ExtendedChannelSwitchActivated are true and the maximum transmit power level is different from the transmit power limit indicated by the operating class, 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.~~

At 725.38 after the first sentence add: “The Coverage Class field is reserved in a DMG BSS.”

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 6479Mark RISON23.4.42631.19 | Why is TVHT operation restricted to a 900 m diameter? | Change "3 us" to "As indicated by the coverage class (see 9.21.4 (Operation with coverage classes))." and fix up aSlotTime to include it |

Discussion:

Peter ECCLESINE has clarified that this is a mistake, and TVWS should have a variable aAirPropagationTime; the aSlotTime should be the value currently shown plus any aAirPropagation time.

Proposed resolution:

REVISED

At 2631.19 change “3 μs” to “As indicated by the coverage class (see 9.21.4)”.

At 2631.6 change “24 μs (BCUs: 6 MHz or 7 MHz)” to “24 μs (BCUs: 6 MHz or 7 MHz) plus any coverage-class-dependent aAirPropagationTime (see Table 8-76)”.

At 2631.7 change “20 μs (BCUs: 8 MHz)” to “20 μs (BCUs: 8 MHz) plus any coverage-class-dependent aAirPropagationTime (see Table 8-76)”.

Change all 10 instances of “plus any coverage-class-dependent aAirPropagationTime Table 8-76” to add “(see” before “Table”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6480Mark RISON21.12.42453.54 | Having an inequality as the aAirPropagationTime does not help with all the equations in Clause 9 which use the parameter | Change "< 100 ns" to "As indicated by the coverage class (see 9.21.4 (Operation withcoverage classes)).", or indicate how a device knows what aAirPropagationTime a peer device is assuming |

Discussion:

The aAirPropagationTime cannot be changed in a DMG BSS (see resolution to CID 6482). So aAirPropagationTime should just be the maximum allowed BSS diameter, namely 100 ns (15 m). Carlos CORDEIRO has confirmed this it is reasonable for DMG STAs to assume such a BSS diameter.

Proposed resolution:

REVISED

Delete the “<” in “< 100 ns” at the cited location.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6496Mark RISON9.3.2.3.31250.16 | 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). A STA which achieves the required local SIFS timing accuracy of ≤ ±0.9 μs (assuming short slots) when the aAirPropagationTime is 0 μs does not suddenly have a local SIFS timing inaccuracy of ±10.2 μs when the aAirPropagationTime is 93 μs. Should “at the antenna connector” be added after “measured on the medium” below to make this clearer?

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. Well, except that it seems the spec is in error re TVHT, and it can be much more than 3 μs (see CID 6482).

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 defined to be separated by a 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 defined to be separated by a 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 6308Mark 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 6506Mark RISON20.3.20.5.12368.25 | 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 the rebuttal that while currently certain PHYs operating outside the 2.4 GHz band do not operate in any band which requires CCA-ED, this might change, so statements on CCA-ED were still apposite.

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

Note regarding the following statements in Clauses 18, 22 and 23 respectively:

Unless required by regulation, the CCA-ED shall not be required for license-exempt operation.

The CCA-ED is not required for license-exempt operation in any band.

The CCA-ED is not required for license-exempt operation in any band.

Peter ECCLESINE has commented on these as follows:

The statement is valid until it is not valid, and some future amendment revises it.

The statement precludes optional CCA-ED in 5 GHz in Europe, watch ETSI BRAN EN 301 893 replacement insist on optional CCA-ED by the end of 2015

The statement does not belong in any of the PHY clauses, as it is a behavior of some bands, not a property of a PHY.

So all the info on CCA-ED applicability should be in one place only (Annex D), and there should otherwise be no statements on the applicability of CCA-ED.

Note also that the group expressed a preference for using “detect” rather than “indicate” for what CCA-ED does, on the basis that CCA-ED itself does not indicate, the PHY does.

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. ~~Unless required by regulation, the CCA-ED shall not be required for license-exempt operation.~~

CCA-ED shall ~~indicate~~detect 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—The requirement to ~~indicate~~detect 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)~~.

CCA-ED shall detect 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—The requirement to detect 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. ~~The CCA-ED is not required for license-exempt operation in any band.~~

CCA-ED shall ~~indicate~~detect 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—The requirement to ~~issue~~detect 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. ~~The CCA-ED is not required for license-exempt operation in any band.~~

CCA-ED shall ~~indicate~~detect 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. The CCA-ED thresholds for the operating classes requiring CCA-ED are subject to the criteria in D.2.5 (CCA-ED threshold).

NOTE—The requirement to ~~issue~~detect 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~~The PHY 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 6583Mark 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!).

There are some places where it is not clear that a field that is ignored on reception is required to be 0 on transmission. We need to determine whether it is safe to make such fields reserved (which requires them to be 0 on transmission). Note that not doing so means a field cannot be used for forward-compatibility (future extension).

Proposed changes:

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

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

Change 942.62 as follows “~~A non-AP STA always sets Bits 0–1 to 0. An AP ignores Bits 0–1 on reception.~~Bits 0–1 are reserved in a transmission to an AP.”.

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 in a transmission from an AP.”

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~~The Query Response Length Limit is reserved in a transmission from the requesting STA to the responding STA.”

Change 1001.14 as follows: “The ~~value of the~~ AID field is ~~ignored~~reserved in Association Request, Reassociation Request and Probe Request frames and when used in an IBSS”; Carlos CORDEIRO has confirmed that it is OK to require the transmitter to set this field to 0 in the cases enumerated.

Do not change 1011.37: “The value of the PCP Active subfield is ignored when it applies to a CBAP or SP that resides in a PCP Doze BI”; Payam TORAB has confirmed that it is desirable for the PCP to be able to signal 1 even though at certain times it may not be applicable at the non-PCP STA.

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

At 1865.3 insert a new subclause 11.1 Conventions with the following content and renumber subsequent clauses:

Reserved fields and subfields are set to 0 upon transmission and are ignored upon reception.

Change 1870.34 as follows: “field ~~value~~ is ~~ignored~~reserved” (required to be 0 on tx; see next change).

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.”).

At 1914.36 change “Reserved” to “Zeros”.

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 and also add some other cases in MAC clauses.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6375Mark RISON10.3.5.31596.24 | "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 6376Mark RISON10.3.51593 | 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 6377Mark RISON10.3.51593 | 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.

Also, step c) in 10.3.5.3 AP or PCP association receipt procedures is deleted because it is duplicated in step j) of the same subclause. Jouni MALINEN clarifies that this design of delete-keys-only-on-success was added by 11w but it somehow got lost in the 11mb clean-ups later; note this step does not occur in the reassociation subclause.

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 and the STA is a non-DMG STA, the SME shall refuse the reassociation request by issuing an MLME‑REASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.
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.

NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

1. 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.
2. 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.
3. 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.
4. ~~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).~~
5. 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 2—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, the state ~~variable~~ for the STA shall be set to State 4, or to State 3 if RSNA establishment is required ~~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 and the STA is a non-DMG STA, the SME shall refuse the association request by issuing an MLME‑ASSOCIATE.response primitive with ResultCode NOT\_AUTHENTICATED.
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.

~~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))~~

1. 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.
2. 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.

NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

1. 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.
2. 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.
3. 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.
4. ~~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 2—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, the state for the STA shall be set to State 4, or to State 3 if RSNA establishment is required.
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.~~

**10.3.8 Neighbor report information upon rejection with suggested BSS transition *[Editor: this is a new subclause to be inserted]***

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 has the Reason Code field set to REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION and that includes one or more Neighbor Report elements.

**10.14 SA Query procedures**

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

To send an SA Query Request or SA Query Response frame to a peer STA, the SME shall issue an MLME-SA-QUERY.request or MLME-SA-QUERY.response primitive respectively. Reception of an SA Query Request or SA Query Response frame is signalled to the SME with an MLME-SA-QUERY.indication or MLME-SA-QUERY.confirm primitive respectively . ***<paragraph break>***

A STA that supports the SA Query procedure and receives an SA Query Request frame shall respond with an SA Query Response frame ~~when all~~unless any of the following are true: ***<list>***

* the ~~receiving~~ STA is not currently associated to the ~~sending~~ STA which sent the SA Query Request frame
* the STA has sent a (Re)Association Request frame but has not received a corresponding (Re)Association Response frame and the (Re)AssociateFailureTimeout has not expired~~, and no pending MLME-ASSOCIATE.request or MLME‑REASSOCIATE.request primitives are outstanding for the 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, except in the case of FT to the same AP, 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. 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 delete the SA and temporal keys held for communication with the STA by using the MLME-DELETEKEYS.request primitive and the non-AP STA may move into State 1 (or State 2, for a DMG STA) 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 6625Mark RISON111865.1 | 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 6824Mark RISON111865.1 | 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 temporal key (TK) is defined at 44.17 as “The combination of temporal encryption key and temporal message integrity code (MIC) key.”, which is rather odd (a temporal key is the combination of two temporal keys!). It seems this is some TKIP-related horror, since temporal MIC keys only appear in TKIP-related material; presumably 43.32 is also a TKIP-only thing. To avoid the confusion, just call them “MIC keys”, and make aure they are flagged with TKIP so that when we get rid of TKIP we’ll remember to get rid of them too. This then leaves a TK as being the same thing as a TE(ncryption)K for non-TKIP; again, flag this so we can clean it up one day.

Note that PTK != Pairwise Temporal Key (rather, == Pairwise Transient Key), and similarly for STK. But GTK == Group Temporal Key, and similarly for IGTK and MGTK and MTK.

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~~are 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 43.31: “**station-to-station link (STSL) transient key (STK):** A ~~value that is~~ concatenation of session keys derived from the STSL master key (SMK)~~, initiator MAC address (MAC\_I), peer MAC address (MAC\_P), initiator nonce (INonce), and peer nonce (PNonce), using the pseudorandom function (PRF)~~. ~~The value is split into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), and EAPOL-Key confirmation key (KCK).~~ Its components are an STSL key confirmation key (SKCK), an STSL key encryption key (SKEK), and a temporal key (TK), which is used to protect information exchanged over the link.”

At 44.17: “**temporal key (TK):** TKIP only: The combination of a temporal encryption key and a ~~temporal~~ message integrity code (MIC) key. Non-TKIP: A temporal encryption key.”

At 44.20: “**~~temporal~~ message integrity code (MIC) key:** TKIP only: The portion of a transient key used to validate the integrity of medium access control (MAC) service data units (MSDUs) or MAC protocol data units (MPDUs).” and move to the correct alphabetic ordering position.

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 1953.50: “NOTE 2—When reauthenticating and changing the pairwise key, a race condition might occur when using TKIP. If a frame is received while MLME-SETKEYS.request primitive is being processed, the received frame might be decrypted with one key and

the MIC checked with a different key. Two possible options to avoid this race condition are as follows: the frame might be checked against the old MIC key, and the received frames might be queued while the keys are changed.”

At 1981.50: “Set Temporal Encryption Key and (TKIP only) MIC Key~~s~~” (twice)

At 1982.6 (note that several TKs are involved in step e), namely a pairwise TK, a group TK and possibly an integrity group TK, so the plural is appropriate):

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, and push TKIP’s “a TK is two TKs” confusion behind a clearly-labelled cordon sanitaire.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6576Mark RISON11.5.1.1.101930.12 | 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:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6573Mark RISONB.42647.1 | 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 6716Mark 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:

REVISED [alternate proposal to translate to “MIIT Radio Administration [YYYY] No.nnn”]

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

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

Discussion:

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

There is already inconsistency w.r.t. “boolean” v. “Boolean” (the latter is the majority), but the others (“gaussian”, “legendre”) can be left to the IEEE-SA publications editor.

Proposed resolution:

REVISED

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

This comment will be forwarded to the IEEE-SA publications editor for consideration during publication:

Change “gaussian” to “Gaussian” at 12.9, 12.10 (in D4.0)?

Change “legendre” to “Legendre” at 55.13, 1881.25 (in D4.0)?

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6582Mark 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 6661Mark 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 attribute” to “characteristic” at 1840.1, 1840.8.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6754Mark 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 6771Mark RISON | A few "retry bit"s | Change all of them to "Retry bit"s |

Discussion:

(The commenter intended to write “Retry subfield” in the proposed change.)

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 6795Mark 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 that are not IBSSs” at 1730.45.

Change “non-IBSS network” to “BSS that 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 that are not infrastructure BSSs” at 80.57, 952.9.

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6788Mark RISON | "bufferable" v. "buffered" -- there is confusion in these terms. Probably move to "buffered" for most cases | As it says in the comment |
| CID 6819Mark RISON3.221.31 | "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 6298Mark 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 6561Mark 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.

As regards calling what are actually MMPDUs frames, the boat has not only sailed but circumnavigated the globe several times and is now enjoying life taking tourists around tropical island paradises. The best we can do is be honest about the terminological laxity, except in those situations where exactness is critical (e.g. exactly what the unit of buffering is in PS mode).

Proposed changes:

Change 26.1 as follows (note to the Editor: the deletion in the definition of BU is also made in 15/1010, which also adds a NOTE):

**~~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 and renumber subsequent NOTEs in this subclause:

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.

NOTE 2—MMPDUs are, however, often informally referred to as frames, e.g. a “Probe Response frame” rather than a “Probe Response MMPDU”.

Change “MMPDU” to “frame” at 1265.45, 2286.57, 2851.11.

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

Change “An Action, Disassociation, or Deauthentication frame” to “An MMPDU that is carried in one or more Action, Disassociation, or Deauthentication frames” at 1548.30.

Change “An individually addressed Probe Response frame that is sent in an IBSS in response to an individually addressed Probe Request frame” to “An individually addressed MMPDU that is carried in one or more Probe Response frames and that is sent in an IBSS in response to an individually addressed Probe Request frame” at 1548.33.

