IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some comments on 11md/D3.0 (SB1) | | | | |
| Date: 2020-08-xx | | | | |
| 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 various CIDs on 11md/D3.0. 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.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4393  Mark RISON | It doesn't make sense to sometimes plonk "(no data)" after the frame name | Delete "(no data)" throughout except in Table 9-1--Valid type and subtype combinations |

Discussion:

In general, references to Data frames that contain no data are not qualified with “(no data)”. For example there are about 8 instances of “QoS Null (no data)” and over 100 instances of “QoS Null” without “(no data)”.

Proposed resolution:

REVISED

In D3.1:

At 782.10 change:

*QoS (+)Null* frame refers to all three QoS data subtypes with “no data”: the QoS Null (no data) frame, subtype 1100; the QoS CF-Poll (no data) frame, subtype 1110; and the QoS CF-Ack +CF-Poll frame, subtype 1111.

to:

*QoS (+)Null* frame refers to all three QoS data subtypes with an empty frame body: the QoS Null frame, subtype 1100; the QoS CF-Poll frame, subtype 1110; and the QoS CF-Ack +CF-Poll frame, subtype 1111.

Delete “ (no data)” at 785.60, 786.15/18/20, 790.48 (2x), 790.49, 799.43, 850.32 (3x), 850.33 (2x), 1860.24, 3605.32/35/39/47, 3613.23/27/30/41.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4432  Mark RISON  11 | "The Address 1 field of the TIM frame shall be set to the broadcast address." -- equivalent statements are needed for other Management frames that are always broadcast e.g. Beacon, FILS Discovery frames | As it says in the comment |

Discussion:

The following Management frames are already explicitly specified to be transmitted as broadcasts:

The Address 1 field of the **TIM** frame shall be set to the broadcast address.

An AP shall transmit **Measurement Pilots** *[sic]* to the broadcast address.

However, I cannot find anything to say that FILS Discovery frames or Timing Advertisement frames are broadcast, nor indeed that Beacon frames are broadcast!

Additionally, there is nothing about the addressing of (Extended) Channel Switch Announcement frames, but since by definition they are to notify everyone of a change and the MAC SAP does not allow a receiver address to be specified (see 6.3.17.1 MLME-CHANNELSWITCH.request and 6.3.35.2 MLME-EXTCHANNELSWITCH.request) it must be that they are broadcast.

Note: SAKODA Kazuyuki provided the following info on mesh-related frames:

Mesh Action frame is transmitted in broadcast fashion, depending on the element the frame is containing. Some example addressing use are described in 14.10.7 (Addressing of HWMP Mesh Path Selection frame). So we may not need to add anything for this frame though.

[…]

the following action frames are also supposed to be transmitted in broadcast fashion:

* Gate Announcement (stated that “This frame is transmitted using group addresses” in 9.6.16.4)
* Congestion Control Notification (stated that “This frame is transmitted using individual addresses or group addresses” in 9.6.16.5)
* MCCA Setup Request (stated that “This frame is transmitted using individual addresses or group addresses” in 9.6.16.6)
* MCCA Advertisement (stated that “This frame is transmitted using group addresses or individual addresses.” in 9.6.16.9)
* MCCA Teardown (stated that “This frame is transmitted using group addresses or individual addresses.” in 9.6.16.10)

Note: Abhishek PATIL pointed out that 11ax/D6.0 proposes adding the following sentence to 11.46.2.1:

The Address 1 field of the FILS Discovery frame shall be set to the broadcast address.

Note: DMG beacons don’t have an RA, just a BSSID, and S1G beacons don’t have an RA either, just a SA.

Note: various Management frames can be broadcast or unicast depending on the situation (e.g. Announce frames).

Proposed resolution:

REVISED

In D3.1:

At the end of the first para of 11.46.2.1 FILS Discovery frame transmission add “The Address 1 field of the FILS Discovery frame shall be set to the broadcast address.”.

At the end of the second para (“In a non-DMG and non-S1G BSS, …”) of 11.1.3.1 General (in 11.1.3 Maintaining synchronization) add “The Address 1 field of the Beacon or Timing Advertisement frame shall be set to the broadcast address.”.

At the end of the third para (“In a DMG infrastructure BSS, ...”) of 11.1.3.1 General (in 11.1.3 Maintaining synchronization) add “The Address 1 field of the Timing Advertisement frame shall be set to the broadcast address.”.

At the end of second para of 14.13.3.1 Beacon generation in MBSSs add “The Address 1 field of the Beacon frame shall be set to the broadcast address.”.

At the end of 11.8.8.1 General (in 11.8.8 Selecting and advertising a new channel) add a para “The Address 1 field of a Channel Switch Announcement frame shall be set to the broadcast address.”

At the end of 11.9.1 General (in 11.9 Extended channel switching (ECS)) add a para “The Address 1 field of an Extended Channel Switch Announcement frame shall be set to the broadcast address.”

At 2302.47 and 2302.49 change “multiple Beacons, Measurement Pilots, or Probe Response frames” to “multiple Beacon, Measurement Pilot, or Probe Response frames”.

At 2318.56, 2320.52/53(2x)/60/61/63, 2321.1/3/5/13/19/43 change “Measurement Pilots” to “Measurement Pilot frames”. At 327.16 change “measurement pilots” to “Measurement Pilot frames”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4451  Mark RISON  10.23.2.7  1834.13 | "When an AP supports DL-MU-MIMO, frames from a higher or lower priority AC may be included  in a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 when  these frames do not increase the duration of the VHT or S1G MU PPDU beyond that required for the  transmissions of the frames of the primary AC(#2426)." -- why the not increase duration constraint, given that the previous bullet does allow extension? Maybe special-case for TXOP Limit 0, i.e. only in that case do not extend (since otherwise TXOP Limit is the limit, irrespective of content)? | Change to "When an AP supports DL-MU-MIMO, frames from a higher or lower priority AC may be included  in a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 when  the TXOP limit for the primary AC is nonzero." |
| CID 4557  Mark RISON  10.23.2.7  1834.11 | "When an AP supports DL-MU-MIMO, frames from a higher or lower priority AC may be included  in a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 when  these frames do not increase the duration of the VHT or S1G MU PPDU beyond that required for the  transmissions of the frames of the primary AC" conflicts with "Frames from a higher priority AC may be included when at least one frame from the primary AC has been transmitted and all frames from the primary AC have been transmitted": can I transmit higher priority AC frames even if the PPDU is thereby made longer? | As it says in the comment |

Discussion:

The current wording is:

**10.23.2.7 Sharing an EDCA TXOP**

(#1195)The AC associated with the EDCAF that gains an EDCA TXOP is referred to as the primary AC. Frames from ACs other than the primary AC shall not be included in the TXOP, with the following exceptions (TXOP sharing):

— Frames from a higher priority AC may be included when at least one frame from the primary AC has been transmitted and all frames from the primary AC have been transmitted.

— When an AP supports DL-MU-MIMO, frames from a higher or lower priority AC may be included in a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 when these frames do not increase the duration of the VHT or S1G MU PPDU beyond that required for the transmissions of the frames of the primary AC(#2426). Frames from the primary AC shall be transmitted first.

The first bullet allows higher-priority frames to be included in the TXOP, even if this causes the TXOP to be lengthened, as long as the primary AC frames have gone out (and implicitly as long as the TXOP limit is not violated).

However, the second bullet disallows (or can be read as disallowing) higher-priority frames from being included in the MU PPDU if that would lengthen the MU PPDU. It should be made clearer that this is not the case, i.e. just as for the first bullet, higher-priority frames can be included even if they lengthen the MU PPDU (and possibly also the TXOP), subject to the overall restrictions.

Also, the final sentence of the second bullet is not clear. There might not be frames for the primary AC for all users, and higher-priority stuff should go ahead of lower-priority stuff, since lower-priority stuff should only be allowed if it’s getting a completely free ride that would go unused otherwise.

Examples with the EDCAF that wins contention being VI, with a non-zero TXOP limit, and the TXOP not exceeding that limit:

* Sending some SU PPDUs with VI traffic (none left to tx) and then some SU PPDUs with VO traffic: OK
* Sending some SU PPDUs with VI traffic (none left to tx) and then some SU PPDUs with BE traffic: not OK
* Sending some MU PPDUs with one user having just VI traffic (no extraneous padding) and another user having just BE traffic (no VI/VO traffic to send): OK
* Sending some MU PPDUs with one user having just VI traffic but extraneous padding so that another user can have extra BE traffic: not OK
* Sending some MU PPDUs with one user having just VI traffic (none left to tx; no extraneous padding) and then that user having just VO traffic (no extraneous padding), and another using having just BE traffic throughout (no VI/VO traffic to send): OK
* Sending some MU PPDUs with one user having just VI traffic (none left to tx; no extraneous padding) and then that user having just VO traffic (none left to tx; no extraneous padding) and then that using having BE traffic, and another using having just BE traffic throughout (no VI/VO traffic to send): not OK
* Sending some MU PPDUs with one user having just VO traffic and then that user having VI traffic: not OK

There is no need to explicitly discuss the case where the TXOP limit is 0, since per 10.23.2.9 TXOP limits this means a single A-MPDU to each user, so the case is covered.

Proposed changes:

Change 10.3.2.7 as follows:

**10.23.2.7 Sharing an EDCA TXOP**

(#1195)The AC associated with the EDCAF that gains an EDCA TXOP is referred to as the primary AC. Frames from ACs other than the primary AC shall not be included in the TXOP, with the following exceptions (TXOP sharing):

— Frames from a higher priority AC may be included when at least one frame from the primary AC has been transmitted and all frames from the primary AC have been transmitted.

NOTE—The frames from a higher priority AC might be included in successive PPDUs in the TXOP and/or in one or more MU PPDUs.

— When an AP supports DL-MU-MIMO, frames from a ~~higher or~~ lower priority AC may be included in an ~~VHT or S1G~~ MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 when these frames do not increase the duration of the ~~VHT or S1G~~ MU PPDU beyond that required for the transmissions of the frames of the primary AC(#2426) and any frames from a higher priority AC. For a given user, any frames from the primary AC shall be transmitted first and then any frames from a higher priority AC immediately next.

The EDCAF remains bound by the TXOP limit for its AC (i.e. the primary AC), irrespective of the AC(s) of the frames transmitted during the TXOP.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4451 and CID 4557 in <this document>, which address the issues raised by the commenter in the direction suggested.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4433  Mark RISON  10.27.3.1  1902.28 | Table 10-22--Applicable HT protection mechanisms only goes up to 40 MHz non-HT dup. However, it also applies to VHT through 10.27.5 Protection rules for VHT STAs ("A VHT STA is subject to all of the rules for HT STAs that apply to its operating band, except that a PPDU  with the TXECTOR FORMAT parameter set to VHT may be substituted for a PPDU with the TXVECTOR  FORMAT parameter set to HT\_MF."). Therefore it should also cover the use of 80/80+80/160 non-HT dup for RTS" | In Table 10-22 change "40 MHz transmissions use non-HT duplicate frames defined in Clause 19 (High-throughput (HT) PHY  specification)" to "40 MHz, 80 MHz, 160 MHz and 80+80 MHz transmissions use non-HT duplicate frames defined in Clause 19 (High-throughput (HT) PHY  specification) and Clause 21" |

Discussion:

10.27.5 says:

**10.27.5 Protection rules for VHT STAs**

A VHT STA is subject to all of the rules for HT STAs that apply to its operating band, except that a PPDU with the (#4228)TXVECTOR FORMAT parameter set to VHT may be substituted for a PPDU with the TXVECTOR FORMAT parameter set to HT\_MF.

So this means Table 10-22 in 10.27.3 Protection mechanisms for transmissions of HT PPDUs applies to VHT STAs too. This says:

**Table 10-22—Applicable HT protection mechanisms(#67)**

|  |
| --- |
| **HT protection mechanism** |
| Control frames such as RTS/CTS or CTS-to-self prior to the HT transmissions:  — 20 MHz transmissions use the rates defined in Clause 17 (Orthogonal frequency division multiplexing (OFDM) PHY specification) or Clause 18 (Extended Rate PHY (ERP) specification)  — 40 MHz transmissions use non-HT duplicate frames defined in Clause 19 (High-throughput (HT) PHY specification) |
| As the first PPDU in the TXOP, send one of:  — a non-HT PPDU containing a frame that requires an immediate response  — (#4434)an HT-mixed format PPDU containing a frame that requires an immediate response in a non-HT PPDU  PPDUs after the first PPDU exchange may be HT-greenfield format PPDUs and/or be separated by RIFS. |

As the comment says, protection of 80+ MHz transmissions should also be covered for VHT.

TGm prefers, however, not to make changes to Table 10-22 since it sees that table as being for HT STAs.

Proposed resolution:

REVISED

At the end of the sentence in 10.27.5 Protection rules for VHT STAs add “ and that the applicable HT protection mechanisms are extended to include 80, 160 and 80+80 MHz transmissions using non-HT duplicate frames defined in Clause 21” (1906.11 in D3.0).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4582  Mark RISON | The definition of dot11EDCATableMSDULifetime (and QAP version) needs to allow for A-MSDUs and MMPDUs, since those are/can be sent under a particular AC. Also similarly change 1763.63 in 10.3.4.4 and dot11MaxTransmitMSDU Lifetime in C.3 | As it says in the comment |

Discussion:

dot11EDCATableMSDULifetime’s definition says that it “specifies the maximum duration an MSDU, for a given AC, would be retained by the MAC before it is discarded.”

So which attribute specifies the lifetime for MMPDUs? It must be this one too, since there’s no other one for this.

However, we don’t need to explicitly allow for A-MSDUs, since MSDUs are a component of A-MSDUs (see also e.g. D3.1/1843.43).

1763.63 is:

Retries for failed transmission attempts shall continue until the SRC for the MPDU with the Type subfield

equal to Data or Management is equal to dot11ShortRetryLimit or until the LRC for the MPDU with the Type subfield equal to Data or Management is equal to dot11LongRetryLimit. When either of these limits is reached, retry attempts shall cease, and the MPDU with the Type subfield Data (and any MSDU of which it is a part) or Management shall be discarded. A DMG STA, in addition to using random access within a CBAP, may transmit retries in available scheduled SPs.

so it’s not entirely clear what the commenter is on about here (is this a similar point to CID 4168?).

The range of the EDCA MSDU lifetimes seems odd, too. It allows 0, i.e. the MSDUs are stillborn, and it only allows up to 500 TUs. It should be the same as the range for DCF MSDU lifetimes, which goes from 1 TU to 232‑1 TUs (for the *really* determined).

Proposed changes:

Change D3.1 as follows:

**10.4 MSDU and MMPDU fragmentation**

The source STA shall maintain a transmit MSDU/MMPDU timer for each MSDU/MMPDU being transmitted. The attribute dot11MaxTransmitMSDULifetime specifies the maximum amount of time allowed to transmit an MSDU/MMPDU. The timer starts on the initial attempt to transmit the (#1452)MSDU/MMPDU, or first fragment of the MSDU/MMPDU (#1452)if the MSDU/MMPDU is fragmented. If the timer exceeds dot11MaxTransmitMSDULifetime, then (#1452)any remaining fragments are discarded by the source STA and no attempt is made to complete transmission of the MSDU/MMPDU.

**10.7 MSDU transmission restrictions**

(#66)A STA should select a value of dot11MaxTransmitMSDULifetime that is sufficiently large that the STA does not discard MSDUs or MMPDUs~~A-MSDUs~~ due to the transmit MSDU/MMPDU timer being exceeded, ~~excessive Transmit MSDU timeouts~~ under normal operating conditions.

**10.23.2.12 Retransmit procedures**

**10.23.2.12.1 General**

(#2432)A QoS STA shall maintain a transmit MSDU/MMPDU timer for each MSDU passed to the MAC and for each MMPDU. dot11EDCATableMSDULifetime specifies the maximum amount of time allowed to transmit an MSDU/MMPDU for a given AC. The transmit MSDU/MMPDU timer shall be started when the MSDU/MMPDU is passed to the MAC.

(#2432)When A-MSDU aggregation is used, the HT STA maintains a single timer for the whole A-MSDU. The timer is restarted each time an MSDU is added to the A-MSDU. The result of this procedure is that no MSDU in the A-MSDU is discarded before a period of dot11EDCATableMSDULifetime has elapsed.

(#2664)(#1505)Retries for failed transmission attempts shall continue until one or more of the following conditions occur:

— (#2664)The frame retry count for the MSDU, A-MSDU, or MMPDU is equal to dot11ShortRetryLimit.

— (#2664)The drop-eligible frame retry count for the MSDU, A-MSDU, or MMPDU is equal to dot11ShortDEIRetryLimit.

— (#2664)The unsolicited frame retry count for the A-MSDU is equal to dot11UnsolicitedRetryLimit.

— (#2432)The transmit MSDU/MMPDU timer for the MSDU/MMPDU or any undelivered fragments of that MSDU/MMPDU exceeds dot11EDCATableMSDULifetime.

**C.3 MIB detail**

dot11MaxTransmitMSDULifetime OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

UNITS "TUs"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

~~The MaxTransmitMSDULifetime is~~This attribute specifies the elapsed time, after the initial transmission of an MSDU/MMPDU (or the first fragment thereof), after which further attempts to transmit the MSDU/MMPDU are terminated."