Change “All other Management frames” to “All other MMPDUs” at 1548.37.

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 a 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 for CID 6788:

Make the changes shown under “Proposed changes” for CIDs 6788, 6819, 6298, 6561 in <this document>.

Proposed resolution for CIDs 6819 and 6298:

Make the changes shown under “Proposed changes” for CIDs 6788, 6819, 6298, 6561 in <this document>, which effect the requested change.

Proposed resolution for CID 6561:

Make the changes shown under “Proposed changes” for CIDs 6788, 6819, 6298, 6561 in <this document>. These clarify that MMPDUs are often loosely referred to as frames.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 5062Adrian StephensM.4.23489.6 | 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:

REVISED [alternate proposal to delete the reference code in 15/0999r4]

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 |
| CID 6295Mark RISON | The things which are cached are the SAs, not just the Ks | Change "PMK cached" to "PMKSA cached" at 1926.5, "SMK cache" to "SMKSA cache" at 2903.32, "SMK caching" to "SMKSA caching" at 3287.31 |

Discussion:

There are three instances of “K cach” in the current draft (and none of “key cach”):

1926.4: PMKSA: A result of a successful IEEE Std 802.lX exchange, SAE authentication, preshared PMK information, or PMK cached via some other mechanism.

2903.32: The maximum lifetime of an SMK in the SMK cache.

3287.20: The dot11RSNSMKcachingGroup object class provides the necessary support for managing SMK caching functionality in the STA.

There are 26 instances of “KSA cach”, 24 of which are “PMKSA caching”; the two others and one of the “PMKSA caching” ones being:

1940.53: The PMKSA is inserted into the PMKSA cache.

2899.39: The maximum lifetime of a PMK in the PMKSA cache.

3287.10: The dot11RSNPMKcachingGroup object class provides the necessary support for managing PMKSA caching functionality in the STA

Note a PMKSA contains more than just a PMK, e.g. it contains the PMKID to identify the SA and the addresses to identify the pairwise link to which it applies (see 11.5.1.1.2). Similarly an SMKSA contains more than just an SMK (see 11.5.1.1.11).

It is not meaningful to just cache a PMK or SMK. You need to cache the whole SA, so that you can identify it and which pairwise link it applies to, etc. Ergo, we need to change references to cached Ks to being about cached KSAs.

It’s not clear that SMKSAs can actually be cached, though. There is a lot of text about PMKSA caching (e.g. 4.10.7 PMKSA caching; 11.5.10.3 Cached PMKSAs and RSNA key management) but essentially nothing about SMKSA caching. It seems SMKSA caching was the result of over-enthusiastic cut and pasting.

Proposed resolution:

REVISED

Change 1926.4 to read: “PMKSA: A result of a successful IEEE Std 802.lX exchange, SAE authentication, or preshared PMK information. A PMKSA can be cached.”

Add a full stop at the end of the sentence at 3287.10: “The dot11RSNPMKcachingGroup object class provides the necessary support for managing PMKSA caching functionality in the STA”.

At 2903.32 change “SMK cache” to “SMKSA cache”.

At 3287.21 change “SMK caching” to “SMKSA caching”.

Change 2903.26, 2903.39 and 3287.18 (dot11RSNAConfigSMKLifetime, dot11RSNAConfigSMKReauthThreshold and dot11RSNSMKcachingGroup) to read “STATUS deprecated” and at the start of the DESCRIPTION for each of these add “Deprecated because SMKSAs cannot be cached.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6364Mark RISON11.3.5.41884.56 | "KCK || KEK" is not the way it's done anywhere else, and the inconsistency leads to unnecessary doubt | Change "KCK || PMK" to "kck\_and\_pmk" at 1884.56.Add "KCK = L(kck\_and\_pmk, 0, 256)" after the equation at 1884.56.Add "PMK = L(kck\_and\_pmk, 256, 256)" after the equation at 1884.56.In all cases, italicise "kck\_and\_pmk". |
| CID 6365Mark RISON11.3.5.41884.56 | "KCK || KEK" is not the way it's done anywhere else, and the inconsistency leads to unnecessary doubt | Change "KCK || PMK" to "kck\_and\_pmk" at 1884.56.Add "KCK = L(kck\_and\_pmk, 256, 256)" after the equation at 1884.56.Add "PMK = L(kck\_and\_pmk, 0, 256)" after the equation at 1884.56.In all cases, italicise "kck\_and\_pmk". |
| CID 6366Mark RISON11.3.5.41884.56 | "KCK || KEK" is not the way it's done anywhere else, and the inconsistency leads to unnecessary doubt | Change all other instances of extraction of subfields from a KDF to use the || formulation (I can provide a list of such instances) |

Discussion:

Clearly the proposed changes for CIDs 6364 and 6365 cannot both be correct.

It is better to use a single formulation for extraction of subfields (KCK, KEK, etc.) from a KDF, so that there can be no doubt about the intent and no question that things are being done differently. The formulation with explicit extraction using the L operator seems preferable to that with implicit extraction using assignment to multiple concatenated entities (and the former is used everywhere except for one instance of the latter). So the opposite of the proposed change for CID 6366 should be adopted (i.e. the changes proposed for one of CIDs 6364 and 6365).

So the only question is: what was intended at 1884.56? Is it the same as all the others, or the other way round?

Well, as 1914.43 suggests, A || B needs to be regarded as the string where A comes first (smaller bit indices) and B comes last (larger bit indices): Does this need to be made more explicit?



So in KCK || PMK = KDF-512 (…) the bit string given by the KDF is taken such that KCK comes first (smaller bit indices). Therefore the second argument of L() would be 0 in the assignment to KCK. Reassuringly, this matches 1954.19 (though the formatting is all messed up), 1957.11, 1961.45, 1997.40.

Proposed resolution for CID 6364:

ACCEPTED

Proposed resolution for CID 6365:

REJECTED

This is not the correct order. See CID 6364.

Proposed resolution for CID 6366:

REJECTED

It is clearer and more consistent to show the assignments to KCK and KEK separately. See CID 6364.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6527Mark RISON | It sometimes says "STA in an ESS" and sometimes "STA in an infrastructure network" or "... BSS" | Be consistent. Reserve "STA in an ESS" to the cases which require a multi-BSS STA. Use "STA in an infrastructure BSS" (or "... network" -- see other comment) for other cases |
| CID 6529Mark RISON | It says "AP in an infrastructure BSS" or "... network" or "... ESS" | Delete "in an infrastructure \*" in all cases |

Discussion:

An ESS can in theory consist of a single infrastructure BSS, but it is only “interesting” if it consists of more than one. Thus when something applies irrespective of whether there are multiple BSSen, the term “infrastructure BSS” should be used in preference.

An AP can’t be in anything else than an infrastructure BSS.

Proposed resolution for CID 6527:

REVISED

Change “In an ESS” to “In an infrastructure BSS” at 110.35, 116.22, 1938.61, 1939.4, 1951.8, 2008.6.

Change “in an ESS” to “in an infrastructure BSS” at 649.54, 649.59, 1272.4, 1591.58, 1592.20, 1865.60, 1866.18, 1867.33, 1872.63, 1930.11, 1934.49, 1934.51, 1935.39, 1936.19, 1939.38, 1941.8, 1943.30, 3158.64.

Proposed resolution for CID 6529:

REVISED

Change 876.41 from “An AP in an infrastructure BSS or a STA in an IBSS sets” to “An AP, or a STA in an IBSS, sets”.

Delete “in an infrastructure BSS” at 1686.32.

Delete “in an ESS” at 2897.27.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6676Mark RISON | How do "CH\_OFFSET\_ABOVE/BELOW/NONE" relate to "CH\_OFF\_20/40/20L/20U"? | Clarify |
| CID 6677Mark RISON | Get rid of the wacko HT modes signalled by CH\_OFF\_20U/L, since they're not used. | As it says in the comment |

Discussion:

The core of the problem is that there are two uses of “CH\_OFFSET”s.

The CHANNEL\_OFFSET parameter in the PHYCONFIG\_VECTOR can take the value CH\_OFFSET\_NONE, CH\_OFFSET\_ABOVE or CH\_OFFSET\_BELOW, and indicates the relative position of the secondary channel, if any, compared with the primary channel.

The CH\_OFFSET parameter in the TXVECTOR can take the value CH\_OFF\_20, CH\_OFF\_40, CH\_OFF\_20U or CH\_OFF\_20L, and indicates which part of the channel is used for transmission.

The 20/40 MHz mask PPDU definitions in Clause 3 refer to CH\_OFFSET (and CH\_BANDWIDTH, another TXVECTOR parameter).

Table 20-2 describes what goes over the air, again based on CH\_OFFSET and CH\_BANDWIDTH in the TXVECTOR.

The PHYCONFIG\_VECTOR CH\_OFFSETs are in fact only used in VHT Subclause 22.2.4.3 Support for HT formats:



Calling the PHYVECTOR\_CONFIG something other than “OFFSET” would help, since it’s not really a channel offset, it’s an ordering.

I’m still not clear on how CH\_OFF\_20U and CH\_OFF\_20L are used. Is it that the one corresponding to the primary channel has to be selected by the MAC, when using a 20 MHz transmission in a 40 MHz channel? Where is this specified? The fact that CHANNEL\_OFFSET is only used in Clause 22 makes me suspect that this is a VHT mistake: instead of inventing a new CHANNEL\_OFFSET parameter, the MAC should be selecting the appropriate CH\_OFFSET (CH\_OFF\_20U or CH\_OFF\_20L) when trying to transmit a 20 MHz HT PPDU. Similarly, it looks as if OPERATING\_CHANNEL is a mistake: the pre-VHT PHYs use dot11CurrentFrequency/PrimaryChannel/SecondaryChannel and this PHYVECTOR\_CONFIG parameter is not otherwise used at all.

Proposed changes:

Change CHANNEL\_OFFSET to SECONDARY\_CHANNEL\_OFFSET at 545.32, 2469.55, 2470.31 and 2470.60.

Change CH\_OFFSET\_NONE to SECONDARY\_CHANNEL\_NONE at 545.33 and 2470.60.

Change CH\_OFFSET\_ABOVE to SECONDARY\_CHANNEL\_ABOVE at 545.35 and 2470.61.

Change CH\_OFFSET\_BELOW to SECONDARY\_CHANNEL\_BELOW at 545.38 and 2470.61.

Add a new subclause after 20.2.2 TXVECTOR and RXVECTOR parameters:

 **20.2.2b PHYCONFIG\_VECTOR parameters**

The PHYCONFIG\_VECTOR carried in a PHY-CONFIG.request for an HT PHY contains an OPERATING\_CHANNEL parameter, which identifies the operating or primary channel. The PHY shall set dot11CurrentPrimaryChannel to the value of this parameter.

The PHYCONFIG\_VECTOR carried in a PHY-CONFIG.request for an HT PHY contains a SECONDARY\_CHANNEL\_OFFSET parameter, which takes one of the following values:

* SECONDARY\_CHANNEL\_NONE if no secondary channel is present; in this case the PHY shall set dot11CurrentSecondaryChannel to 0.
* SECONDARY\_CHANNEL\_ABOVE if the secondary channel is above the primary channel; in this case the PHY shall set dot11CurrentSecondaryChannel to dot11CurrentPrimaryChannel + 4.
* SECONDARY\_CHANNEL\_BELOW if the secondary channel is below the primary channel; in this case the PHY shall set dot11CurrentSecondaryChannel to dot11CurrentPrimaryChannel – 4.

Add a new subclause after 22.2.2 TXVECTOR and RXVECTOR parameters:

 **22.2.2b PHYCONFIG\_VECTOR parameters**

The PHYCONFIG\_VECTOR carried in a PHY-CONFIG.request for a VHT PHY contains an OPERATING\_CHANNEL parameter, which identifies the operating or primary channel. The PHY shall set dot11CurrentPrimaryChannel to the value of this parameter.

The PHYCONFIG\_VECTOR carried in a PHY-CONFIG.request for a VHT PHY contains a CHANNEL\_WIDTH parameter, which identifies the operating channel width and takes one of the values 20 MHz, 40 MHz, 80 MHz, 160 MHz and 80+80 MHz. The PHY shall set dot11CurrentChannelWidth to this value.

<repeat for dot11CurrentChannelCenterFrequencyIndex0/1>

In 18.3.8.4.1 change “The OFDM PHY shall use dot11CurrentFrequency to determine the operating frequency.” to “The PHYCONFIG\_VECTOR carried in a PHY-CONFIG.request for an OFDM PHY contains an OPERATING\_CHANNEL parameter, which identifies the operating channel.” <and change the MIB variable to being written by the PHY> <and add similar wording in the DSSS and HR/DSSS PHYs and the ERP>

In 22.2.4.2 Support for NON\_HT format when NON\_HT\_MODULATION is OFDM: <this kind of stuff is needed in Clause 20 too, to cover Clause 16-19 PPDUs>

When the VHT PHY receives a Clause 22 (Very High Throughput (VHT) PHY specification) PHYCONFIG.request(PHYCONFIG\_VECTOR) primitive, the VHT PHY shall, for the purposes of OFDM PPDU transmission and reception, behave as if it were a Clause 18 PHY that had received a ~~issue a Clause 18 (Orthogonal frequency division multiplexing (OFDM) PHY specification)~~ PHYCONFIG.request(PHYCONFIG\_VECTOR) primitive but with the ~~OPERATING\_CHANNEL and~~ CHANNEL\_OFFSET parameter~~s~~ discarded from PHYCONFIG\_VECTOR. In order to transmit a non-HT PPDU, the MAC shall set the CH\_BANDWIDTH and CH\_OFFSET in the TXVECTOR to achieve the required non-HT PPDU format (see Table 20-2); for 20 MHz bandwidth transmissions in a 40 MHz channel, the CH\_OFFSET shall be CH\_OFF\_20U if $above, or CH\_OFF\_20L if $below. ~~In order to transmit a non-HT non-duplicate PPDU on the primary channel, the MAC shall [why is all this “the MAC shall” stuff buried in a PHY clause anyway?] configure dot11CurrentFrequency to dot11CurrentPrimaryChannel before transmission.~~