DEFVAL { 512 }

::= { dot11OperationEntry 6 }

dot11EDCATableMSDULifetime OBJECT-TYPE

SYNTAX Unsigned32 (~~0..500~~1..4294967295)

UNITS "TUs"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

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

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum duration an MSDU/MMPDU, for a given AC, would be retained by the MAC at the non-AP STA before it is discarded."

DEFVAL { 500 }

::= { dot11EDCAEntry 6 }

dot11QAPEDCATableMSDULifetime OBJECT-TYPE

SYNTAX Unsigned32 (~~0..500~~1..4294967295)

UNITS "TUs"

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute specifies the maximum duration an MSDU/MMPDU, for a given AC, would be retained by the MAC at the AP before it is discarded."

DEFVAL { 500 }

::= { dot11QAPEDCAEntry 6 }

Proposed resolution:

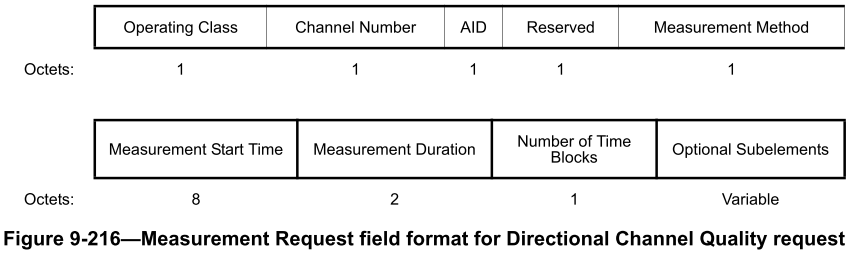
REVISED

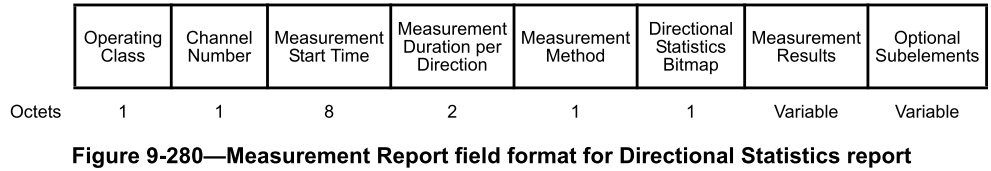
Make the changes shown under “Proposed changes” for CID 4582 in <this document>, which address the issue raised by the commenter (except for the one at 1763.63 -- see CID 4168).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4284  Mark RISON  9.4.2.20.18  1043.59 | Should Figure 9-219--Measurement Request field format for Directional Statistics request not allow for optional subelements, like the corresponding report, and like most requests? Ditto Directional Measurement request | As it says in the comment |

Discussion:

Most requests/reports allow for optional subelements, if only to allow for vendor-specific subelements. E.g.:





However, for some reason, Directional Statistics requests and Directional Measurement requests don’t allow for optional subelements. There is no reason for this limitation.

Proposed changes:

In Figure 9-218—Measurement Request field format for Directional Measurement request and Figure 9-219—Measurement Request field format for Directional Statistics request add a field at the end “Optional Subelements” with “Variable” as the number of octets.

At the end of 9.4.2.20.17 Directional Measurement request insert:

The Optional Subelements field contains zero or more subelements. The subelement format and ordering of subelements are defined in 9.4.3.

The Subelement ID field values for the defined subelements are shown in Table 9-xx.

Immediately after, insert a Table 9-xx with caption “Optional subelement IDs for Directional Measurement request” and contents the same as Table 9-177—Optional subelement IDs for Measurement Pilot Transmission.

Immediately after, insert:

The Vendor Specific subelements have the same format as their corresponding elements (see 9.4.2.25). Zero or more Vendor Specific subelements are included in the list of optional subelements.

At the end of 9.4.2.20.18 Directional Statistics request insert:

The Optional Subelements field contains zero or more subelements. The subelement format and ordering of subelements are defined in 9.4.3.

The Subelement ID field values for the defined subelements are shown in Table 9-yy.

Immediately after, insert a Table 9-yy with caption “Optional subelement IDs for Directional Statistics request” and contents the same as Table 9-177—Optional subelement IDs for Measurement Pilot Transmission.

Immediately after, insert:

The Vendor Specific subelements have the same format as their corresponding elements (see 9.4.2.25). Zero or more Vendor Specific subelements are included in the list of optional subelements.

Remember to hyperlinkify all the xrefs!

Proposed resolution:

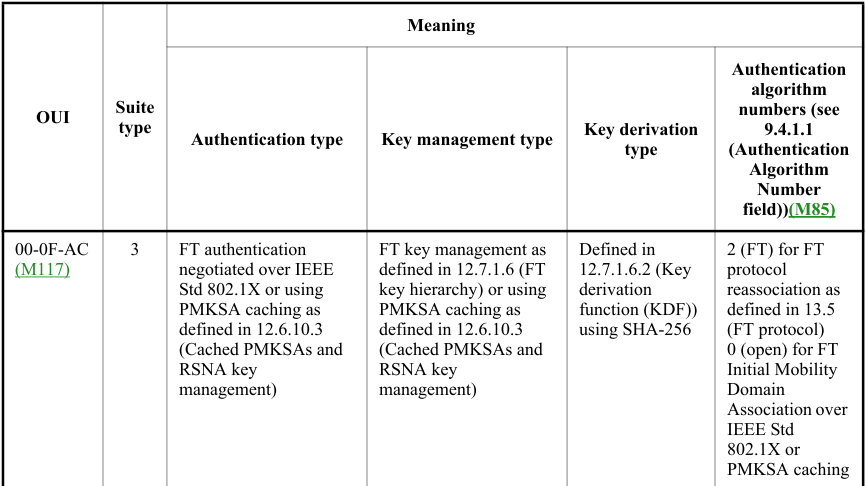
REVISED

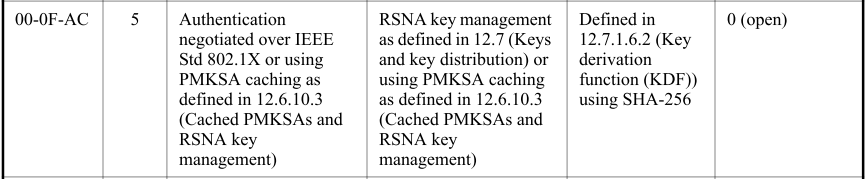
Make the changes shown under “Proposed changes” for CID 4284 in <this document>, which allow for optional subelements in the requests identified by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4205  Mark RISON  9.4.2.24.3  1101.29 | Table 9-151--AKM suite selectors has overlapping conditions. For example, 00-0F-AC:3 and 00-0F-AC:5 have the same key derivation, can both use 0 for the auth alg num, have subset key management type (since 12.7.1.6 is a subclause of 12.7) and have subset authentication (since FT authentication  negotiated over IEEE  Std 802.1X is a type of Authentication  negotiated over IEEE  Std 802.1X). Similarly :8 and :9, etc. | Make sure each suite selector has no overlap with other suite selectors |
| CID 4206  Mark RISON  9.4.2.24.3  1101.29 | Table 9-151--AKM suite selectors has overlapping conditions. For example, 00-0F-AC:3 and 00-0F-AC:5 have the same key derivation, can both use 0 for the auth alg num, have subset key management type (since 12.7.1.6 is a subclause of 12.7) and have subset authentication (since FT authentication  negotiated over IEEE  Std 802.1X is a type of Authentication  negotiated over IEEE  Std 802.1X). Similarly :8 and :9, etc. | In the auth type for :5 change "Authentication  negotiated over IEEE  Std 802.1X " to "Non-FT authentication  negotiated over IEEE  Std 802.1X " |

Discussion:

Here are the conditions for 00-0F-AC:3 and :5:





So, when the auth alg num is 0, what distinguishes :3 and :5? How does the receiver know which is intended?

* “FT authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3”

is a subset of

“Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3”

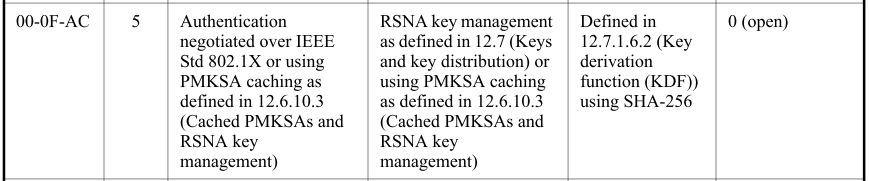
* “FT key management as defined in 12.7.1.6 or using PMKSA caching as defined in 12.6.10.3”

is a subset of

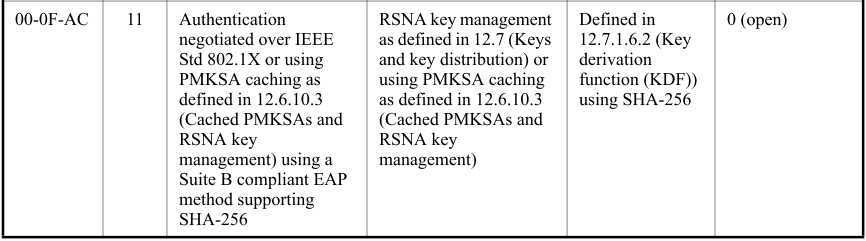
“RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3”

* The key derivation type is the same (“Defined in 12.7.1.6.2 using SHA-256”)

Similarly, the only difference between



and



is that :11 guarantees that it's Suite B compliant (extra text at end of third cell). However, even that extra text has vanished in D3.4, apparently as a result of the resolution to CID 4204.

Jouni MALINEN has commented as follows:

I don't see need to add "using 802.1X" or "using PSK" to the FT key mgmt column. That difference between EAP/PSK(and /SAE) is important for the authentication part for FT, but less so for key management as far as 12.7.1.6 (FT key hierarchy) is concerned. That "using PSK" in references to 12.7 is somewhat more applicable, but I would not have much against deleting that from the key management column for :2, :6, and :20 if there is desire to make this more consistent (i.e., leave 802.1X(=EAP in this context)/PSK/SAE in for auth, but remove from key mgmt).

00-0F-AC:11 is indeed the "Suite-B 128-bit" AKM and the extra constraint it has as compared to 00-0F-AC:5 is described in REVmd/D3.4 page 1107 line 19. That said, I do not think there would be any real deployments using 00-0F-AC:11 due to the changes in Suite B (now CNSA Suite) requirements (i.e., only the 192-bit variant 00-0F-AC:12 would be used).

I don't like the direction of starting to add "non-FT" or "non-FILS" for cases that do not use FT/FILS. I think "PSK" is clear enough as-is when comparing to "FT using PSK". I don't think I would come to the same conclusion on the "FT X" is a subset of "X" parts or the need to distinguish that any further in Clause 9.

and subsequently:

Yes, [a note] about additional out-of-scope restriction might be the best approach (i.e., the restrictions in P802.11 for cipher suite selection and these out-of-scope for P802.11 restriction on other things).

"Non-FT" for :5 is technically correct. Though, I still don't like the direction of adding non-FT/non-FILS/non-something-else to this type of things, i.e., I'd rather leave the current text as-is.

Proposed resolution:

REVISED

In D3.4:

In Table 9-153—AKM suite selectors delete “using PSK” in the Key management type cell for the :2, :6 and :20 rows.

In Table 9-153—AKM suite selectors, for the :11, :12 and :13 rows, at the bottom of the four rightmost cells, create a new merged cell with contents “NOTE—Restrictions apply on the use of this AKM suite selector that are outside the scope of this standard.”

In Table 9-153—AKM suite selectors, in the Authentication type column:

* for the :5 row change “Authentication” to “Non-FT authentication”
* for the :6 row prepend “Non-FT authentication using”
* for the :8 row prepend “Non-FT”
* for the :20 row prepend “Non-FT authentication using”

Alternative proposed resolution:

REVISED

In D3.4:

In Table 9-153—AKM suite selectors delete “using PSK” in the Key management type cell for the :2, :6 and :20 rows.

In Table 9-153—AKM suite selectors, for the :11, :12 and :13 rows, at the bottom of the four rightmost cells, create a new merged cell with contents “NOTE—Restrictions apply on the use of this AKM suite selector that are outside the scope of this standard.”

Note to the commenter: expressions such as "FT authentication" in the Authentication type column are an implicit reference to a particular and distinct key hierarchy, which allows AKM suite selectors to be distinguished.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4499  Mark RISON | If the term "slave" is no longer acceptable (CID 2020), is the term "master" still acceptable (other than "master key" contexts)? There are only a few such instances | As it says in the comment |

Discussion:

If “slave” is objectionable, then so is “master”, in those contexts that imply the existence of a “slave”.

“master white space device” and “Master STA TVWS operation” are used in regulations, however, so cannot be changed.

Proposed resolution:

REVISED

In 9.5.6 Beamformed Link Maintenance field inc. Figure 9-852—Beamformed Link Maintenance field format and Table 9-344—The Beamformed Link Maintenance negotiation, change “isMaster” to “isController” (5x). In 9.5.6 Beamformed Link Maintenance field change “master of the data transfer” to “controller of the data transfer”.

In 11.1.2.1 TSF for an infrastructure BSS or a PBSS change “timing master” to “timing source”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4715  Mark RISON  6.3.68  576.10 | MLME-FINETIMINGMSMTRQ primitives are not used anywhere | In Figure 6-17---Fine timing measurement primitives and timestamps capture add at the top a MLME-FINETIMINGMSMT.request from STA B's SME to STA B's MLME, a Fine Timing Measurement Request frame from STA B's MLME to STA A's MLME and a MLME-FINETIMINGMSMT.request from STA A's MLME to STA A's SME |
| CID 4716  Mark RISON  6.3.68  576.10 | MLME-FINETIMINGMSMTRQ primitives are not used anywhere | Delete 6.3.68 |

Discussion:

6.3.56 has information on the MLME-FINETIMINGMSMT primitives, including a figure showing how the primitives map to frames over the air. However, 6.3.68 has no similar information on the MLME-FINETIMINGMSMTRQ primitives.

Mark HAMILTON further points out:

Perhaps, if we are going to show the “RQ” primitives in the figure(s) (that is, Figure 6-17, and maybe as suggested in Figure 6-16 also), then we should merge those primitives into the subclause also.  That is, merge subclause 6.3.68 into 6.3.56 (and maybe 6.3.67 into 6.3.55)?

Those later clauses have the primitive definitions for MLME-[FINE]TIMINGMSMTRQ, .request and .indication.  In the current subclause with Figure 6-17, there are only the primitives for the FTM frames themselves.  But, the clause states this, w.r.t. Figure 6-17:

The following set of primitives supports exchange of FTM information from one SME to another.

(M138)The diagram in Figure 6-17 (Fine timing measurement primitives and timestamps capture) shows

various points in time that are of interest to the FTM procedure.

Given the combination of both sets of actions in the Figure, I think having both sets of primitives in the subclause makes sense.  Right now, the subclauses are very far apart, and there is no cross-reference hint to go look at the other one, to understand the whole picture that Figure 6-17 is trying to convey.

Proposed changes:

Change the first para of 6.3.56.1 General as follows:

The following set of primitives supports triggering an FTM(#1022) procedure or stopping an ongoing FTM procedure, and exchange of FTM information from one SME to another. (M138)~~The diagram in~~ Figure 6-17 (Fine timing measurement primitives and timestamps capture) shows the use of these primitives and various points in time that are of interest to the FTM procedure.

Change Figure 6-17 as follows, adding the material in red:



Insert 6.3.68.2 MLME-FINETIMINGMSMTRQ.request and 6.3.68.3 MLME-FINETIMINGMSMTRQ.indication after 6.3.56.1, renumbering them to 6.3.56.2 and 6.3.56.3 respectively, and renumbering the current 6.3.56.2 and 6.3.56.3 to 6.3.56.4 and 6.3.56.5 respectively. Delete 6.3.68 Fine timing measurement request and 6.3.68.1 General.

Change the first para of 6.3.55.1 General as follows:

The following set of primitives supports triggering a Timing Measurement procedure or stopping an

ongoing Timing Measurement procedure, and exchange of timing measurement information from one SME to another. (M138)The diagram in Figure 6-16 (Timing measurement primitives and timestamps

capture(#1563)) shows various points in time that are of interest to the timing measurement procedure.

Change Figure 6-16 by adding the material shown in red above, but with “FINE” and “Fine ” deleted.