In 22.2.4.3 Support for HT formats:

When the VHT PHY receives a Clause 22 (Very High Throughput (VHT) PHY specification) PHYCONFIG.request(PHYCONFIG\_VECTOR) primitive, the VHT PHY shall, for the purposes of HT PPDU transmission and reception, behave as if it were a Clause 20 PHY that had received a ~~issue a Clause 20 (High Throughput (HT) PHY specification)~~ PHYCONFIG.request(PHYCONFIG\_VECTOR) primitive but with the CHANNEL\_WIDTH parameter discarded from the PHYCONFIG\_VECTOR and ~~the OPERATING\_CHANNEL parameter set to min(40 MHz, dot11CurrentChannelWidth) and~~ the SECONDARY\_CHANNEL\_OFFSET parameter set to SECONDARY\_CHANNEL~~\_OFFSET~~\_NONE if dot11CurrentChannelWidth indicates 20 MHz, to SECONDARY\_CHANNEL~~\_OFFSET~~\_ABOVE if $above, or to SECONDARY\_CHANNEL~~\_OFFSET~~\_BELOW if $below. In order to transmit an HT PPDU, the MAC shall set the CH\_BANDWIDTH and CH\_OFFSET in the TXVECTOR to achieve the required HT PPDU format (see Table 20-2); for 20 MHz bandwidth transmissions in a 40 MHz channel, the CH\_OFFSET shall be CH\_OFF\_20U if $above, or CH\_OFF\_20L if $below. ~~In order to transmit a non-HT PPDU or 40 MHz HT PPDU on a 40 MHz channel, the MAC shall~~ [isn’t all this “the MAC shall” stuff needed in a non-VHT HT STA’s MAC too? And shouldn’t it in both cases be in Clause 9 or 10?] ~~configure dot11CurrentSecondaryChannel [why does this need to be stated? Both the HT and VHT PHYs have dot11CurrentSecondaryChannel so it’s already set] to $secondary before transmission~~. The quantities $primary and $secondary are defined in 22.3.7.3 (Channel frequencies).

Change “PHYCONFIG-VECTOR” to “PHYCONFIG\_VECTOR” at 545.42.

Proposed resolution:

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6323Mark RISON3.243.10 | The definition of "STSL" appears to preclude a direct link between STAs in a PBSS | Add "or PCP" after "AP" at 43.12 |
| CID 6459Mark RISON11 | What is the difference between an STSL and a TDLS link? The must be different because there's an STKSA and also a TPKSA | Clarify |

Discussion:

An STSL is defined as follows:

**station-to-station link (STSL):** A direct link established between two stations (STAs) while associated to a common access point (AP). This term refers to a generic mechanism that allows direct station-to-station communication while remaining in the infrastructure mode. Establishment of this type of link includes an initialization step. The STSL is terminated by specific teardown procedures under the conditions prescribed in this standard.

As written, this does indeed preclude direct links between STAs in a PBSS, since it explicitly talks of APs. It’s also slightly ambiguous in that it could be read as referring to a plain STA-AP link.

However, it is not clear the whole concept has any value. It seems to be the terminology for the (non-tunnelled) direct links introduced in 11e. The tunnelled direct links introduced in 11z have their own terminology, including different SAs (TPKSA as opposed to STKSAs). The STSL SAs are incompletely specified (e.g. there are references to SMK caching but no actual words to specify it). Since everyone uses 11z TDLS and no-one uses 11e DLS, it seems simpler to just kill 11e STSLs.

For reference, if/when 11e STSLs are killed, search for “STSL”, “SKEK”, “SKCK”, “SMK”, “SMKSA”, “STK”, “STKSA”, “PeerKey”, “DLS” not as part of “TDLS”, “direct link” (possibly hyphenated) not as part of “tunnelled direct link” (including those in TSPECs?). But note that “AP PeerKey” is an 11aa thing which is distinct from 11e “PeerKey”, though it does result in an SMKSA and STKSA.

Missing deletion of TPKs around 103.34?

Proposed changes:

Change 43.10 as follows:

**station-to-station link (STSL):** A direct link established between two non-access-point (non-AP) stations (STAs) while associated to a common access point (AP), that was not established using tunneled direct-link setup (TDLS). ~~This term refers to a generic mechanism that allows direct station-to-station communication while remaining in the infrastructure mode. Establishment of this type of link includes an initialization step. The STSL is terminated by specific teardown procedures under the conditions prescribed in this standard.~~

Add at the start of 10.7.1 General (in 10.7 DLS operation): “The STSL mechanism is obsolete. Consequently, the DLS protocol might be removed in a later revision of the standard.”

Add at the start of 11.1.5 RSNA PeerKey Support: “The STSL mechanism is obsolete. Consequently, the PeerKey protocol (not to be confused with the AP PeerKey protocol) might be removed in a later revision of the standard.”

Proposed resolution:

REVISED

Make the changes the changes shown under “Proposed changes” for CID 6323 and 6459 in <this document>. These restrict the scope of STSLs to direct links in an infrastructure BSS, that have not been set up using TDLS, and obsolete such links.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6426Mark RISON9.3.2.12.31262.53 | "When a Data, Management or Extension frame is received in which the Retry subfield of the Frame Control field is equal to 1, the appropriate cache is searched for a matching frame. If the search is successful, the frame is considered to be a duplicate." -- this does not apply when an MSDU is sent under a BA agreement, since the Retry bit need not be set and in any case the BA bitmap is consulted to look for dupes, not the cache | Amend the wording accordingly |
| CID 6490Mark RISON9.3.2.12.31262.47 | This subclause does not cover BA, where a SN cache is not consulted (a BA bitmap window is consulted), even if the Retry bit is set (1262.53) | Add words to that effect |

Discussion:

The Retry bit is not required to be set in MPDUs sent under a BA agreement, per 1364.14: “A non-DMG originator does not need to set the retry bit to 1 for any possible retransmissions of the MPDUs.” (Ooh, this only applies to non-DMG STAs! DMG STAs do set the retry bit to 1 even under BA!)

Mark HAMILTON observes:

Disagree. The text at the start of 9.3.2.12 says, "Additional duplicate filtering is performed during Receive Buffer Operation for frames that are part of a block ack agreement". This indicates that the receiver cache filtering is done under Block Ack agreement (although only if the Retry bit is equal to 1). If the Retry bit really can never be equal to 1 under Block Ack, then the receiver cache text is moot, per the sentence the commenter quoted, so no change is needed. If the Retry bit can ever be equal to 1 under Block Ack, then the question is whether the receiver cache would falsely discard a valid (non-duplicate) frame. There does not seem to be such a problem case, so again, it is equivalent function to invoke the receiver cache or not, along with the Block Ack processing rules, and no change is necessary.