Insert 6.3.67.2 MLME-TIMINGMSMTRQ.request and 6.3.67.3 MLME-TIMINGMSMTRQ.indication after 6.3.55.1, renumbering them to 6.3.55.2 and 6.3.55.3 respectively, and renumbering the current 6.3.55.2 and 6.3.55.3 to 6.3.55.4 and 6.3.55.5 respectively. Delete 6.3.67 Timing measurement request and 6.3.67.1 General.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CIDs 4715 and 4716 in <this document>, which clarify the use of MLME-FINETIMINGMSMTRQ primitives and also MLME-TIMINGMSMTRQ primitives.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4591  Mark RISON | The way UTF-8 strings are referred to is inconsistent. We have a definition of UTF-8 string (in 9.2.2) so just use that | In 9.4.2.2 change “the SSID is interpreted using UTF-8 encoding” to “the SSID is a UTF-8 string”. In 9.4.2.21.14 change “The Public Identifier URI/FQDN field contains a URI encoded using UTF-8 and formatted in accordance  with IETF RFC 3986” to “The Public Identifier URI/FQDN field contains a URI as a UTF-8 string, formatted in accordance  with IETF RFC 3986,”. In 9.4.2.26 change “The SSID in this BSS is interpreted using UTF-8 encoding” to “The SSID in this BSS is a UTF-8 string”. At 1217.8 change “an UTF” to “a UTF”. In 9.4.5.4 and 9.4.5.5 change “UTF-8 encoded field” to “UTF-8 string”. In 9.4.5.10 change “a UTF-8 encoded character string” to “a UTF-8 string” and “in UTF-8 format” to “in UTF-8”. In 9.4.5.17 change “field encoded using UTF-8 and “ to “UTF-8 string,”. In 9.4.5.21 change “UTF-8 formatted field “ to “UTF-8 string “. In 9.4.5.22 change “a UTF-8 formatted string” to “a UTF-8 string” |

Discussion:

The definition in 9.2.2 (which covers the conventions for structures defined in the MAC sublayer) defines a UTF‑8 string as follows:

A[…] UTF-8 string is a sequence of […] UTF-8 encoded code points […] without a terminating null.

[For those who are not character representation geeks: a code point is a number that represents (in general) a character in a character set, and an encoding is a mechanism for representing a code point as one or more numbers (see e.g. <https://unicode.org/glossary/> ). For example, the (non-Greek) micro character µ is Unicode code point U+00B5 and is encoded in UTF-8 (Unicode/UCS transformation format 8) as the octet sequence 0xC2 0xB5. For characters in ASCII, the UTF-8 encoding is the same as the ASCII encoding.]

An important point of the above definition is that it states that for the purposes of the MAC sublayer a UTF-8 string does not have a terminator. That is, the UTF-8 string “Password” is represented as “Password” (8 octets), not “Password\0” (9 octets, where \0 is the null character) -- this is obviously important where the string is being tested for equality or hashed.

Proposed changes:

Move the following sentence from 9.2.2 Conventions to the end of 1.4 Word usage:

An ASCII or UTF-8 string is a sequence of ASCII or UTF-8 encoded code points, respectively, without a

terminating null.

and replace it in 9.2.2 with the following sentence (remember to hyperlinkify the xref!):

ASCII and UTF-8 strings are defined in 1.4.

Change 12.1 Conventions as follows (remember to hyperlinkify the xref!):

ASCII and UTF-8 strings are defined in ~~9.2.2 (Conventions)~~1.4.

Change 9.4.2.2 SSID element as follows:

When the UTF-8 SSID subfield of the Extended Capabilities element is equal to 1 in the frame that includes the SSID element, or the Extended Capabilities of the source of the SSID information is known to include the UTF-8 SSID capability based on a previously received Extended Capabilities element, the SSID is ~~interpreted using UTF-8 encoding~~a sequence of UTF-8 encoded code points. Otherwise, the character encoding of the octets in this SSID element is unspecified.

NOTE—If the SSID is a sequence of UTF-8 encoded code points, a terminating null might or might not be present.

Change 9.4.2.21.14 Location Identifier report as follows:

The Public Identifier URI/FQDN field contains a URI ~~encoded using UTF-8 and~~as a UTF-8 string, formatted in accordance with IETF RFC 3986, that points to a location object or an FQDN that identifies a location server.

Change Table 9-153—Extended Capabilities field as follows:

The SSID in this BSS is ~~interpreted using UTF-8 encoding~~a sequence of UTF-8 encoded code points

Change 9.4.2.68.5 Diagnostic subelement descriptions as follows:

The Certificate ID field contains a~~n~~ UTF-8 string indicating an identifier assigned to the STA in a manner

outside the scope of the standard. The Certificate ID typically takes the form of “WFA3991” and might be

used by a receiving STA to look up the certificate assigned to that ID.

Change 9.4.5.4 Venue Name ANQP-element as follows:

The Venue Name field is a ~~variable length(#183)~~ UTF-8 ~~encoded field~~string containing the venue’s name.

Change 9.4.5.5 Emergency Call Number ANQP-element as follows:

The Emergency Call Number field is a ~~variable length(#183)~~ UTF-8 ~~encoded field~~string containing information, used to reach emergency services, from the network (e.g., dialed digits, emergency service URN label [B40]).

Change 9.4.5.10 NAI Realm ANQP-element as follows:

The NAI Realm Encoding Type subfield(M101) is a 1-bit subfield. It is set to 0 to indicate that the NAI Realm in the NAI Realm subfield is formatted in accordance with IETF RFC 4282. It is set to 1 to indicate it is a UTF-8 ~~encoded character~~ string that is not formatted in accordance with IETF RFC 4282.

If there is more than one NAI Realm in this subfield, the NAI Realms are delimited by a semicolon character (i.e., “;”, which is encoded in UTF-8 ~~format~~ as 0x3B).

Change 9.4.5.17 Emergency NAI ANQP-element as follows:

The Emergency NAI Information field is a ~~variable length(#183)~~ ~~field encoded using~~ UTF-8 string ~~and~~ formatted in accordance with IETF RFC 4282.

Change 9.4.5.21 Advice of Charge ANQP-element as follows:

The Plan Information field is a ~~variable length~~ UTF-8 ~~formatted field~~string that carries an XML description of an Advice of Charge plan.

Change 9.4.5.22 Local Content ANQP-element as follows:

(#2203)The Label field is a ~~variable length(#183)~~ ~~field~~UTF-8 string containing a text description of the URL. It provides the type and potential usage of the URL. ~~This is a UTF-8 formatted string.~~

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4591 in <this document>, which canonicalise references to UTF-8 strings or encoded code point sequences.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4679  Mark RISON  9.3.3.1  854.23 | "a) The Address 1 field of the Management frame is the RA (=DA) and is determined as the destination  of the frame.  b) The Address 2 field of the Management frame is the TA (=SA) and is determined as the address of  the STA transmitting the frame(#2013)." arguably duplicates 9.2.4.3.1 | As it says in the comment |

Discussion:

The description in 9.2.4.3.1 is:

Certain address field usage is specified by the relative position of the address field (1–4) within the MAC header, independent of the type of address present in that field. For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.

However, the examples duplicate more specific information, e.g. in 9.3.3.1 for Management frames:

A STA uses the contents of the Address 1 field to perform the address matching for receive decisions.

The address fields for all Management frames except Multihop Action frames are as follows:

a) The Address 1 field of the Management frame is the RA (=DA) and is determined as the destination of the frame.

b) The Address 2 field of the Management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame(#2013).

and in 9.3.2.1.2 for Data frames:

The content of the address fields of Data frames are dependent upon the values of the To DS and From DS subfields in the Frame Control field and whether the Frame Body field contains either an MSDU (or fragment thereof) or an entire A-MSDU, as determined by the A-MSDU Present subfield of the QoS Control field (see 9.2.4.5.9 (A-MSDU Present subfield)). The content of the address fields transmitted by nonmesh STAs is defined in Table 9-32 (Address field contents). The content of the address fields transmitted by mesh STAs is defined in 9.3.5 (Frame addressing in an MBSS), and the content of the fields transmitted by GLK STAs is defined in 10.65 (Addressing of GLK Data frame(M101) transmission(11ak)).(11ak) Where the content of a field is shown as not applicable (N/A), the field is omitted. Note that Address 1 always holds the receiver address of the intended receiver (or, in the case of group addressed frames, receivers), and that Address 2 always holds the address of the STA that is transmitting the frame.

and in 9.3.1.x for Control frames, e.g. in 9.3.1.2 for RTS:

(MDR2)The RA field of the RTS frame is the address of the STA, on the WM, that is the intended immediate recipient of the pending individually addressed Data, Management, or Control frame.

(MDR2)The TA field is the address of the STA transmitting the RTS frame or the bandwidth signaling TA of the STA transmitting the RTS frame.

Also, it is not the case that “the receiver address of […] Ack frames is always obtained from the Address 2 field in the corresponding […] frame being acknowledged”, because per 9.3.1.4:

The RA field of the Ack frame is the nonbandwidth signaling TA from the Address 2 field of the immediately previous individually addressed Data, Management, BlockAckReq, BlockAck, or PS-Poll frames.

so the RA of the Ack might not be the same as the A2 (TA) of the preceding frame. Though I suppose “obtained from” could be argued to be different from “copied from”.

It is possible to argue that 9.2.4.3.1’s ad libbing is helpful to set out general principles, however.

Proposed changes:

Proposed resolution:

REVISED

Alternative 1:

Delete “For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.” in 9.2.4.3.1.

Alternative 2:

After “For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.” in 9.2.4.3.1 add:

NOTE—The receiver address of Ack frames does not equal the Address 2 field of the frame being acknowledged, if that field was a bandwidth signalling TA.

Alternative 3:

Change “For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.” in 9.2.4.3.1 to “Specifically, the Address 1 field in received frames always identifies the receiver(s) of the frame, and the Address 2 field in received frames, where present, always identifies the transmitter of the frame.”

Make the changes shown under “Proposed changes” for CID in <this document>, which

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4689  Mark RISON  9.4.3 | "The optional  subelements are ordered by nondecreasing subelement ID." (2x) -- they're ordered per 9.4.3 ("Subelements within an element are ordered by nondecreasing Subelement ID.") | Change to refer to 9.4.3 as for most optional subelement lists |

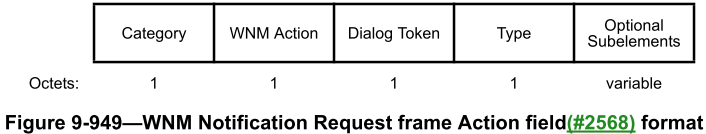
Discussion:

It has been pointed out that

In 9.4.3, subelements are within an element. In 9.6.7.37 and 9.6.7.38, subelements are within a field. Therefore, cannot change to refer to 9.4.3 in 9.6.7.37 and 9.6.7.38.

This is valid of itself, although pedantically in lots of places (if not most/all) subelements are within a field, though sometimes this is itself within an element.

Conversely, Figure 9-865—Measurement Pilot frame Action field format has an Optional Subelements field, is not in an element, and yet says "The Optional Subelements field contains zero or more subelements. The subelement format and ordering of subelements are defined in 9.4.3 (Subelements)." Ditto Figure 9-949—WNM Notification Request frame Action field(#2568) format:



Proposed resolution:

REVISED

In 9.4.3 change “Subelements within an element are ordered by nondecreasing Subelement ID.” (1465.1 in D3.0) to “Subelements within an element and subelements in a field outside of an element are in each case ordered by nondecreasing Subelement ID.”

In 9.6.7.37 and in 9.6.7.38 change “The Optional Subelements field contains zero or more subelements, each consisting of a 1-octet Subelement ID field, a 1-octet Length field, and a variable-length Data field, as defined in 9.4.3 (Subelements). The optional subelements are ordered by nondecreasing subelement ID.” (1566.1 and 1567.36 in D3.0) to “The Optional Subelements field contains zero or more subelements, The subelement format and ordering of subelements are defined in 9.4.3 (Subelements).”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4809  Mark HAMILTON  9.6.12.3  1589.40 | Change 6 occurrences of "in response to a received", to be simpler and match the majority language in the draft. | Delete "received" (and change "a" to "an" as appropriate) at P1589L40, P1590L53, P1592L56, P2180L1, P2482L30, and P2482L39. |

Discussion:

This was ACCEPTED in motion 167. However, there are ~20 “in response to the rec\* of \*” which by the same token should be just “in response to \*”.

Proposed additional changes:

In D3.2, change “in response to the reception of”/“in response to the receipt of” to “in response to” at 637.33, 971.18/21/22, 1181.14, 1600.24, 1654.28, 1656.30, 2033.55, 2332.48, 2467.55, 2478.38, 3042.28, 3539.50, 4016.40, 4620.37, 4621.55. At 4611.43 change “in response to the receipt of MLME-” to “in response to an MLME-”. [This is all instances of “in response to the rec” except the one on page 1908.]

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4767  Mark HAMILTON  5.2.3.2  312.7 | Now that 802.11 data frames can carry a DEI indicator (in the HT control field), the 802.11 SAP (MA-UNITDATA primitives) should support a drop\_eligible parameter, to match 802.1AC's general assumptions. (802.1AC's Annex B.1.5 will also need to be updated to match this, by 802.1 WG.) | At P312L7, insert a new parameter “drop eligible”, after “priority”.  At P312L35 insert a new paragraph, “The drop eligible parameter provides guidance on whether this request can be discarded in preference to other requests when there are insufficient resources in a STA. If drop\_eligible is TRUE, the request can be discarded in preference to other requests in which drop\_eligible is FALSE. The default drop\_eligible value is FALSE.”  At P314L43, insert a new parameter “drop eligible” after “priority”.  At P315L6 insert a new paragraph, “The drop eligible parameter indicates if the received MSDU was designated as DEI in the received protocol headers. If no protocol header designation was received, the parameter value is FALSE.”  At P164L25, insert “drop eligible, “ after “priority, “.  At P808L27, append “, per the value of the drop eligibile parameter received in the MA-UNITDATA.request, if any.” to the end of the sentence. (... if there are insufficient resources at the recieving STA, per the value of the drop eligible ...”  At P1802L51, add to the end of the paragraph, “If the MSDU(s) received in an MPDU with the DEI subfield set to true are delievered via an MA-UNITDATA.indication, the drop eligibile parameter of the MA-UNITDATA.indication is set to TRUE. Otherwise, the parameter is set to FALSE.” |

Discussion:

This was ACCEPTED in motion 169. However, what does "The default drop\_eligible value is false." mean? It's not marked as an optional parameter. Similarly specious ", if any" at 808.28. More generally, the wording around drop eligibility is a bit haphazard.

Proposed additional changes:

In D3.2:

At 164.24 change “drop eligible” to “drop eligibility”.

At 312.36 change “(#4767)The drop eligible parameter provides guidance on whether this request can be discarded in preference to other requests when there are insufficient resources in a STA. If drop eligible is true,(Ed) the request can be discarded in preference to other requests in which drop eligible is false.(Ed) The default drop eligible value is false.(Ed)” to “(#4767)The drop eligible parameter is a Boolean that indicates whether this MSDU can be discarded in preference to other MSDUs when there are insufficient resources in a STA. If drop eligible is true,(Ed) the MSDU can be discarded in preference to other MSDUs for which drop eligible is false.(Ed)”

At 315.8 change “(#4767)The drop eligible parameter indicates if the received MSDU was designated as DEI in the received protocol headers. If no protocol header designation was received, the parameter value is false.(Ed)” to “(#4767)The drop eligible parameter is a Boolean that indicates whether the received MSDU was designated as drop eligible in the DEI subfield of the HT variant HT Control field of the incoming frame, if present. If no HT variant HT Control field was present, the parameter value is false.(Ed)”

At 808.27 change “drop eligible parameter received in” to “drop eligible parameter in”. At 808.28 delete “, if any”.

At 1790.51 change “(#4767-Ed)If MSDU(s) received in an MPDU are delivered via an MA-UNITDATA.indication, the drop eligible parameter of the MA-UNITDATA.indication is set to true if the DEI subfield is equal to 1 and set to false if the DEI subfield is equal to 0.” to “(#4767-Ed)If MSDU(s) received in an MPDU are delivered via an MA-UNITDATA.indication, the drop eligible parameter of the MA-UNITDATA.indication is set to true if the MPDU contains an HT variant HT Control field and the DEI subfield is equal to 1 and set to false otherwise.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4625  Mark RISON | Since 1.4 defines x-y as being inclusive, the word "inclusive" is no longer needed for ranges | Delete "inclusive" in Clause 6 (10x), 9.2.2, 9.2.4.6.1 (2x), 9.4.2.5.1, 9.4.2.21.10, 9.4.2.45 (2x), 9.4.2.94, 9.4.2.154, 9.4.2.167 (3x), 10.19, 10.21 (3x), 11.10.14, 12.5.2.3.3, 19.3.9.3.2, 21.3.8.2.1, Table 23-1, dot11TxPowerLevelExtended in C.3 (2x). Delete "(all inclusive)" in 10.3.2.12 (x). Delete " (inclusive)" in 10.47.6 (second instance), 11.3.9.2, Table 21-23 (2x), Table 22-21 (2x), Table 23-29 (2x). Delete ", inclusive" in 12.3.3.3.6 |

Discussion:

This was ACCEPTED in motion 160. However, there is still one suspect “(inclusive)” in 10.47.6:

The PTSF subfield is set to TSF[Partial TSF Offset+4: Partial TSF Offset+11] (inclusive)

The problem is that [x:y] isn’t defined globally, though there are some hints:

* In 1.5: “dec(A[b:c]) is the cast from binary to decimal operator, where c is the least significant bit in binary value [b:c]”
* In 10.21: “AID[b:c] represents bits b to c (#4625)of the AID”
* and a bunch of MAC address slicing contexts.

The first is nearly there but (a) it has a dec() wrapper and (b) it doesn’t *quite* get around to saying what [b:c] actually *means*.