However:

* Some bits of the spec suggest all STAs (including DMG STAs) are allowed to not set the Retry bit for things under a BA agreement
* Table 9-4—Receiver Caches doesn’t admit an exclusion for things sent under a BA agreement in a non-DMG BSS
* Table 9-4—Receiver Caches does not require duplicate QoS Data frames to be discarded (!)
* Table 9-4—Receiver Caches and Table 9-3—Transmitter sequence number spaces are inconsistent as to their position on the (+)ness of QoS Nulls

Proposed changes:

Change the table at 1264.1 to modify the header and RC2 rows and insert a new RC9 row:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Receiver ~~C~~cache ~~I~~identifier** | **Cache ~~Name~~** | **Applies to** | **Status** | **Multiplicity / Cache size** | **Receiver requirements** |
| RC2 | QoS Data | A QoS STA receiving anindividually addressed QoSData frame, excluding RC3 and, if supported, RC9 | Mandatory | Indexed by: <Address 2, TID, sequence number, fragment number>.At least the most recent cache entry per <Address 2, TID> pair in this cache. | RR1RR5 |
| RC9 | QoS Data under BA | A non-DMG QoS STA receiving a QoS Data frame sent under a BA agreement | Recommended | None | RR4 |

Also change the caption from “Receiver Caches” to “Receiver caches”.

Change 1265.24 as follows:

RR4: For the purposes of duplicate detection using receiver caches, QoS (+)Null frames and, in a non-DMG BSS, QoS Data frames under a BA agreement, shall be ignored.

Change 1262.53 as follows:

When a Data, Management or Extension frame is received in which the Retry subfield of the Frame Control field is equal to 1, the appropriate cache, if any, is searched for a matching frame. If the search is successful, the frame is considered to be a duplicate. Duplicate frames are discarded.

Change “QoS Null” to “QoS (+)Null” at 1263.24 (2x) and 1264.23 (2x).

Change 1334.16 as follows (note to Editor: a different CID might change “Retry field” to “Retry subfield”):

All retransmission attempts by a non-DMG STA for an MPDU that is not sent under a block ack agreement and that has failed the acknowledgment procedure one or more times shall be made with the Retry field set to 1 in the Data or Management frame. All retransmission attempts by a DMG STA for an MPDU that has failed the acknowledgment procedure one or more times shall be made with the Retry field set to 1 in the Data or Management frame.

Proposed resolution:

REVISED

Make the changes the changes shown under “Proposed changes” for CID 6426 and 6490 in <this document>, which clarify the duplicate filtering rules as they pertain to BA operation.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6452Mark RISON9.3.2.91260.38 | How does EIFS (= aSIFSTime + ACKTxTime + DIFS) work if the ack timeout (= aSIFSTime + aSlotTime + aRxPHYStartDelay) is a significant fraction of it, in the case where the Ack is corrupted? | At 1260.38, after "In this instance, the STA shall invoke its backoff procedure at the PHY-RXEND.indication primitive and may process the received frame" add "NOTE---If a frame with an incorrect FCS is received, EIFS is used in the course of this backoff procedure (see 9.3.2.3.7)." |

Discussion:

If the Ack immediately following a frame needing an Ack is corrupted, 1260.35 will cause backoff to be invoked. Assuming something was received at the STA expecting the Ack, 1252.34 will also cause EIFS to be used by that STA. This interplay is not immediately obvious.

Proposed changes:

Change 1260.24 as follows:

After transmitting an MPDU that requires an Ack frame as a response (see Annex G), the STA shall wait for an AckTimeout interval, with a value of aSIFSTime + aSlotTime + aRxPHYStartDelay, starting at the PHYTXEND.confirm primitive. If a PHY-RXSTART.indication primitive does not occur during the AckTimeout interval, the STA concludes that the transmission of the MPDU has failed, and this STA shall invoke its backoff procedure upon expiration of the AckTimeout interval. If a PHY-RXSTART.indication primitive does occur during the AckTimeout interval, the STA shall wait for the corresponding PHY-RXEND.indication primitive to determine whether the MPDU transmission was successful. The recognition of a valid Ack frame sent by the recipient of the MPDU requiring acknowledgment, corresponding to this PHY-RXEND.indication primitive, shall be interpreted as successful acknowledgment, permitting the frame sequence to continue, or to end without retries, as appropriate for the particular frame sequence in progress. The recognition of anything else, including any other valid frame, shall be interpreted as failure of the MPDU transmission. In this instance, the STA shall invoke its backoff procedure at the PHY-RXEND.indication primitive and may process the received frame.

NOTE—The backoff procedure in the specific case of reception of a corrupted Ack frame results, subject to dot11DynamicEIFSActivated, in EIFS rather than DIFS or AIFS being used after the AckTimeout interval and subsequent reception of the corrupted Ack frame (see 9.3.4.3 and 9.22.2.4 respectively).

An exception is that recognition of a valid Data frame sent by the recipient of a PS-Poll frame shall also be accepted as successful acknowledgment of the PS-Poll frame.

Proposed resolution:

REVISED

Insert “NOTE—The backoff procedure in the specific case of reception of a corrupted Ack frame results in EIFS rather than DIFS or AIFS being used after the AckTimeout interval and subsequent reception of the corrupted Ack frame (see 9.3.4.3 and 9.22.2.4 respectively).” at the location suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6235Mark RISON | "basic MCS set" could be confused with the VHT version thereof | Change "basic MCS set" to "basic HT-MCS set" throughout (case-preservingly) |

Discussion:

See 15/1010r8.

Proposed changes:

Add a new definition in Subclause 3.2:

**high throughput modulation and coding scheme (HT-MCS):** A specification of the HT physical layer (PHY) parameters that consists of modulation order (e.g., BPSK, QPSK, 16-QAM, 64-QAM) and forward error correction (FEC) coding rate (e.g., 1/2, 2/3, 3/4, 5/6) and that is used in an HT PHY protocol data unit (PPDU).

At 2655.44 change “VHT Basic MCS Set” to “Rate selection constraints for VHT PPDUs”.

At 1288.46 change “9.7.4 Basic Rate Set and Basic MCS Set for mesh STA” to “9.7.4 Basic rate set, basic HT-MCS set and basic VHT-MCS and NSS set for mesh STA”.

Globally change “Basic MCS Set” to “Basic HT-MCS Set” (case sensitive).

Globally change “basic MCS set” to “basic HT-MCS set” (case sensitive).

Globally delete “BSS” in “BSS basic VHT-MCS and NSS set” (and change to “Basic” if at the start of a sentence etc.).

At 1606.65 delete “BSS” in “BSS basic rate set”.

At 1607.65 delete “BSS” in “BSS basic HT MCS set” and replace the space in “HT MCS” with a hyphen.

Proposed resolution:

Make the changes the changes shown under “Proposed changes” for CID 6235 in <this document>, which effect the requested change and tidy up a couple of related things too.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6802Mark RISON | In clauses other than clause 8, it is not clear that reserved fields are ignored on reception (some honourable exceptions, e.g. in Table 21-11--Control PHY header fields and 18.3.4.4 Parity (P), Reserved (R), and SIGNAL TAIL fields). | Make the behaviour at the receiver clear for reserved bits in all clauses |
| CID 6803Mark RISON | Sometimes the value of reserved bits is not specified in the PHY. | Specify them |

Discussion:

It is important to be clear what value reserved bits are to be set to on transmission, and that these bits are to be ignored on reception (see CID 6583 for theMAC/security version of this).

Proposed changes:

At 2174.28 change to “The LENGTH parameter provided […]”.

At 2174.41 change to “The SERVICE parameter shall be null.”

At 2175.18 and 2176.30 change “1, 2 Mb/s” to “Null”.

At 2175.20 change “Level1, Level2, Level3, Level4” to “1 to 8”.

At 2175.55 change “SERVICE” to “RXVECTOR SERVICE” and change the next line to read “The SERVICE parameter shall be null.”

At 2178.58 change the first sentence to “The 8-bit SERVICE field is reserved for future use; it shall be set to 0 on transmission and ignored on reception.” (Note: this aligns with the wording proposed in 16.3.7 under the “CS zoo” resolution.)

At 2201.55 change “Three” to “Two”.

At 2202.3 add “on transmission and ignored on reception” to the end of the sentence.

Change 2206.6 as follows:

The SIGNAL ~~and SERVICE~~ field~~s combined shall~~ indicates the ~~modulation~~rate that ~~shall be~~is used to transmit the PSDU. ~~The SIGNAL field indicates the rate, and the SERVICE field indicates the modulation.~~ The transmitter and receiver shall initiate the ~~modulation and~~ rate indicated by the SIGNAL ~~and SERVICE~~ field~~s~~, starting with the first octet of the PSDU

Change 2207.6 as follows:

The SIGNAL ~~and SERVICE~~ field~~s combined shall~~ indicates the ~~modulation~~rate that ~~shall be~~is used to transmit the PSDU. ~~The SIGNAL field indicates the rate, and the SERVICE field indicates the modulation.~~ The transmitter and receiver shall initiate the ~~modulation and~~ rate indicated by the SIGNAL ~~and SERVICE~~ fields, starting with the first octet of the PSDU.

Change 2229.59 under Value to “Null”.

Change 2230.41 to “The SERVICE parameter shall be null.”

Change 2232.60 to “The SERVICE parameter shall be null.”

Add “RXVECTOR” to the subclause titles at 2232.50 and 2232.58.

At 2243.23 after “All reserved bits shall be set to 0” add “ on transmission and ignored on reception”.

Change 2277.49 under Value to the first sentence there and then just “Null”.

Change 2291.33 and 2291.40 under Value to “null” after the comma.

Change 2412.25 under “Description” to “Differential detector initialization”.

Change 2412.39/40 and 2417.29/30 and 2431.7 under “Description” to be an empty cell.

Change the first two sentences at 2430.52 and 2417.13 to “Contains a copy of the parameter LAST\_RSSI from the TXVECTOR, or 0. When 0, this field is ignored by the receiver.”

Proposed resolution:

Make the changes the changes shown under “Proposed changes” for CID 6802 and 6803 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6684Mark RISON | Suspect uses of "will not", e.g. "The value of Nr within an explicit Beamforming feedback frame transmitted by a VHT beamformee will not exceed the value indicated in the Beamformee STS Capability subfield of the VHT Capabilities element." and "The AP will not deliver the requested streams at the delivery interval as specified by the non-AP STA in the FMS Request element." Either make into a NOTE or reformulate with "shall" or otherwise (e.g. latter is "does not" nearby). | As it says in the comment |

Discussion:

The first citation does not appear in D4.0. However, the second does and the general thrust of the comment is valid: “will not” is a modal verb without a defined meaning in the context of this standard, so should not be used except (a) in NOTEs, (b) when describing behaviour of a third party and (c) when describing behaviour signalled by formatting (in Clause 8).

Proposed changes:

Not sure about 854.22: “A station sending a preauthentication frame to the BSSID will not receive a response even if the AP indicated by the BSSID is capable of preauthentication.”

Change 985.58 as follows:

Bit 2: Proactive PREP subfield (0 = off, 1 = on). The Proactive PREP subfield is of relevance only if the Target Address is the broadcast address (all 1s). If equal to 1, every recipient of a PREQ element with Target Address equal to the broadcast address replies with a PREP element. If equal to 0, ~~it will~~recipients reply only under certain conditions (see 13.10.4.2 (Proactive PREQ mechanism)); ~~it will~~recipients do not reply otherwise.

Change 1568.40 as follows: “The AP ~~will~~does not deliver the requested streams at the delivery interval as specified by the non-AP STA in the FMS Request element.”

Change 1869.22 as follows: “In an infrastructure BSS, the STAs with emergency services association should discard all group addressed frames they receive, as they do not possess the Group Key and ~~will not be~~so are not able to decrypt group addressed frames.”

Not sure about 2939.18: “The STA will not transmit Location Track Notification frames when the Normal Report Interval is 0.” (is this about a third-party STA?).

Change 3268.31 as follows:

This attribute is used only by the responding STA in a GAS exchange. When true, it indicates that the responding STA ~~will~~does not transmit a GAS Initial Response frame until it receives the query response from the Advertisement Server or a timeout occurs. When false, the STA ~~will~~does not wait for a response from the Advertisement Server before transmitting the GAS Initial Response frame. The setting of this MIB object is outside the scope of this standard.

Not sure about 3583.29: “Unlike an AP providing RM capability, an AP Advertisement location capability will not return an “incapable” response if the non-AP STA requests the “remote” location.” (I don’t even understand what this means: how can a capability return anything?).

Change 3590.24 as follows: “While no mechanism is defined to measure the average data rate and the frame error rate, ~~it is expected that numeric values will not~~numeric values are not expected to exhibit large nonmonotonic variations in amplitude over the lifetime of a path.”

Proposed resolution:

Make the changes the changes shown under “Proposed changes” for CID 6684 in <this document>.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 6299Mark RISON | What is a "frame exchange" (anything with not more than one non-Control frame?)? What is a "frame exchange sequence" (anything with SIFS/RIFS separation?)? | Clarify (see strawmen in comment) |

Discussion:

There are 254 instances of “frame exchange”, of which 114 are followed by “sequence”; neither of these terms is defined (though Annex G is entitled “Frame exchange sequences” and hence could be considered a definition by enumeration).