Previous strawman:

Change 1.5 as follows:

*dec*(A[*b*:*c*]) is the ~~cast from binary to decimal operator~~ value of bits *b* to *c* of A, where *c* is the least significant bit (i.e. bit 0 of the output of the operator) ~~in binary value [b:c]~~.(#1300)

Change 10.47.6 as follows:

The PTSF subfield is set to *dec*(TSF[Partial TSF Offset+4 : Partial TSF Offset+11]) ~~(inclusive)~~

TBD. Maybe use dec() in 10.47.6 and clarify in 1.5 that [b:c] means bits b to c **inclusive**?

Proposed additional changes:

In D3.2:

Change/add to 1.5 to say:

A[*b*:*c*] is bits *b* to *c* of A. If A is a MAC address, then it is represented such that bit 0 is the Individual/Group bit and bit 47 is the last transmitted bit.

NOTE—*b* might be less than, greater than or equal to *c*. The first bit of the output is the value of bit *b* or bit *c*, whichever is lower-numbered.

*int* (A[*b*:*c*]) is the value of bits *b* to *c* of A. If A is a MAC address, then it is represented such that bit 0 is the Individual/Group bit and bit 47 is the last transmitted bit.

NOTE—*b* might be less than, greater than or equal to *c*. Bit 0 of the output is the value of bit *b* or bit *c*, whichever is lower-numbered.

Change the following as shown:

9.2.2: delete “MAC\_ADDR[b:c] represent bits b to c (#4625)of MAC address MAC\_ADDR.(#1300)”

9.4.2.45: change “ZERO[b:c] denotes bits b to c (#4625)of a 48-bit address set to 0(#1300)

REF\_BSSID[b:c] denotes bits b to c (#4625)of the REF\_BSSID address(#1300)” to

“ZERO is a 48-bit all-zeroes address”

10.19: delete “In Table 10-12 (Settings for the TXVECTOR parameters GROUP\_ID and PARTIAL\_AID for VHT STAs(11aj))(11aj), Table 10-13 (Settings for the TXVECTOR parameter PARTIAL\_AID for CMMG STAs(11aj)) and this clause, BSSID[b:c] and RA[b:c] represent bits b to c (#4625)of the BSSID and RA, respectively, with the 48-bit MAC address represented such that bit 0 is the Individual/Group bit and bit 47 is the last transmitted bit, in which bit position b is then scaled by 20 and c by 2c-b. See Figure 9-1 (Representation of a 48-bit MAC address(#1300)(Ed)).(#1300)”

10.21: change “In Table 10-14 (Settings for the TXVECTOR parameter PARTIAL\_AID for NDP frames(#1300)(11ah)), Table 10-15 (Settings for the TXVECTOR parameter PARTIAL\_AID for non-1 MHz PPDUs and non-NDP frames(#1300)(11ah)), and in this clause(#1300):

— AID[b:c] represents bits b to c (#4625)of the AID of the recipient STA for an individually addressed frame with bit 0 being the first transmitted, and represents bits b to c (#4625)of the group AID of the recipient STAs for a group-addressed frame with bit 0 being the first transmitted.

— BSSID[b:c] represents bits b to c (#4625)of the BSSID, with bit 0 being the Individual/Group bit. In this representation, the 48-bit MAC address is represented such that the Individual/Group bit is BSSID[0] and BSSID[47] is the last transmitted bit. See Figure 9-1 (Representation of a 48-bit MAC address(#1300)(Ed)).(#1300)(#1146)”

to

“In Table 10-14 (Settings for the TXVECTOR parameter PARTIAL\_AID for NDP frames(#1300)(11ah)), Table 10-15 (Settings for the TXVECTOR parameter PARTIAL\_AID for non-1 MHz PPDUs and non-NDP frames(#1300)(11ah)), and in this clause(#1300), AID is the AID of the recipient STA for an individually addressed frame and the group AID of the recipient STAs for a group-addressed frame.”

10.47.6: The PTSF subfield is set to *int* (TSF[Partial TSF Offset+4 : Partial TSF Offset+11]) ~~(inclusive)~~

Change any remaining instances of “*dec* (” or “*dec*(” to “*int* (” (9.4.2.45 Multiple BSSID element (3x), Table 10-12—Settings for the TXVECTOR parameters GROUP\_ID and PARTIAL\_AID for VHT STAs (3x), Table 10-14—Settings for the TXVECTOR parameter PARTIAL\_AID for NDP frames (2x), Table 10-15—Settings for the TXVECTOR parameter PARTIAL\_AID for non-1 MHz PPDUs and non-NDP frames (2x), 10.21 Group ID, partial AID, Uplink Indication, and COLOR in S1G PPDUs non-tables (3x), plus any hidden in non-searchable equations or graphics).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4245  Mark RISON  10.2.3.2  1717.62 | 10.2.3.2 HCF contention based channel access (EDCA) says defaults are always used ("When communicating within a BSS, the EDCA parameters used are [...] from the default values for the parameters when [...] when the STA is a mesh STA") but various other parts of the spec say that EDCA parameters are passed around in various frames when a STA is a QoS STA (as all mesh STAs are) | As it says in the comment |

Discussion:

SAKODA Kazuyuki has confirmed that:

* “mesh STAs always use EDCA parameters from default value. As such, EDCA parameter or QoS Capability element are not present for mesh BSSs”
* “11ah/11ad STAs will not become a mesh STA”

Proposed changes:

In D3.0:

Change 14.1 Mesh STA dependencies at 2769.27 as follows:

When dot11DMGOptionImplemented or dot11S1GOptionImplemented is true, dot11MeshActivated shall be false.

In 9.4.2.34 QoS Capability element at 1144.21 delete the following sentence:

The QoS Capability element is present in Beacon frames that do not contain the EDCA Parameter Set element and in (Re)Association Request frames.

In the table in 6.3.11.2.2 Semantics of the service primitive [for 6.3.11.2 MLME-START.request] at 397.51 change the rightmost cell of the EDCAParameterSet row as follows:

The initial EDCA parameter set values to be

used in the BSS. The parameter is present if

dot11QosOptionImplemented is true and dot11MeshActivated is false;

otherwise not present.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4245 in <this document>, which clarify that the EDCA Parameter Set element is not used in MBSSes, and that S1G STAs are not used in MBSSes.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4087  Rojan Chitrakar  12.5.3.4.1  2608.25 | As per 12.5.3.3 (P2607L59), the MIC is also encrypted along with the plaintext MPDU, so it is not possible to obtain the original MIC at this stage. The original MIC can only be obtained after CCM decryption stage. The figure 12-23 is misleading, either it should be clarified that the MIC that is fed into the CCM decryption block is encrypted MIC, or the entire encrypted MPDU (instead of MIC and data) should be passed to the CCM decryption block. | Rectify the Figure 12-23 as per comment. Specifically, the MIC that is fed into the CCM decryption module should be "encrypted MIC" |

Discussion:

It is agreed that the MIC is encrypted in CCMP (though not in GCMP; see CID 4093).

However, the group preference is not to refer to encryptedness in the figures, except at the edges, but instead to have text that maps the 802.11 objects to the cipher engine objects.

In addition, the CCMP test vectors have an unclear MIC size. See the "Encrypted Frame Frame Body"s in J.6.4 CCMP test vectors, e.g.:

=== CCMP 256 test vector ====

[…]

(11ah)CCMP PV1 test vectors

[…]

PV1 test vector #1:

[…]

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd

a8 eb 7e 78 a0 50

[…]

Encrypted Frame Frame Body - hexdump(len=28): dd d7 40 e2 a5 86 e1 2b 06 0e 45 69

d0 a3 93 61 60 41 2e 45 82 62 ff 2d b5 77 65 73

Figure 12-17—Expanded PV1 CCMP MPDU shows the frame body as being data+MIC, and the text above says the MIC is 8 octets for CCMP-128 and 16 octets for CCMP-256. So why is the encrypted frame frame body in the test vector only 8 octets longer than the plaintext frame body?

Rojan CHITRAKAR says:

I believe its simply an editorial mistake. I believe PV1 frames were meant to be under CCMP-128 Test vectors instead of CCMP-256 Test Vectors? I noted that the first example under CCMP-256 explicitly mentions CCPM-256 AAD, Nonce etc., but the PV1 examples do not. 802.11ah\_2016 simply mentioned “***Insert the following text at the end of J.6.4:***”, I believe that’s why it ended up under CCMP-256 Test Vector.

It does seem the intent was that the CCMP PV1 test vectors are distinct from the CCMP 256 (sic) test vector, but this is laid out less than clearly.

Proposed changes:

In D3.0:

In Figure 12-18—CCMP encapsulation block diagram:

* change "Encrypted Data ," to "Data," on the right
* lowercase "Nonce"

In Figure 12-23—CCMP decapsulation block diagram:

* change "Plaintext data" to "Data" on the right
* lowercase "Nonce"
* change "PN ’" to "Replay counter"

In Figure 12-27—GCMP encapsulation block diagram:

* change "Encrypted Data" to "Data" on the right
* lowercase "Nonce" and "Header"

In Figure 12-29—GCMP decapsulation block diagram:

* change "Plaintext Data" to "Data" on the right
* lowercase "Nonce" and "Header"
* change "PN\*" to "Replay counter"

Sharpen up Figure 12-23—CCMP decapsulation block diagram.

Change "MIC" to "Encrypted MIC" at 2608.51½ and 2609.9½.

Change 12.5.3.3.7 CCM originator processing as follows:

There are four inputs to CCM originator processing (see Figure 12-18—CCMP encapsulation block diagram):

a) Key: the temporal key ~~(16 octets)~~.

b) Nonce: the nonce ~~(13 octets)~~ constructed as described in (#2720)12.5.3.3.3 (Construct AAD(#2720)) b ((11ah)For PV1 MPDUs, the format of the AAD is shown in Figure 12-20 (AAD construction for PV1 MPDUs(M110)(11ah)).).

c) ~~Frame body~~Plaintext data: the plaintext frame body of the MPDU to be encrypted and transmitted.

d) AAD: the AAD ~~((11ah)16–30 octets) constructed from the~~ that is the canonical MPDU header as described in (#2720)12.5.3.3.3 (Construct AAD(#2720)).

(#2720)CCM originator processing provides authentication and integrity of the frame body and the AAD as well as data confidentiality of the frame body. The output from (#2720)CCM originator processing consists of the encrypted data and an encrypted MIC (see Figure 12-16 (Expanded CCMP MPDU)).

The CCM encryption algorithm is described in IETF RFC 3610. The key, nonce, plaintext data and AAD described above are passed to the CCM encryption algorithm as K, N, m and a respectively. The CCM encryption algorithm yields a final result c containing the encrypted message and an encrypted authentication value U; from this the encrypted frame body is taken as the encrypted message and the MIC is taken as U.

Change 12.5.3.4.2 CCM recipient processing as follows:

There are ~~four~~five inputs to CCM recipient processing (see Figure 12-23 (CCMP decapsulation block diagram)):

— Key: the temporal key ~~(16 octets)~~.

— Nonce: the nonce ~~(13 octets)~~ constructed as described in 12.5.3.3.3 (Construct AAD(#2720)) b ((11ah)For PV1 MPDUs, the format of the AAD is shown in Figure 12-20 (AAD construction for PV1 MPDUs(M110)(11ah)).).

— Encrypted ~~frame body~~data: the encrypted portion of the frame body from the received MPDU~~. The encrypted frame body includes~~ , excluding the MIC (see Figure 12-16 (Expanded CCMP MPDU) and Figure 12-17 (Expanded PV1 CCMP MPDU)).

— MIC: the encrypted MIC from the received MPDU.

— AAD: the AAD ~~((11ah)12–30 octets)~~ that is the canonical MPDU header as described in (#2720)12.5.3.3.3 (Construct AAD(#2720)).

(#2720)CCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as decrypting the frame body. The plaintext is returned only if the MIC check is successful.

The CCM decryption algorithm is described in IETF RFC 3610. The key, nonce, AAD and encrypted data described above are passed to the CCM decryption algorithm as K, N, a and c respectively. The CCM decryption algorithm yields a decrypted message m and a value T; from this the plaintext frame body described below is taken as m, if the MIC described above matches T.

There is one output from error-free CCM recipient processing:

— Frame body: the plaintext frame body, which is 8 octets (CCMP-128) or 16 octets (CCMP-256) smaller than the encrypted portion of the frame body.

Change 12.5.5.3.6 GCM originator processing as follows:

There are four inputs to GCM originator processing (see Figure 12-27—GCMP encapsulation block diagram):

a) Key: the temporal key ~~(16 octets)~~.

b) Nonce: the nonce ~~(12 octets)~~ constructed as described in 12.5.5.3.4 (Construct GCM nonce).

c) ~~Frame body~~Plaintext data: the plaintext frame body of the MPDU to be encrypted and transmitted.

d) AAD: the AAD ~~(22-30 octets) constructed from the~~ that is the canonical MPDU header as described in 12.5.5.3.3 (Construct AAD).

~~The~~ GCM originator processing provides authentication and integrity of the frame body and the AAD as well as data confidentiality of the frame body. The output from the GCM originator processing consists of the encrypted data and 16 additional octets of encrypted MIC (see Figure 12-26 (Expanded GCMP MPDU)).

The GCM encryption algorithm is described in NIST Special Publication 800-38D. The key, nonce, plaintext data and AAD described above are passed to the GCM encryption algorithm as *K*, *IV*, *P* and *A* respectively. The GCM encryption algorithm yields a ciphertext *C* and an authentication tag *T*; from this the encrypted frame body is taken as *C* and the MIC is taken as *T*.

Change 12.5.5.4.2 GCM recipient processing as follows:

There are ~~four~~five inputs to GCM recipient processing (see Figure 12-29 (GCMP decapsulation block diagram)):

— Key: the temporal key ~~(16 octets)~~.

— Nonce: the nonce ~~(12 octets)~~ constructed as described in 12.5.5.3.4 (Construct GCM nonce).

— Encrypted ~~frame body~~data: the encrypted portion of the frame body from the received MPDU~~. The encrypted frame body includes a 16-octet MIC~~ (see Figure 12-26 (Expanded GCMP MPDU)).

— MIC: the MIC from the received MPDU.

— AAD: the AAD ~~(22-30 octets)~~ that is the canonical MPDU header as described in 12.5.5.3.3 (Construct AAD).

~~The~~ GCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as decrypting the frame body. The plaintext is returned only if the MIC check is successful.

The GCM decryption algorithm is described in NIST Special Publication 800-38D. The key, nonce, encrypted data, AAD and MIC described above are passed to the GCM decryption algorithm as *K*, *IV*, *C*, *A* and *T* respectively. The GCM decryption algorithm yields a plaintext *P* or an indication of inauthenticity *FAIL*; from this the plaintext frame body is taken as *P*, if there was no indication of inauthenticity.

There is one output from error-free GCM recipient processing:

— Frame body: the plaintext frame body, which is ~~16 octets smaller than~~the same size as the encrypted portion of the frame body.

In S.1 change “encrypted Frame Body” to “encrypted portion of the frame body”.

In J.6.4 CCMP test vectors move the PV1 test vectors (4514.44 to end of subannex) to immediately above the CCMP 256 test vector (i.e. to 4514.18), changing the first line from “CCMP PV1 test vectors” to “==== CCMP-128 PV1 test vectors ====”. Change “==== CCMP 128 test mpdu ====” at 4513.39 to “==== CCMP-128 PV0 test vector ====”. Move the equals sign at the end of 4528.54 to the start of 4514.19 (changing the font to match), so that there are always four equal signs, and change “GCMP 256” to “GCMP-256”.

In J.11.1 Test vector change “GCMP test mpdu #1” to “GCMP-128 test vector #1”, “GCMP test mpdu #2” to “GCMP-128 test vector #2” and “GCMP-256 test mpdu #3” to “GCMP-256 test vector”. Change the heading for J.11.1 to “GCMP test vectors” and the font for the body to a monospaced font like J.6.4.

Proposed resolution:

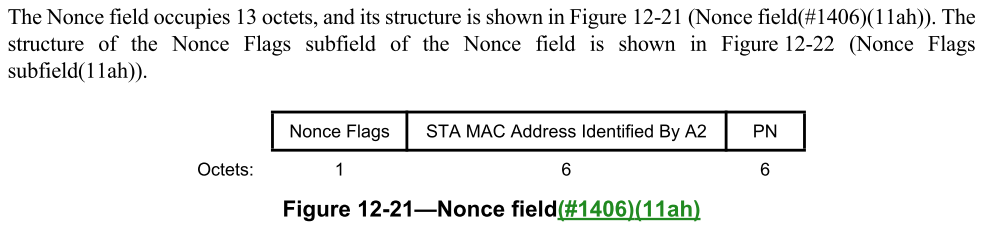
REVISED

Make the changes shown under “Proposed changes” for CID 4087 in <this document>, which tidy up the description of CCM and GCM originator and recipient processing (including explicitly mapping CCMP and GCMP objects to CCM and GCM objects) and tidy up the layout of the test vectors.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4611  Mark RISON  12  2609.5 | "4) The nonce(#1406) value is constructed from the STA MAC Address Identified By A2, PN, and Nonce Flags fields." is just duplication of Figure 12-21--Nonce field. Ditto duplication of Figure 12-28--Nonce field for GCMP | Delete the cited text, and "3) (11ah)The nonce(#1406) value is constructed from the A2, PN, and Nonce Flags fields." in 12.5.3.4.1 and "c) The nonce(#1406) value is constructed from the A2 and PN fields." in 12.5.5.4.1 |
| CID 4612  Mark RISON  12  2609.5 | "4) The nonce(#1406) value is constructed from the STA MAC Address Identified By A2, PN, and Nonce Flags fields." is just duplication of Figure 12-21--Nonce field. Ditto duplication of Figure 12-28--Nonce field for GCMP | Replace the cited text, and "3) (11ah)The nonce(#1406) value is constructed from the A2, PN, and Nonce Flags fields." in 12.5.3.4.1 and "c) The nonce(#1406) value is constructed from the A2 and PN fields." in 12.5.5.4.1, with references to the figures. Also remove the "The Nonce field has an internal structure of Nonce Flags || (11ah)STA MAC Address Identified By A2 || PN" and "The Nonce field has an internal structure of A2 || PN" duplication (of figures immediately above!) |
| CID 4614  Mark RISON  12.5.3.3.4  2606.37 | "(11ah)STA MAC Address Identified By A2 field occupies octets 1-6. This shall be encoded with the octets ordered with (11ah)STA MAC Address Identified By A2 octet 0 at octet index 1 and (11ah)STA MAC Address Identified By A2 octet 5 at octet index 6." says nothing of value, but omits the key point of what the field actually contains | Change to "The STA MAC Address Identified By A2 field contains the Address 2 field from the PV0 MPDU or the address derived from the A2 field from the PV1 MPDU (see 9.8.3.2)." |

Discussion:

Duplication is baaad, m’kay? For instance:



v. (just 10 lines down!)

The Nonce field has an internal structure of Nonce Flags || STA MAC Address Identified By A2 || PN

v. (2 pages later)

3) The nonce value is constructed from the A2, PN, and Nonce Flags fields.

Note: Yongho SEOK has confirmed that PV1 Management frames are Management frames (i.e. obey the behavioural rules that apply to Management frames). This includes management frame protection.

Proposed changes:

In D3.0:

At 2608.45 change:

1) (11ah)The encrypted MPDU is parsed to construct the AAD and nonce values.

2) (11ah)The AAD is formed from the MPDU header of the encrypted MPDU.

3) (11ah)The nonce(#1406) value is constructed from the A2, PN, and Nonce Flags fields.

to:

1) The encrypted MPDU is parsed to construct the AAD (see 12.5.3.3.3 (Construct AAD)) and nonce (see 12.5.3.3.4 (Construct CCM nonce)) values

and renumber the following list item numbers.

At 2608.63 change:

1) The encrypted MPDU is parsed to construct the AAD and nonce values.

2) The CCMP header is constructed as defined in (#2720)12.5.3.3.6 (Construct CCMP header for PV1 MPDUs(#2720)(11ah)).

3) The AAD is formed from the MPDU header of the encrypted MPDU.

4) The nonce(#1406) value is constructed from the STA MAC Address Identified By A2, PN, and Nonce Flags fields.

to:

1) The encrypted MPDU is parsed to construct the AAD (see 12.5.3.3.3 (Construct AAD)) and nonce (see 12.5.3.3.4 (Construct CCM nonce)) values.

2) The CCMP header is constructed as defined in (#2720)12.5.3.3.6 (Construct CCMP header for PV1 MPDUs(#2720)(11ah)).

and renumber the following list item numbers.

At 2618.23 change:

a) The encrypted MPDU is parsed to construct the AAD and nonce values.

b) The AAD is formed from the MPDU header of the encrypted MPDU.

c) The nonce(#1406) value is constructed from the A2 and PN fields.

to:

a) The encrypted MPDU is parsed to construct the AAD (see 12.5.5.3.3 (Construct AAD)) and nonce (see 12.5.5.3.4 (Construct GCM nonce)) values.

and reletter the following list item numbers.

At 2606.23 change:

The Nonce field has an internal structure of Nonce Flags || (11ah)STA MAC Address Identified By A2 || PN, where

— The Priority subfield of the Nonce Flags field shall be set to the priority value of the MPDU.

— When management frame protection is negotiated, the Management field of the Nonce Flags field shall be set to 1 if the (11ah)PV0 MPDU’s Type field of the Frame Control field is 00 (Management frame) (11ah)or the PV1 MPDU’s Type field of the Frame Control field is 001 (Management frame); otherwise, it shall be set to 0.

— (11ah)The PV1 subfield of the Nonce Flags field shall be set to 1 when the Protocol Version field of the Frame Control field of the MPDU header is equal to 1. The PV1 subfield of the Nonce Flags field shall be set to 0 otherwise.

— Bits (11ah)6 to 7 of the Nonce Flags field shall be set to 0.

— (11ah)STA MAC Address Identified By A2 field occupies octets 1–6. This shall be encoded with the octets ordered with (11ah)STA MAC Address Identified By A2 octet 0 at octet index 1 and (11ah)STA MAC Address Identified By A2 octet 5 at octet index 6.

— The PN field occupies octets 7–12. The octets of PN shall be ordered so that PN0 is at octet index 12 and PN5 is at octet index 7.

to:

The Priority subfield shall be set to the priority value of the MPDU.

The Management subfield shall be set to 1 if the MPDU is a Management frame and management frame protection is negotiated; otherwise, it shall be set to 0.

The PV1 subfield shall be set to 1 for a PV1 frame; otherwise, it shall be set to 0.

The Zeros subfield shall be set to 0.

The STA MAC Address Identified By A2 subfield shall contain the Address 2 field from the MAC header for PV0 MPDUs and the MAC address identified by the A2 field in the MAC header for PV1 MPDUs (see 9.8.3.2).

The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

At the end of 9.8.5.1 Format of PV1 Management frames add a para:

PV1 Management frames are Management frames.

Change 782.56 as follows:

The components of (PV0) (M101)Management frame bodies are defined in 9.4 (Management and Extension frame body components).

Change 853.41 as follows:

9.3.3 (PV0) Management frames(#2569)

9.3.3.1 Format of (PV0) Management frames

At 2616.55 change:

The Nonce field has an internal structure of A2 || PN, where

— MPDU address A2 field occupies octets 0 to 5. This shall be encoded with the octets ordered with A2 octet 0 at octet index 0 and A2 octet 5 at octet index 5.

— The PN field occupies octets 6 to 11. The octets of PN shall be ordered so that PN0 is at octet index 11 and PN5 is at octet index 6.

to:

The A2 subfield shall contain the Address 2 field from the MAC header.

The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

Change “ciphertext” to “cipher text” at 2587.8, 2588.25, 2718.36/39, 2720.54/63, 4620.7.

Change “plain text” to “plaintext” at 158.10, 4526.64.

Change “Plain Text” to “Plaintext” at 4526.64.

Change “Plain text” to “Plaintext” at 4527.1, 4530.29.

Proposed resolution for CIDs 4611, 4612, 4614:

REVISED

Make the changes shown under “Proposed changes” for CID 4611, 4612, 4614 in <this document>, which make changes in the direction suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4259  Mark RISON | "QoS Data frame" is ambiguous. It could mean Type = Data, Subtype has b7 set, or it could mean Type = Data, Subtype = QoS Data | After "QoS CF-Poll frame refers specifically to the QoS CF-Poll frame, subtype 1110." add "Similarly, QoS Data frame refers specifically to the QoS Data frame, subtype 1000.". Also delete the comma in " whereas," in 3.2 and "Whereas " in 9.2.2 |

Discussion:

In some parts of the spec, “QoS Data” clearly just refers to the specific subtype, because it’s in a context like “QoS Data or QoS Null frame”. On the other hand, we have an explicit definition of “QoS Data frame” that means it applies to all Data frames with b7 set in FC. So it’s a mess, and there’s no non-Herculanean solution.

Proposed resolution:

REVISED

In 9.3.2.1.1 (846.55 in D3.2) change:

Data frames with a 1 in the QoS subfield of the Subtype subfield are collectively referred to as *QoS*

*Data frames*. Each of these data subtypes contains QoS in their names, and this frame format is

distinguished by the presence of a QoS Control field in the MAC header.

to:

Data frames with the QoS subfield of the Subtype subfield (see 9.2.4.1.3) set to 1 contain *QoS* in their names and contain a QoS Control field in the MAC header. Depending on the context, *QoS Data frame* either refers to any such frame, or refers specifically to the Data frame with subtype 1000. References nearby to other specific Data frames with *QoS* in their name (e.g. QoS Null or QoS Data +CF-Poll) typically suggest the latter interpretation.

Delete the comma in " whereas," in 3.2 (182.42 in D3.2).

Delete "Whereas " in 9.2.2 (782.18 in D3.2).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4531  Mark RISON  9 | "bit representation plus 1" (5x) -- it's not clear what "bit representation" is supposed to mean here, and in any case this would be better expressed in the canonical "minus 1" form | As it says in the comment |

Discussion:

As it says in the comment. The canonical form is e.g.:

The NUM\_STS subfield contains an unsigned integer representing the number of space-time streams minus 1.

If the Feedback Type field indicates MU, then Nc Index indicates the number of columns minus 1

set to maximum number of space-time streams that the STA can receive in a VHT NDP minus 1.

In fact, the existing text makes no sense. “bit representation” must mean “the value indicated by what the bits are set to”, but then by definition the field is set to this, not to this plus 1.

Proposed resolution:

REVISED

In D3.2:

At 894.55 change:

The A-BFT Length subfield specifies the size of the A-BFT following the BTI and is defined in units of a sector sweep slot (10.42.5 (Beamforming in A-BFT)). (MDR2)This field is in the range 1 to 8, with the field being set to the bit representation plus 1.

to:

The A-BFT Length subfield indicates number of sector sweep slots (10.42.5 (Beamforming in A-BFT)) in the A-BFT following the BTI, minus 1.

At 1295.53 change:

The Number of RX DMG Antennas subfield indicates the total number of receive DMG antennas of the STA. (MDR2)This subfield is set to the bit representation plus 1, which ranges from 1 to 4.

to:

The Number of RX DMG Antennas subfield indicates the total number of receive DMG antennas of the STA minus 1.

At 1295.62 change:

The Total Number of Sectors subfield indicates the total number of transmit sectors the STA uses in a transmit sector sweep combined over all DMG antennas, including any LBIFS required for DMG antenna switching (see 10.42 (DMG beamforming)). (MDR2)This subfield is set to the bit representation plus 1, which ranges from 1 to 128.

to:

The Total Number of Sectors subfield indicates the total number of transmit sectors the STA uses in a transmit sector sweep combined over all DMG antennas, including any LBIFS required for DMG antenna switching (see 10.42 (DMG beamforming)), minus 1.

At 1445.61 change:

This field ranges from 1 to 4, with the value being equal to the bit representation plus 1.

to:

Set to the number of antennas minus 1.

At 1446.26 change:

This field ranges from 1 to 128, with the value being equal to the bit representation plus 1.

to:

Set to the number of transmit sectors minus 1.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4543  Mark RISON  9.4.2.14  1008.34 | "The Power Capability element specifies the minimum and maximum transmit powers with which a STA is capable of transmitting in the current channel." - what is "the current channel" if sent in association? | As it says in the comment |

Discussion:

There are a number of other uses of the queried term in normative text, e.g.:

The Power Constraint element contains the information necessary to allow a STA to determine the local maximum transmit power in the current channel. (2x)

the transmit power as measured at the output of the antenna connector to be used by the transmitting STA on the current channel

A STA shall determine a regulatory maximum transmit power for the current channel by selecting the

minimum of the following:

Proposed resolution:

REJECTED

The term “the current channel” is used widely in the spec. In the context of association, it must refer to the channel on which the BSS operates.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4549  Mark RISON  9.3.1.2  826.15 | "The RA field of the RTS frame is the address of the STA, on the WM, that is the intended immediate recipient of the pending individually addressed Data, Management, or Control frame." -- what if there's no pending individual frame (e.g. it's to protect a broadcast)? What if it's to protect an Extension frame? | As it says in the comment |

Discussion:

This sentence predates the introduction of Extension frames, so that is probably just spec rot.

As for broadcasts, there are topologies in which RTS-CTS might work (e.g. all the other STAs in the BSS are bunched up in the same general direction), though it is not immediately clear how the transmitter might determine that this is the case. However, the group prefers to use e.g. CTS-to-self for this, since the topologies in which RTS-CTS might work are not frequent and it’s not clear which STA to ask for the CTS from. Also some STAs might ignore traffic after an RTS addressed to someone else.

“on the WM” seems rather otiose.

Proposed changes:

REVISED

Change the cited text to “The RA field of the RTS frame is the address of the STA that is the intended immediate recipient of a pending individually addressed frame.”

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4510  Mark RISON  9.3.1.1  824.52 | There should be a general statement that Control frames do not have an Address 3, and some do not have an Address 2 either | As it says in the comment |

Discussion:

For Data and Management frames there is a broad introductory statement:

The Frame Control, Duration, Address 1, Address 2, Address 3, and Sequence Control fields are present in all data frame subtypes. The presence of the Address 4 field is determined by the setting of the To DS and From DS subfields of the Frame Control field (see below). The QoS Control field is present when the QoS subfield of the Subtype subfield is set to 1.

The Frame Control, Duration, Address 1, Address 2, Address 3, and Sequence Control fields are present in all management frame subtypes.

Proposed resolution:

REVISED

Insert the following para as the second para of 9.3.1.1 Format of Control frames:

The Frame Control, Duration and Address 1 (RA) fields are present in all control frame subtypes. The Address 2 (TA) field is present in some control frame subtypes.

At the end of the first para of 9.3.2.1.1 General change the last sentence to the following two sentences:

The presence of the QoS Control field is determined by the setting of the QoS subfield of the Subtype subfield (see 9.2.4.1.3) of the Frame Control field. The presence of the HT Control field is determined by the setting of the +HTC subfield of the Frame Control field (see 9.2.4.1.10).

After the second sentence of the first para of 9.3.3.1 Format of Management frames add:

The presence of the HT Control field is determined by the setting of the +HTC subfield of the Frame Control field (see 9.2.4.1.10).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4505  Mark RISON  11.41 | We now have two Operating Mode Notification frames (9.6.22.4 and 9.6.29.3). So which is intended when the spec talks of "the Operating Mode Notification frame"? | In 9.6.29.3 prepend "CMMG " to "Operating Mode Notification". At the top of 11.41 add "In this subclause, references to an Operating Mode Notification frame or element should be understood as referring to a CMMG Operating Mode Notification frame or element, when transmitted or received by a CMMG STA." |

Discussion:

Small mercies: at least the eponymous element does have a different name!

Proposed changes:

In D3.2:

Change 9.6.29.3 Operating Mode Notification frame format(11aj) as follows

**9.6.29.3 CMMG Operating Mode Notification frame format(11aj)**

The CMMG Operating Mode Notification frame (#2568)is used to notify STAs that the transmitting STA is changing its operating channel width, the maximum number of spatial streams it can receive, or both.

In the context of CMMG STAs, references to an Operating Mode Notification frame or element should be understood as referring to a CMMG Operating Mode Notification frame or element, respectively.

The Action field of the CMMG Operating Mode Notification frame contains the information shown in Table 9-523 (Operating Mode Notification frame Action field format(#4252)(11aj)).

**Table 9-523—CMMG Operating Mode Notification frame Action field format**

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4505 in <this document>, which resolve the name of the frame and specify that in CMMG contexts “Operating Mode Notification” refers to the CMMG flavour.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4512  Mark RISON  9.4.2.55.3  1176.10 | "This field is an integer in the range 0 to 3." -- well, duh, it's a 2-bit field, so it can't really be anything else, can it? | Delete the cited text, and also in Table 9-300--Subfields of the S1G Capabilities Information field and in C.3, and "This field is an integer in the range 0 to 7." in Table 9-271--Subfields of the VHT Capabilities Information field and in Table 9-314--Subfields of the A-MPDU Parameters field |

Discussion:

School maths requires that an n-bit field contain values in the range 0 to 2n – 1. This does not need to be stated (and indeed is generally not stated). Only if the field is not allowed to contain all mathematically possible values need the range be specified.

There is an argument for saying the range needs to be specified to show that it’s an unsigned integer. Unfortunately (a) giving the range doesn’t actually specify the encoding and (b) there are many many many unsigned integer fields that are not specified to be such. The first few in 9.4.2 are:

The Length field indicates the number of octets in the element excluding the Element ID and Length fields.

The DTIM Count field indicates how many Beacon frames (including the current frame) appear before the next DTIM. A DTIM count of 0 indicates that the current TIM is a DTIM. The DTIM Count field is a single octet. When a TIM element is included in a TIM frame, the DTIM Count field is reserved.

The DTIM Period field indicates the number of beacon intervals or short beacon intervals(11ah) between successive DTIMs.

When the TIM is carried in a non-S1G PPDU, the remaining 7 bits of the field form the Bitmap Offset

Proposed changes:

Insert the following as the second para of 9.2.2 Conventions:

Unless specified otherwise, a number in a field is encoded as an unsigned integer.