The strawman proposal is to add definitions like these to 3.2:

**frame exchange**: A sequence of frames that does not include more than Data or Management frame

**frame exchange sequence**: A sequence of frames separated by SIFS and/or RIFS

These are easily beaten: an A-MPDU with more than one Data frame, followed by a BlockAck frame, is surely a frame exchange, and as Annex G shows frame exchange sequences can in some cases involve PIFS (though, interestingly, they apparently cannot involve RIFS (“Except where modified by the *pifs* attribute, frames are separated by a SIFS.”)). Another attempt is:

**frame exchange**: A sequence of frames

**frame exchange sequence**: A sequence of frames specified by Annex G

However, the first of these is too vague, because anything with more than one frame would be a frame exchange, even if the two frames are logically completely unconnected. And it is probably the case that many/most of the instances of “frame exchange” are actually referring to something specified by Annex G (i.e. the “sequence” should be there).

Perhaps the solution is to only define “frame exchange sequence” and try to patch up other terms if and when they are found lacking?

An example of this (ironically, involving a third term “frame sequence” which appears 49 times, though a number are “GAS frame sequence”s or “ASEL training frame sequence”, and a number are search artefacts) is in 10.2.5:

In dynamic SM power save mode, the STA enables its multiple receive chains when it receives the start of a frame sequence addressed to it. Such a frame sequence shall start with a single-spatial stream individually addressed frame that requires an immediate response and that is addressed to the STA in dynamic SM power save mode. An RTS/CTS sequence may be used for this purpose. The STA shall, subject to its spatial stream capabilities (see 8.4.2.55.4 (Supported MCS Set field) and 8.4.2.157.3 (Supported VHT-MCS and NSS Set field)) and operating mode (see 10.42 (Notification of operating mode changes)), be capable of receiving a PPDU that is sent using more than one spatial stream a SIFS after the end of its response frame transmission. The STA switches to the multiple receive chain mode when it receives the RTS addressed to it and switches back immediately when the frame sequence ends.

NOTE—A STA in dynamic SM power save mode cannot distinguish between an RTS/CTS sequence that precedes a MIMO transmission and any other RTS/CTS and, therefore, always enables its multiple receive chains when it receives an RTS addressed to itself.

The STA can determine the end of the frame sequence through any of the following:

— It receives an individually addressed frame addressed to another STA.

— It receives a frame with a TA that differs from the TA of the frame that started the TXOP.

— The CS mechanism (see 9.3.2.1 (CS mechanism)) indicates that the medium is idle at the TxPIFS slot boundary (defined in 9.3.7 (DCF timing relations)).

If the STA switches back too early, it will miss some of the AP’s frames. If it switches back too late, it will waste power.

Proposed changes:

In Subclause 3.2 add the following definition:

**frame exchange sequence**: A sequence of frames specified by Annex G

In Subclause 10.2.5 make the following changes:

In dynamic SM power save mode, the STA enables its multiple receive chains when it receives the start of a frame exchange sequence addressed to it. Such a frame exchange sequence shall start with a single-spatial stream individually addressed frame that requires an immediate response and that is addressed to the STA in dynamic SM power save mode. An RTS/CTS sequence may be used for this purpose. The STA shall, subject to its spatial stream capabilities (see 8.4.2.55.4 (Supported MCS Set field) and 8.4.2.157.3 (Supported VHT-MCS and NSS Set field)) and operating mode (see 10.42 (Notification of operating mode changes)), be capable of receiving a PPDU that is sent using more than one spatial stream a SIFS after the end of its response frame transmission. The STA switches to the multiple receive chain mode when it receives the ~~RTS~~frame addressed to it and switches back immediately when the frame exchange sequence ends.

NOTE—A STA in dynamic SM power save mode cannot distinguish between an RTS/CTS sequence that precedes a MIMO transmission and any other RTS/CTS and, therefore, always enables its multiple receive chains when it receives ~~an~~the RTS addressed to it~~self~~.

The STA can determine the end of the frame exchange sequence through any of the following:

— It receives an individually addressed frame addressed to another STA.

— It receives a frame with a TA that differs from the TA of the frame that started the TXOP.

— The CS mechanism (see 9.3.2.1 (CS mechanism)) indicates that the medium is idle at the TxPIFS slot boundary (defined in 9.3.7 (DCF timing relations)).

Delete “sequence” in “if no frame sequence is detected by which the NAV can be set” at 159.30, 201.46.

Delete “sequence” and “correctly” in “until a frame sequence is detected by which it can correctly set its NAV” at 1453.28, 1550.32, 1649.1, 1715.32, 1715.47.

At 992.9 change “The Key RSC denotes the last frame sequence number sent using the GTK” to “The Key RSC denotes the last TSC or PN sent using the GTK”.

At 1984.17 change “Key RSC denotes the last frame sequence number sent using the GTK” to “Key RSC denotes the last TSC or PN sent using the GTK”.

At 1985.5 change “Key RSC = last transmit sequence number for the GTK” to “Key RSC = last TSC or PN for the GTK”.

At 1986.62 change “with the last sequence number used with the GTK (RSC)” to “with the last TSC or PN used with the GTK (RSC)”.

At 1243.8 add “exchange” before “sequence” in “This requires an AP that provides non-QoS CF-polling to adhere to frame sequence restrictions considerably more complex than, and less efficient than, those specified for either PCF or HCF.”

At 1256.63 add “exchange” before “sequence” in “shall be interpreted as successful response, permitting the frame sequence to continue (see Annex G)”.

At 1260.34 add “exchange” before “sequence” (2x) in “shall be interpreted as successful acknowledgment, permitting the frame sequence to continue, or to end without retries, as appropriate for the particular frame sequence in progress”.

At 1383.7 add “exchange” before “sequence” in “all Data frames sent in response to PS-Poll that are not proceeded in the frame sequence by a Data frame with the “more fragments” field equal to1”.

At 2644.17 add “exchange” before “sequence” in “FS frame sequence”. At 2676.8 add “exchange” before “sequence” in “frame sequences supported” and remove the line break after it. At 2676.11 add “exchange” before “sequence” in “Basic frame sequences”. At 2676 add “exchange” before “sequence” in “CF-Frame sequences” and lowercase “frame”.

At 3361.42 replace the space with a hyphen in “frame sequence”.

Proposed resolution:

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

Discussion:

Proposed changes:

Proposed resolution:

Another missing space: “ignorethe”; “AVHT”; “IETFRFC”; “setthe”; “bit1”; “tuplesbetween” (several), “aPHY-CCA.indication”, “TDLS\_UNSPECIFIED\_REASONexcept”, “STAcan”, “STAswitches”.

Font size wacko: 1265.8 “RR5”, 513.53: “6.4.3 Convergence function state list”, 1720.6 “nonprimary”, 564.33 “DMG Beacon” (whole line).

Hyphen should be minus: “EIFS-” on e.g. page 1252

Number and its unit split because not NBSP in 17.3.6.8 (“25 µs”) and 10.1.3.9 (“±40 ppm”) and 2200.56 (“1 Mb/s”).

**References:**

802.11mc/D4.0