In Table 9-18—ASEL Command and ASEL Data subfields change “A number in the range 0 to 15, the number being the” to “The” and delete the other “0 to 15” (5x).

In Table 9-24—MFB subfield in the CMMG variant HT Control field delete “in the range 0 to 31”

In Table 9-57—Subfields of the MIMO Control field and Table 9-87—Subfields of the CMMG MIMO Control field delete “Valid range: 0 to 7.”

In Table 9-185—Subfields of the A-MPDU Parameters field and Table 9-300—Subfields of the S1G Capabilities Information field delete “This field is an integer in the range 0 to 3.”

In Table 9-271—Subfields of the VHT Capabilities Information field and Table 9-314—Subfields of the A-MPDU Parameters field delete “This field is an integer in the range 0 to 7.”

In Table 9-300—Subfields of the S1G Capabilities Information field and Table 9-313—Subfields of the CMMG Capabilities Info field format change “Set to an unsigned integer in the range 0 to 7 if sent by an AP.” to “Set to an unsigned integer if sent by an AP.”

In 10.19 Group ID and partial AID in VHT and CMMG(11aj) PPDUs and 10.21 Group ID, partial AID, Uplink Indication, and COLOR in S1G PPDUs delete “within the range 0 to 7” (2x in each subclause).

In Table 19-11—HT-SIG fields delete “in the range 0 to 65 535”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4512 in <this document>, which delete the requested duhs and a few more, and also make a general statement that fields use unsigned integer encoding by default.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4516  Mark RISON  9.6.22.4 | Should specify that OMN can be broadcast (discussion with Abhi) | As it says in the comment |

Discussion:

Abhishek PATIL might have suggested that it might be desirable to broadcast OMN frames in certain situations, though neither of us can remember the details. But it doesn’t sound unreasonable.

It is already allowed to broadcast OMN information in beacons, so it must be OK to broadcast OMN information in broadcast OMN frames.

Proposed changes:

In D3.2:

Change 11.41 Notification of operating mode changes as follows:

(11ah)A non-S1G AP should notify associated STAs of a change in the maximum number of spatial streams it is able to receive through one or more of the following mechanisms:

— Using individually addressed Operating Mode Notification frames

— Using broadcast Operating Mode Notification frames

— Including the Operating Mode Notification element in Beacon frames for a period of time to allow STAs in PS mode to receive the notification

NOTE—A broadcast Operating Mode Notification frame might not be received by a STA in PS mode.

(11ah)An S1G AP should notify associated STAs of a change in its operating channel width through one or more of the following mechanisms:

— Using the Extended Channel Switch Announcement element, Extended Channel Switch Announcement frame, or both, following the procedure described in 11.9 (Extended channel switching (ECS))

— Using individually addressed Operating Mode Notification frames

— Using broadcast Operating Mode Notification frames

— Using the Channel Width subfield in the S1G Operation element

NOTE—A broadcast Operating Mode Notification frame might not be received by a STA in PS mode.

An AP should notify associated STAs of a change in its operating channel width through one or more of the following mechanisms:

— Using the Channel Switch Announcement element, Channel Switch Announcement frame or both following the procedure defined in 11.8.8.2 (Selecting and advertising a new channel in a non-DMG infrastructure BSS)

— Using the Extended Channel Switch Announcement element, Extended Channel Switch Announcement frame or both, following the procedure described in 11.9 (Extended channel switching (ECS))

— Using individually addressed Operating Mode Notification frames and/or Notify Channel Width frames

— Using broadcast Operating Mode Notification frames and/or Notify Channel Width frames

— Using the STA Channel Width field in the HT Operation element and/or Channel Width field in the VHT Operation element

NOTE—A broadcast Operating Mode Notification or Notify Channel Width frame might not be received by a STA in PS mode.

Change 11.10.6 Requesting and reporting of measurements as follows:

— Measurement requests received in ~~M~~multicast-group addressed Radio Measurement Request frames

— Measurement requests received in ~~B~~broadcast ~~addressed~~ Radio Measurement Request frames

In 11.1.4.3.2 Active scanning procedure for a non-DMG STA and 11.1.4.3.8 Non-scanning probe request transmission change “broadcast addressed” to “broadcast”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4516 in <this document>, which allow for OMN (and NCW) frames to be broadcast.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4353  Mark RISON  9.3.3.1  854.43 | "c) The Address 3 field of the Management frame is set and determined as follows:  1) In Probe Request frames, the Address 3 field is the BSSID. The BSSID is either a specific  BSSID as described in item 4) below" -- but 4) below is "Otherwise" so is not in scope of c)1) | As it says in the comment |
| CID 4560  Mark RISON  9.3.1.1 [sic]  854.43 | "The Address 3 field of the Management frame is set and determined as follows:". 3) covers OCB and 4) covers infra, IBSS and MBSS, but what about e.g. PBSS and TDLS? | In 4) change "AP" to "AP or PCP" and in 3) after "true" add "or the STA is transmitting the Management frame to a peer TDLS STA" |

Discussion:

It would be better to be clear and consistent.

Note that SAKODA Kazuyuki has confirmed that:

As written in 9.3.3.1 “Format of Management frames”, mesh STA sets Address 3 field to TA in general, but the rule is not applied to the Probe Request frame. Address 3 in the Probe Request frame can be either Address 3 (= TA) or wildcard BSSID. (By the way, the description here “In Probe Request frames, the Address 3 field is the BSSID. The BSSID is either a specific BSSID as described in item 4) below” may need a refinement.)

As in 11.1.4.3.4 “Criteria for sending a response”, mesh STA does not apply BSSID filtering when receiving Probe Request frame. Mesh STA discovery is not sensitive to the value of Address 3 field in Probe Request frame.

Here is a thought. If Address 3 field is set to wildcard BSSID in a Probe Request frame, there is a high chance that APs will be responding to the probe request as well as mesh STAs. Maybe, the spec allows such a flexibility.

The rules in a PBSS should be merged into those for an infrastructure BSS, so it’s all in one place. At the moment the following sentence would mean you can’t do a wildcard probe in a PBSS, and/or that you have a conflict with c)1), for example:

Within a PBSS, the BSSID field of a Management frame is set to the MAC address in use by the STA contained in the PCP of the PBSS.

Menzo WENTINK has pointed out that TDLS peer STAs might exchange Management frames such as VHT Compressed Beamforming Report frames. E.g. in 10.36.5.2 Rules for VHT sounding protocol sequences:

NOTE―A STA that transmits a VHT NDP Announcement frame to a TDLS peer STA obtains the AID for the peer STA from TDLS Setup Request, or TDLS Setup Response frame.

However, this is for an infrastructure BSS only, because “A DMG STA shall not use the TDLS protocol.” per 11.21 Tunneled direct-link setup.

Proposed changes:

Change 9.3.3.1 Format of Management frames as follows

c) The Address 3 field of the Management frame is set and determined as follows:

1) In Probe Request frames, the Address 3 field ~~is~~can be ~~the BSSID. The BSSID is either a specific BSSID as described in item 4) below or~~ the wildcard BSSID as defined in the procedures specified in 11.1.4 (Acquiring synchronization, scanning). If Address 3 is not the wildcard BSSID, then it is (for a nonmesh STA) the BSSID of the BSS of the intended recipient(s), or (for a mesh STA) the MAC address of the intended recipient.

NOTE—Per 11.1.4.3.4 (Criteria for sending a response), a mesh STA does not examine the Address 3 field in Probe Request frames it receives. Using an individual address, however, might prevent unwanted responses from other STAs.

2) In Public Action frames, the Address 3 field is the BSSID. The BSSID value is set according to 11.18 (Public Action frame addressing).

3) If dot11OCBActivated is true, the Address 3 field is the wildcard BSSID.

4) Otherwise(#2013):

i) If the STA is an AP or PCP, the Address 3 field is the same as the Address 2 field.

ii) If the STA is transmitting the Management frame to an AP that is not in a multiple BSSID set or to a PCP, the Address 3 field is the BSSID, irrespective of whether the STA is associated with that AP or PCP.

iii) If the STA is transmitting the Management frame to an AP that is in a multiple BSSID set, the Address 3 field is the BSSID of the AP’s BSS (which is either the transmitted BSSID or a nontransmitted BSSID), irrespective of whether the STA is associated with that AP.

iv~~ii~~) If the STA is transmitting the Management frame to one or more IBSS STAs(#2488), the Address 3 field is the BSSID of the IBSS.

~~i~~v) If the STA is a mesh STA, the Address 3 field is the TA.

vi) If the STA is a TDLS STA transmitting the Management frame to a TDLS peer STA, and the AP to which they are associated is not in a multiple BSSID set, the Address 3 field is the BSSID.

vii) If the STA is a TDLS STA transmitting the Management frame to a TDLS peer STA, and the AP to which they are associated is in a multiple BSSID set, the Address 3 field is the BSSID of the AP’s BSS (which is either the transmitted BSSID or a nontransmitted BSSID).

The address fields for (#4249)Multihop Action frames are described in 9.3.5 (Frame addressing in an MBSS).

~~Within a PBSS, the BSSID field of a Management frame is set to the MAC address in use by the STA contained in the PCP of the PBSS.~~

In 10.36.5.2 Rules for VHT sounding protocol sequences change “from (Ed)(#59)TDLS Setup Request, or TDLS Setup Response frame” to “from the TDLS Setup Request or TDLS Setup Response frame”.

Proposed resolution:

REVISED

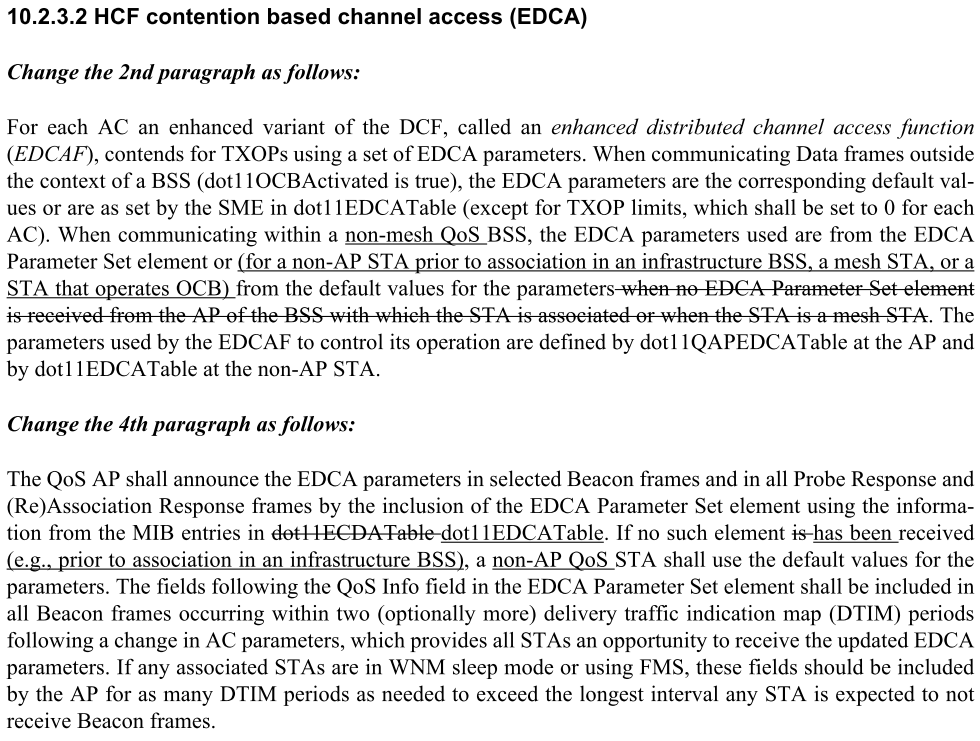
Make the changes shown under “Proposed changes” for CIDs 4353 and 4560 in <this document>, which address the issue raised by the commenter, bringing PBSSes within the same umbrella as other BSSes and extending the description to Management frames transmitted between TDLS peer STAs.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4413  Mark RISON  10.2.3.2  1717.60 | "When communicating within a BSS, the EDCA parameters used are from the EDCA Parameter Set element or  from the default values for the parameters when no EDCA Parameter Set element is received from the AP of  the BSS with which the STA is associated" -- the STA always gets EDCA Params Set from AP in association response, so can't happen | As it says in the comment |
| CID 4703  Mark RISON | There are some places that are poorly worded and suggest the EDCA Parameter Set element is not always provided at association in a QoS BSS | As it says in the comment |

Discussion:

This is apparently a badly worded way of saying “before you’re associated you use the defaults”.

11ax/D6.0 has addressed this:



Proposed resolution:

REVISED

Make the changes shown under CIDs 4413 and 4703 in <this document>, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4501  Mark RISON | "ACM flag" and "ACM bit" should be "ACM subfield", as should "ACM field", for consistency | As it says in the comment |

Discussion:

We don’t have bits or flags, we have fields or subfields. And until we get rid of the pointless distinction between fields and subfields (see CID 4721) we should be calling ACM a subfield, since it’s always something in the context of an AC parameters field.

Proposed resolution:

REVISED

In D3.2:

Change “All ACs with priority higher than that of an AC with an ACM flag equal to 1 should have the ACM flag

set to 1.” at 1839.27 to “All ACs with priority higher than that of an AC for which the ACM subfield is set to 1 should have the ACM subfield set to 1.”

Change “ACM bit” to “ACM subfield” at 1839.30, 2344.2, 4630.54/61, 4631.1/12/14/20/33/41, 4632.1/5/7/17/25/31/35.

Change “ACM field” to “ACM subfield” at page 2424 (8x).

Change “(ACM) bit” to “(ACM) subfield” at 3677.7.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4247  Mark RISON  C.3 | It is meaningless for capability MIB attributes to have defaults | Delete all DEFAULT lines for MIB attributes where the DESCRIPTION says the attribute is a "capability variable" |

Discussion:

As the commenter says, a capability MIB attribute can’t have a default, since by definition it is signalling what the specific implementation is or is not capable of.

Proposed resolution:

REVISED

In D3.2, delete the DEFVAL line for:

dot11TunneledDirectLinkSetupImplemented

dot11TDLSPeerUAPSDBufferSTAActivated

dot11TDLSPeerPSMActivated

dot11TDLSChannelSwitchingActivated

dot11SSPNInterfaceImplemented

dot11MSGCFImplemented

dot11MultibandImplemented

dot11GASExtensionImplemented

dot11RSNAConfigNumberOfSTKSAReplayCounters

dot11LsigTxopProtectionOptionImplemented

dot11PCOOptionImplemented

dot11MeshNbrOffsetMaxNeighbor

dot11DMGOptionImplemented

dot11RelayActivated

dot11TXOPSharingImplicitACKImplemented

dot11S1GSectorTrainingOperationImplemented

dot11ProtectedTWTOperationsImplemented

dot11CDMGOptionImplemented

dot11DynamicChannelTransferImplemented

dot11DynamicChannelTransferActivated

dot11OpportunisticTransmissionsActivated

dot11CDMGSpatialsharingActivated

dot11CDMGClusteringActivated

dot11CMMGMaxMPDULength

dot11CMMGMaxRxAMPDUFactor

dot11CMMGControlFieldOptionImplemented

dot11CMMGTXOPPowerSaveOptionImplemented

dot11CMMGOptionImplemented

dot11CMMGClusteringActivated

dot11ManufacturerID

dot11ProductID

dot11STATransmitPowerClass

dot11CDMGLowPowerSCPHYImplemented

dot11CMMGShortGIOptionImplemented

dot11CMMGTxSTBCOptionImplemented

dot11CMMGRxSTBCOptionImplemented

dot11CMMGBeamFormingOptionImplemented

dot11CMMGMaxNTxChainsImplemented

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4314  Mark RISON  12 | "gives the current message number" (4x) -- the "message number" is not defined | Change "message number" to "TSC or PN" in each case |

Discussion:

Jouni MALINEN has responded to this as follows:

There's already a note describing what the "message number" is for that first GTK case (TSC or PN), so I'm not sure why there would be need to change that "message number".

As far as the IGTK case is concerned, neither PN nor TSC would be correct. BIP calls this IPN.

As far as the BIPN case is concerned, neither PN nor TSC would be correct; it is BIPN. But saying something like "the BIPN field gives the BIPN for the BIGTK" looks pretty pointless. Leaving this as is ("message number") would seem to be better option for this; and likely for the other cases as well. If there is strong need to get rid of the undefined "message number", I would delete the first three sentences as unnecessary description of functionality in Clause 9. I guess I could live with same for the last instance taken into account that sentence is really more of an informative note in that context.

Proposed changes:

In D3.2:

Change 9.4.2.47 Fast BSS Transition element (FTE) as follows:

The RSC field contains the current receive sequence counter (RSC) for the GTK being installed~~. Delivery of the RSC field value~~, to allow~~s~~ a STA to identify replayed MPDUs. If the RSC ~~field value~~ is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the ~~transmit sequence counter (TSC) or packet number (PN)~~ RSC is in the first octet of the RSC field. The RSC for TKIP is the TKIP sequence counter (TSC); for CCMP and GCMP it is the packet number (PN); s~~S~~ee Table 12-8 (Key RSC field).

The IPN field ~~indicates~~contains the current ~~receive sequence counter~~ RSC for the IGTK being installed, to allow a STA to identify replayed protected group addressed robust Management frames. The RSC for an IGTK is the IGTK packet number (IPN).

The BIPN field ~~indicates~~contains the current ~~receive sequence counter~~ RSC for the BIGTK being installed, to allow a STA to identify replayed Beacon frames. The RSC for a BIGTK is the BIGTK packet number (BIPN).

Change 9.4.2.185 Key Delivery element as follows:

The Key RSC field contains the current receive sequence counter (RSC) for the GTK being installed.

Change 9.6.13.19 WNM Sleep Mode Request frame format as follows:

The RSC field contains the current receive sequence counter (RSC) for the GTK being installed~~. The RSC field gives the current message number for the GTK~~, to allow a STA to identify replayed MPDUs. If the RSC ~~field value~~ is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the ~~TSC or PN~~RSC is in the first octet of the RSC field. ***<delete para break>***

~~NOTE—~~The RSC ~~field value~~ for TKIP is the TKIP~~ransmit~~ ~~S~~sequence ~~C~~counter (TSC) ~~and is stored in the first 6 octets~~; for CCMP and GCMP it is the ~~P~~packet ~~N~~number (PN) ~~and is stored in the first 6 octets~~; see Table 12-8 (Key RSC field).

~~The PN field indicates the receive sequence counter for the IGTK being installed.~~ The PN field ~~gives~~contains the current ~~message number~~RSC for the IGTK being installed, to allow a STA to identify replayed ~~MPDUs~~ protected group addressed robust Management frames. The RSC for an IGTK is the IGTK packet number (IPN).

The BIPN field ~~indicates~~contains the current RSC ~~receive sequence counter~~ for the BIGTK being installed~~. The BIPN field gives the current message number for the BIGTK~~, to allow a STA to identify replayed Beacon frames. The RSC for a BIGTK is the BIGTK packet number (BIPN).

Change 12.7.2 EAPOL-Key frames as follows:

g) **Key RSC**. This field is 8 octets in length. It contains the current receive sequence counter (RSC) for the GTK being installed. It is used in message 3 of the 4-way handshake and message 1 of the group key handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. ~~The Key RSC field gives the current message number for the GTK, to allow a STA to identify replayed MPDUs.~~ If the ~~Key~~ RSC ~~field value~~ is less than 8 octets in length, it is stored in the first octets and the remaining octets ~~shall be~~are set to 0. The least significant octet of the ~~TSC or PN should be~~ RSC is in the first octet of the Key RSC field. ~~The encoding of the Key RSC field is defined in~~ The RSC for TKIP is the TKIP sequence counter (TSC); for CCMP and GCMP it is the packet number (PN); see Table 12-8 (Key RSC field).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4314 in <this document>, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4423  Mark RISON | How does a "duration time" or "time duration" differ from a "duration" | Change "duration time" and "time duration" to "duration" throughout |

Discussion:

As it says in the comment.

Proposed changes:

Change the underlined text in the following to “duration”:

* In 9.4.2.21.11 Transmit Stream/Category Measurement report, “If the measured delay has a duration time *t* within Bin *i*”
* In 9.4.2.186 DILS element, “The DILS Duration field contains an unsigned integer that specifies the time duration for the DILS restrictions”
* In 9.4.2.228 Clustering Interference Assessment element, “The Channel Quality Measurement Duration subfield is set to a time duration of directional channel quality measurement”, “The Clustering SPSH Duration subfield is set to a time duration of spatial sharing among BSSs”
* In 9.4.4.2.6 WSM information values, “The Validity field indicates the time duration in minutes for which the Channel Number is available”
* In 10.2.3.2 HCF contention based channel access (EDCA), “The minimum specified idle duration time is not the constant value (DIFS)”, “The minimum idle duration time is assigned either by a management entity or by an AP.”
* In 10.49 Sync frame operation, “a time duration at a TWT defined in the Nominal Minimum TWT Wake Duration field”, “a time duration that is assigned for the STA at a TWT”
* In 11.22.4.2 Location track notification procedures, “shall be separated from the first frame in the previous group of Location Track Notification frames by a minimum time duration indicated by”, “shall be separated from the first frame in the previous group of Location Track Notification frames by a minimum time duration indicated by”
* In 11.22.7.3 BSS transition management request, “might include a time duration after which the non-AP STA will be disassociated”
* In 23.3.7 Mathematical description of signals, “is time duration of the subfield being referenced”
* In 25.3.10 Duplication transmission on a 1080 MHz channel, “*TC* is the SC chip time duration”

Change the underlined text in the following to “Duration”:

* In Figure 9-501—Congestion Notification element format, “Congestion Notification Duration Timer” (4x); note text refers to “four Congestion Notification Duration fields”
* In Figure 9-715—EL Operation element format and 9.4.2.210 EL Operation element, “Recovery Time Duration”

In Table 9-85—Subfields of the Sync Control field change “during a time duration” to “for a duration”.

In 9.4.2.195 S1G Sector Operation element delete “(the sector time duration)”.

In 10.42.7 Beam tracking, “The time duration since the last PPDU it transmitted to the beam tracking responder that requested transmit beam tracking is greater than the beam tracking time limit plus BRPIFS.” change “time duration” to “time”.

In 10.47.1 TWT overview, change “the duration of the AdjustedMinimumTWTWakeDuration time” to “the AdjustedMinimumTWTWakeDuration”.

In 10.47.3 Explicit TWT operation, change “at least Nominal Minimum TWT Wake Duration time” to “a duration of at least Nominal Minimum TWT Wake Duration”.

In 10.47.4 Implicit TWT operation, change “AdjustedMinimumTWTWakeDuration time” to “a duration AdjustedMinimumTWTWakeDuration”.

In 10.53.3 Group sectorization operation, delete “duration” in “their active time duration can overlap”.

In 10.62 Energy limited STAs operation, delete “Time” in “Recovery Time Duration field” (2x) and change “indicate the Recovery Time Duration by including the Recovery Time Duration in the Duration field of an

NDP (PS-Poll-)Ack frame with Idle Indication set to 1” to “indicate the recovery duration in the Duration field of an NDP (PS-Poll-)Ack frame with the Idle Indication field set to 1”.

In 11.10.4 Measurement duration, delete “duration” in “Each separate measurement within the Radio Measurement Request frame shall be performed over a continuous measurement duration time period.”

In C.3, change “This object defines the time duration after the expiration of the GAS Comeback Delay” to “This object defines the time after the expiration of the GAS comeback delay”.

Proposed resolution:

REVISED

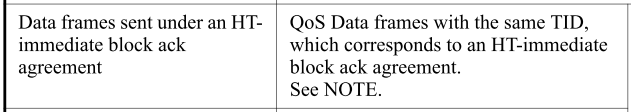
Make the changes shown under “Proposed changes” for CID 4423 in <this document>, which address the issue in the direction suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4717  Mark RISON  10.23.2.7  1834.4 | A figure is needed to illustrate higher-AC TXOP sharing with non-A-MPDUs, since there is considerable subtlety here | Copy Figure 10-27, keep the top unchanged except for making AC\_BE the primary and only having one frame in it, and then show below a sequence where the following are under a "TXOP" arrow: the striped BE frame, an Ack frame, the spotty VO frame, an Ack frame, the lowest VI frame and an Ack frame. At the end of the referenced subclause add "An illustration of TXOP sharing with frames from a higher-priority AC is shown in Figure 10-xx." |
| CID 4718  Mark RISON  10.23.2.7  1834.4 | A figure is needed to illustrate higher-AC TXOP sharing with A-MPDUs, since there is considerable subtlety here | Copy Figure 10-17, keep the top unchanged except for making AC\_BE the primary, and then show below a PPDU containing the two AC\_BE frames to STA-2 and then the AC\_VO frame to STA-2, followed by BA, BAR and BA. At the end of the referenced subclause add "An illustration of TXOP sharing with A-MPDUs is shown in Figure 10-yy." |

Discussion:

As it says in the comments. However, CID 4718 potentially opens a can of worms:

* Table 9-529—A-MPDU contents in the data enabled immediate response context allows a mixture of TIDs if all but one are sent under an HT-delayed BA agreement. We’ve agreed to delete HT-delayed BA, so this is moot.
* Table 9-529—A-MPDU contents in the data enabled immediate response context is not totally clear as to whether you’re allowed a mixture of TIDs all under HT-immediate BA agreements, as long as all but one are sent with Block Ack ack policy:





There was consensus in TGmd that this is not the intent: all the QoS Data frames have to have the same TID and ack policy.

Proposed changes:

Add the figure shown below below Figure 10-27—Illustration of TXOP sharing and PPDU construction and caption it “Figure 10-xx—Illustration of TXOP sharing and PPDU construction (non-A-MPDUs)”:



The Editor is empowered to make the following cosmetic improvements:

* Compress the “Preamble” boxes to be the same height as the boxes for the remainder of the PPDU
* Adjust the remainder of the PPDU boxes to sit exactly on the arrow
* Adjust the spacing between boxes, and the position of the vertical dashed lines, to better match Figure 10-27

Append “ (DL MU-MIMO)” to the caption for Figure 10-27.

Change the last para of 10.3.2.7 as follows:

An illustration of TXOP sharing is shown in Figure 10-27 (Illustration of TXOP sharing and PPDU construction) and Figure 10-xx. ~~In this figure, t~~The AP has frames in queues of three of its ACs. ~~It is assumed that t~~The TXOP was obtained by AC\_VI or AC\_BE, as shown, and is shared by ~~AC\_VO and AC\_BE~~ the other two ACs. ~~It is also assumed that these~~ The frames ~~are~~ target~~ing~~ three STAs, STA-1 to STA-3.

Proposed resolution for CID 4717:

REVISED

Make the changes shown under “Proposed changes” for CID 4717 in <this document>, which add the figure requested by the commenter.

Proposed resolution for CID 4718:

REJECTED

Table 9-529—A-MPDU contents in the data enabled immediate response context indicates that you cannot have Data frames with different TIDs in an A-MPDU. It is therefore not possible to have higher-AC TXOP sharing with(in) A-MPDUs.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4178  Mark RISON | A BSSID is a characteristic of a BSS, not of an AP/STA. So "BSSID of" should not refer to an an AP/STA | As it says in the comment |
| CID 4575  Mark RISON | Is it BSSID of the AP or BSSID of the AP's BSS? | As it says in the comment |
| CID 4576  Mark RISON | Just "BSSID" is often used for infraBSS, but for IBSS it's generally qualified as "BSSID of the IBSS" -- why? | As it says in the comment |

Discussion:

As its name indicates, a BSSID is a characteristic of a BSS. It is not a characteristic, per se, of an AP (although the AP’s MAC address is typically the BSSID) or of a frame (though many frames carry a BSSID).

Also, non-AP STAs associate to an AP. STAs are members of BSSes.

Proposed changes:

In D3.2:

In 4.3.11.4 Frame, change “BSSID of the transmitter” to “BSSID indicated by the transmitter”.

In 9.4.2.21.18 Fine Timing Measurement Range report, change “the BSSID of the AP” to “the BSSID of the BSS of the AP” (2x).

In 9.4.2.36 Neighbor Report element, delete “Each Report element describes an AP and consists of BSSID, BSSID Information, Channel Number, Operating Class, PHY Type, and optionally includes optional subelements.(M101)”. At the start of the first para add “The Neighbor Report element describes an AP.”

In 9.4.2.61 Link Identifier element, change “The BSSID field is set to the BSSID of the BSS to which the TDLS initiator STA is associated.” to “The BSSID field is set to the BSSID of the BSS of which the TDLS initiator STA is a member.”

In 9.4.2.204 S1G Relay element, change “the BSSID of the parent AP” to “the BSSID of the parent AP’s BSS”.

In 9.4.2.208 AID Announcement element, change “the BSSID of the relay AP” to “the BSSID of the relay AP’s BSS”.

In 9.4.5.24 Query AP List ANQP-element, change “the BSSID of an AP that” to “the BSSID of the BSS of an AP that”.

In 9.4.5.25 AP List Response ANQP-element, change “the BSSID of the AP that” to “the BSSID of the BSS of the AP that”.

In 10.3.2.9 CTS and DMG CTS procedure, change “the PBSSID of the AP with which the non-AP STA is associated” to “the PBSSID of the BSS of which the non-AP STA is a member”.

In 10.3.2.11 Acknowledgment procedure, change “BSSID of the (#1261)parent AP” to “BSSID of the (#1261)parent AP’s BSS” (2x).

In 10.23.3.4 NAV operation of a TXOP under HCCA, change “the BSSID of the BSS in which the STA is

associated” to “the BSSID of the BSS of which the STA is a member”.

In 10.52.2 Aperiodic SST operation, change “the BSSID of the BSS with which the STA is associated” to “the BSSID of the BSS of which the STA is a member”.

In 10.53.5.1 Introduction and 10.53.5.2 Procedure, change “the partial BSSID of the AP” to “the partial BSSID of the AP’s BSS”.

In 10.54.5.3 Implicit Ack procedure, change “the BSSID of the S1G relay AP” to “the BSSID of the S1G relay AP’s BSS”.

In 10.54.5.3 Implicit Ack procedure, change “BSSID of the (#1261)parent AP to which the S1G relay STA of the S1G relay is associated” to “BSSID of the BSS of the (#1261)parent AP with which the S1G relay STA of the S1G relay is associated”.

In 11.1.4.3.11 Enhanced FILS active scanning to preferred AP, change “the BSSID of the AP” to “the BSSID of the AP’s BSS”.

In 11.1.4.3.11 Enhanced FILS active scanning to preferred AP, change “the BSSID of this AP” to “the BSSID of this AP’s BSS”.

In 11.2.3.1 General, change “the partial BSSID of its associated AP is equal to the partial BSSID of at least another AP (i.e., the other AP and the associated AP have a different BSSID)” to “the partial BSSID of the BSS of which it is a member is equal to the partial BSSID of another BSS”.

In 11.2.7.4 ATIM frame usage for power management of non-AP STAs, change “the BSSID of the BSS of the STA is a member” to “the BSSID of the BSS of which the STA is a member”.

In 11.3.3 Frame filtering based on STA state, change “the BSSID of the BSS with which STA A is associated” to “the BSSID of the BSS of which STA A is a member”; “a member of the BSS with which STA A is associated” to “a member of the BSS of which STA A is a member”.

In 11.10.15.3 Measurement pilot usage by a STA, change “the BSSID of the Measurement Pilot frame” to “the BSSID field of the Measurement Pilot frame”.

In 11.21.4 TDLS direct-link establishment, change “match the BSSID of the TDLS responder STA” to “match the BSSID of the BSS of which the TDLS responder STA is a member”.

In 11.29.2 Peer Service Discovery, change “the BSSID of the AP or PCP” to “the BSSID of the AP’s or PCP’s BSS”.

In 11.36.3 Procedure at the responder AP, change “the BSSID of the AP” to “the BSSID of the AP’s BSS”.

In 12.6.10.2 Preauthentication and RSNA key management, change “with the DA being the BSSID of a targeted AP and the RA being the BSSID of the AP with which it is associated” to “with the DA being the BSSID of a targeted AP’s BSS and the RA being the BSSID of the BSS of which it is a member”.

In 12.7.1.6.5 PTK, change “BSSID is the BSSID of the target AP” to “BSSID is the BSSID of the target AP’s BSS”. Note to the Editor: this change is also made under CID 4179.

In 12.7.8.2 TPK handshake, change “the BSSID of the current association of the TDLS initiator STA” to “the BSSID of the BSS of which the TDLS initiator STA is a member”.

In 12.11.2.6.2 (Re)Association Request for FILS key confirmation and 12.11.2.6.3 (Re)Association Response for FILS key confirmation, change “AP-BSSID is the BSSID of the AP” to “AP-BSSID is the BSSID of the AP’s BSS”.

In 13.5.2 Over-the-air FT protocol authentication in an RSN (2x), 13.5.3 Over-the-DS FT protocol in an RSN (2x), 13.5.4 Over-the-air FT protocol in a non-RSN (2x), 13.5.5 Over-the-DS FT protocol in a non-RSN (2x), 13.6.2 Over-the-air fast BSS transition with resource request (2x), 13.6.3 Over-the-DS fast BSS transition with resource request (2x), 13.7.1 FT reassociation in an RSN (2x), 13.7.2 FT reassociation in a non-RSN (2x), 13.10.1 Overview, 13.10.2 Remote request broker (RRB), change “the BSSID of the target AP” to “the BSSID of the target AP’s BSS”. Note to the Editor: these changes are also made under CID 4179.

In 13.10.3 Remote Request/Response frame definition, change “the BSSID of the current AP” to “the BSSID of the current AP’s BSS”.

In 23.3.12.2.1.1 NDP\_1M CTS, 23.3.12.2.1.2 NDP\_2M CTS, change “the partial BSSID of the AP transmitting” to “the partial BSSID of the BSS of the AP transmitting”; “the partial BSSID of the receiving AP” to “the partial BSSID of the receiving AP’s BSS”; “the partial BSSID of the transmitting AP” to “the partial BSSID of the BSS of the transmitting AP”.

In 23.3.12.2.7.1 NDP\_2M Beamforming Report Poll, change “the partial BSSID of the AP” to “the partial BSSID of the AP’s BSS”.

In C.3, change “the BSSID of the particular AP” to “the BSSID of the BSS of the particular AP” and “on any AP(s)” to “on the BSS(s) of any AP(s)” in the same para; “BSSID of the STA that transmitted” to “BSSID of the BSS of the STA that transmitted”; “the BSSID of the AP” to “the BSSID of the BSS of the AP” (2x).

In L.3 Sample C code change “BSSIDs per AP” to “BSSIDs in a multiple BSSID set”.

Change “AP’s BSSID” to “AP’s BSS’s BSSID” throughout (11x).

In 9.3.2.1.2 Address and BSSID fields, change “the address of the STA contained in the PCP of the PBSS” to “the address of the STA contained in the PCP” and “the BSSID is the BSSID of the IBSS” to “the BSSID is that selected by the STA that started the IBSS”.

In 9.3.3.1 Format of Management frames, 9.4.2.67.4 Peer-to-peer link event report, C.3 MIB detail, change “the BSSID of the IBSS” to “the BSSID” (2x).

In 9.4.2.138 Multi-band element, delete “If the STA Role subfield is set to IBSS STA, the BSSID subfield contains the BSSID of the IBSS.” (duplicates “The BSSID field specifies the BSSID of the BSS operating on the channel and frequency band indicated by the Channel Number and Band ID fields.” later on).

In 9.4.2.145 Session Transition element, change “the MAC address of the BSSID of the IBSS” to “the BSSID”.

Proposed resolution for CIDs 4178, 4575, 4576:

REVISED

Make the changes shown under “Proposed changes” for CIDs 4178, 4575, 4576 in <this document>, which address the issue in the direction suggested by the commenter.

Note to the Editor: various instances of “BSSID of the [something] frame” were addressed under CID 4177 in 20/0272. They do not appear above (the fixes had been applied by D3.2, per the #4177 tags).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4746  Mark RISON  11.13 | "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" -- this should be in the clauses dealing with receipt of a Deauthentication/Disassociation frame | As it says in the comment |

Discussion:

All the stuff about deauth/disassoc is in Subclause 11.3 … except for this requirement buried here.

Proposed changes:

In D3.2:

In 11.13 delete the following para:

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 might 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 responds to the SA Query request with a valid SA Query response, the non-AP STA should continue to use the SA. If no valid SA Query response is received, the non-AP and non-PCP STA’s SME may delete the SA and temporal keys held for communication with the STA by issuing an MLME-DELETEKEYS.request primitive and the non-AP and non-PCP STA may move into State 1 (or State 2, for a DMG STA) with the AP.

Change 11.3.4.5 Deauthentication—destination STA as follows:

A DMG STA in State 2, State 3 or State 4 that receives a Deauthentication frame shall remain in the same state if it did not perform an IEEE 802.11 authentication exchange.

Otherwise, upon receipt of a Deauthentication frame from a STA for which the state is State 2, State 3, or State 4, the destination STA shall deauthenticate with the originating STA using the following procedure:

a) If management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection is in use and the frame is not discarded per management frame protection processing, the MLME shall issue an MLME-DEAUTHENTICATE.indication primitive to inform the SME of the deauthentication~~, and set the state for the originating STA to State 1~~.

a2) If management frame protection is in use, the state for the STA is 4, the STA has a valid security association, the frame is from the AP or PCP the STA is associated with, the frame is not protected and the reason code is INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME, the MLME shall issue an MLME-DEAUTHENTICATE.indication primitive to inform the SME of the deauthentication.

b) Upon receiving an MLME-DEAUTHENTICATE.indication primitive, the SME shall

0) If the state for the STA is 4, the STA has a valid security association, the STA has negotiated management frame protection, the frame is from the AP or PCP the STA is associated with, and the reason code is INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME, 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 as follows:

i) The SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA every dot11AssociationSAQueryRetryTimeout TUs until an MLME-SA-QUERY.confirm primitive for the STA is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. The SME shall increment the TransactionIdentifier by 1 for each MLME-SA-QUERY.request primitive, rolling it over the value to 0 after the maximum allowed value is reached.

ii) If a MLME-SA-QUERY.confirm primitive for the STA, or an MSDU from the AP or PCP, is received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall ignore the MLME-DEAUTHENTICATE.indication primitive and not proceed with the steps below.

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

0b) The MLME shall set the state for the originating STA to State 1.

TBD: Ditto for Disassoc frames

Proposed resolution:

REVISED

Add the following NOTE to the end of Subclause 11.13:

NOTE—The mechanism by which the MAC, MLME and SME coordinate the actions needed

to effect the operations described in this subclause is outside the scope of this standard.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4137  David Goodall  23.3.8.2.2.5  3370.6 | Why is bit 0 of the SIG-1 symbol of the short preamble reserved and set to 1 rather than 0? Is it reserved for future use or is it reserved for some other reason? If it will always be the value 1 then we can use it to further verify the short preamble signal field, which is protected by a weak CRC4. | Add a note saying why b0 of the S1G-1 symbol of the short preamble is reserved. |

Discussion:

As the commenter indicates, the intent of reserved fields is to allow for forward compatibility: new information can be signalled in the field in the future, but existing implementations will be unaffected as they are directed to ignore it. This is distinct from fields that have a fixed value, that existing implementations are directed to validate.

There is a tricky case for b4 of the OFDM PHY SIGNAL field (often referred to as “L-SIG” in PHYs that build on it). This is described as reserved, but implementations are known to validate it as a means to strengthen the poor validation offered by the single parity bit (b17). So this bit should be described as fixed, but should not explicitly be stated to be validated by the receiver. Note that the situation is different for the SERVICE field, where it is explicitly stated that “All reserved bits shall be set to 0 on transmission and ignored on reception.”, i.e. the canonical definition of reserved bits.

Similarly DMG uses the canonical definition (“Reserved bits are set to 0 by the transmitter and shall be ignored by the receiver.” in 20.4.3.2.1 General and 20.5.3.1.1 General) as do CDMG and CMMG.

The status of the “Reserved” bit in the SERVICE field for VHT is not clear: it is specified to be set to 0 in Table 21-16—SERVICE field but not specified to be validated on receive. Ditto for the “Reserved” bits in VHT-SIG-B. [The wording is “Reserved VHT-SIG-A Indication is defined as a VHT-SIG-A with Reserved bits equal to 0”.]

Proposed changes:

In D3.0:

*[Clause 23 = S1G]*

In 23.3.4.2.3 Construction of SIG-A and 23.3.4.2.6 Construction of SIG-B and 23.3.4.3.3 Construction of SIG and 23.3.4.4.3 Construction of 1 MHz SIG change “the reserved bits” to “the fixed bits”.

In Figure 23-7—SIG-1 structure change “Reserved” (vertical, under B0) to “Fixed”.

In Table 23-11—Fields in the SIG field of short preamble, in the row for B0

change "Reserved" / "Reserved. Set to 1." to "Fixed" / "Set to 1".

In Figure 23-12—SIG-A2 structure for SU PPDU change “Reserved” (vertical, under B12) to “Fixed”.

In Figure 23-13—SIG-A1 structure for MU PPDU change “Reserved” (vertical, under B2) to “Fixed”.

In Figure 23-14—SIG-A2 structure for MU PPDU change “Reserved” (vertical, under B1) to “Fixed”.

In Table 23-13—Fields in the SIG-A field of S1G\_LONG preamble SU PPDU, in the row for B12

change "Reserved" / "Reserved. Bit set to 1." to "Fixed" / "Set to 1".

In Table 23-14—Fields in the SIG-A field of S1G\_LONG preamble MU PPDU, in the rows for B2 in SIG-A1 and B1 in SIG-A2

change "Reserved" / "Reserved. Bit set to 1." to "Fixed" / "Set to 1"

and in the row for B20-23 change “is reserved” to “is fixed” (4x).

In Table 23-16—Fields in the SIG-B field for MU PPDU change “Reserved” to “Fixed”.

In 23.3.8.2.3.3.6 CRC calculation for SIG SIG-B field change “Reserved field” to “Fixed field” (2x) and change the heading to “CRC calculation for S1G SIG-B field”.

In Figure 23-16—Structure of the 6 symbol SIG field of S1G\_1M PPDU change “Reserved” to “Fixed” (vertical, under B6).

In Table 23-18—Fields in the SIG field of S1G\_1M PPDU, in the row for B6 in SIG-2

change "Reserved" / "Reserved. Set to 1." to "Fixed" / "Set to 1".

In Table 23-19—SERVICE field change “Reserved” to “Fixed”.

In 23.3.19 PHY receive procedure change "Reserved bits equal to 0" to "any Fixed field equal to 0".

and at the end of the para referring to “Reserved SIG-B Indication” add “Invalid SIG-B Indication is defined as a SIG-B with the Fixed field not all-1s or an S1G-MCS not included in 23.5 (Parameters for S1G-MCSs).”

In 23.3.19 PHY receive procedure change “Reserved SIG or SIG-A Indication” to “Invalid SIG or SIG-A Indication” (3x), “Reserved SIG-A Indication” to “Invalid SIG-A Indication”, “an SIG” to “a SIG”.

*[Clause 17 = OFDM]*

In 17.3.2.1 General change “reserved bit” to “fixed bit” (2x).

In Figure 17-1—PPDU format, Figure 17-17—Transmit PHY, Figure 17-18—PHY transmit state machine, Figure 17-19—Receive PHY, change “Reserved” to “Fixed”.

In 17.3.4.1 General change “Bit 4 shall be reserved for future use.” to “Bit 4 is fixed.”

In Figure 17-5—SIGNAL field bit assignment change “R” to “F” above “4”.

In 17.3.4.4 Parity (P), Reserved (R), and SIGNAL TAIL fields change “Reserved (R)” to “Fixed (F)” in the caption and in the body change “Bit 4 is reserved. It shall be set to 0 on transmit and ignored on receive.” to “Bit 4 is fixed. It shall be set to 0 on transmit.”

*[Clause 19 = HT]*

In 19.3.9.3.5 L-SIG definition change “reserved bit” to “fixed bit”.

In Figure 19-5—L-SIG structure change “R” to “F” above “4”.

In Table 19-11—HT-SIG fields change "Reserved" to "Fixed".

In Figure 19-6—Format of HT-SIG1 and HT-SIG2 change “Reserved” to “Fixed” (above “2” in HT-SIG2).

In 19.3.21 PHY receive procedure change "Reserved field = 0" to "Fixed field = 0" and “Reserved HT-SIG Indication” to “Invalid HT-SIG Indication” (9x).

*[Clause 21 = VHT]*

In 21.3.4.5 Construction of VHT-SIG-A and 21.3.4.8 Construction of VHT-SIG-B change “the reserved bits” to “the fixed bits”.

In 21.3.8.2.4 L-SIG definition change “The Reserved (R) field” to “The Fixed (F) field”.

In Figure 21-18—VHT-SIG-A1 structure change “Reserved” (2x vertical under B2 and B23) to “Fixed”.

In Figure 21-19—VHT-SIG-A2 structure change “Reserved” (3x inc. 1x vertical under B9) to “Fixed”.

In Table 21-12—Fields in the VHT-SIG-A field

change “Reserved” / “Reserved. Set to 1.” to “Fixed” / “Set to 1” in the row for B2 in VHT-SIG-A1

and change “The bit is reserved and set to 1” to “The bit is fixed and set to 1” in the row for B22 in VHT-SIG-A1

and change “Reserved” to “Fixed” in the row for B23 in VHT-SIG-A1

and change “this field is reserved and set to 1” to “this field is fixed and set to 1” in the row for B2 in VHT-SIG-A2

and change “is reserved and set to 1” to “is fixed and set to 1” (4x) in the row for B4-B7 in VHT-SIG-A2

and change “Reserved and set to 1” to “Fixed and set to 1” in the row for B8 in VHT-SIG-A2

and change “Reserved” / “Reserved and set to 1” to “Fixed” / “Set to 1” in the row for B9 in VHT-SIG-A2.

In Table 21-14—Fields in the VHT-SIG-B field change “Reserved” to “Fixed”.

In Table 21-16—SERVICE field and Figure 21-23—VHT-SIG-B and SERVICE field relationship change “Reserved” to “Fixed”.

In 21.3.20 PHY receive procedure change "Reserved bits equal to 0" to "any Fixed field equal to 0" and change “Reserved VHT-SIG-A Indication” to “Invalid VHT-SIG-A Indication” (3x).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4137 in <this document>, which make a distinction between reserved fields, which are ignored by the receiver, and fixed fields, which are checked by the receiver and typically cause the PPDU to be rejected if they do not have the expected value.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4277  Mark RISON | We have all of "BA session" (4x), "block ack session" (17x), "BlockAck session" (4x) (and none are defined) | Change all to "block ack session" and define the term |

Discussion:

On 2020-06-29 the group confirmed a preference for “block ack session”.

Note a difference between NDP\_1M BlockAck and NDP\_2M BlockAck:

Up to 8 MSDUs and A-MSDUs when the NDP BlockAck is used during a BlockAck session. Each bit that is equal to 1 in the NDP BlockAck bitmap acknowledges the (#2604)reception of a single MSDU or A-MSDU in the order of sequence number, with the first bit of the NDP BlockAck bitmap corresponding to the MSDU or A-MSDU with the sequence number that matches the value of the Starting Sequence Control field.

v.

Up to 16 MSDUs and A-MSDUs . Each bit that is equal to 1 in the NDP BlockAck bitmap acknowledges the (#2604)reception of a single MSDU or A-MSDU in the order of sequence number, with the first bit of the NDP BlockAck bitmap corresponding to the MSDU or A-MSDU with the sequence number that matches the value of the Starting Sequence Control field.

There is no clear reason for this difference, so it is assumed to be accidental.

More digging suggests the concept of a “block ack session” was introduced by S1G. The normal terminology is about block ack agreements.

Re “fragment BA session”, the normal terminology is to talk of the “fragment BA procedure”.

Proposed changes:

In D3.2:

Change “BlockAck session” to “block ack agreement” in 9.6.4.1 General, 23.3.12.2.6.1 NDP\_1M BlockAck (2x) and 23.3.12.2.6.2 NDP\_2M BlockAck.

In 23.3.12.2.6.2 NDP\_2M BlockAck, change “Up to 16 MSDUs and A-MSDUs.” to “Up to 16 MSDUs and A-MSDUs when the NDP BlockAck is used during a block ack agreement.”

In 11.5.2.2 Procedure at the originator, change “shall set up the Block Ack” to “shall set up the block ack agreement”.

In 11.5.2.3 Procedure at the recipient, change “support Block Ack initialization and modification” to “support block ack agreement set up and modification”.

Change “block ack session” to “block ack agreement” in 10.25.2 Setup and modification of the block ack parameters (5x), 10.25.5 Selection of BlockAck and BlockAckReq variants (3x), 10.25.6.7 Originator’s behaviour (6x), 11.5.2.2 Procedure at the originator (3x).

Change “during a fragment BA session” to “in a fragment BA procedure” in 23.3.12.2.6.1 NDP\_1M BlockAck (2x), 23.3.12.2.6.2 NDP\_2M BlockAck (2x).

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4277 in <this document>, which use “block ack agreement” throughout.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4286  Mark RISON | It is not clear what the difference between 802.1X authentication and EAP authentication is. Jouni said "In the context of IEEE 802.11 standard, 802.1X authentication is really referring to EAP authentication, so these would also be interchangeable here" | Change "EAP authentication" to "802.1X authentication" throughout, except in the definition of IEEE 802.1X authentication and Extensible Authentication Protocol (EAP) reauthentication protocol (EAP-RP) and in the arrow label in Figure 4-31--IEEE 802.1X EAP authentication and Figure 4-37--Example using IEEE 802.1X authentication. Delete "EAP" in the caption of Figure 4-31--IEEE 802.1X EAP authentication and in Table 9-198--Transition and Transition Query reasons and in last para of 12.6.10.3 Cached PMKSAs and RSNA key management. Change "Successful completion of EAP authentication over IEEE Std 802.1X" to "Successful completion of IEEE Std 802.1X authentication" and "full EAP authentication via IEEE 802.1X authentication." to "full IEEE 802.1X authentication." |

Discussion:

As it says in the comment.

Proposed changes:

In D3.2:

Change “EAP authentication” to “802.1X authentication” in 12.6.1.1.2 PMKSA, 13.2.2 Authenticator key holders, 13.2.3 Supplicant key holders, 13.9.2.2 R0KH state machine states, 13.9.3.3 R1KH state machine variables, 13.9.4.2 S0KH state machine states, C.3 (for dot11FTR0KeyLifetime),

In 12.2.5 RSNA assumptions and constraints change “EAP authentication methods” to “EAP methods”.

Change “apFailedIeee8021XEapAuthentication” to “apFailedIeee8021XAuthentication” in C.3 (3x).

In 12.6.10.2 Preauthentication and RSNA key management change “EAP authentication over IEEE Std 802.1X” to “802.1X authentication”.

In 12.6.10.3 and Table 9-198—Transition and Transition Query reasons and Figure 4-31—IEEE 802.1X EAP authentication caption change “IEEE 802.1X EAP authentication” to “802.1X authentication”.

In 12.11.2.3.5 Non-AP STA processing of Authentication frame change “full EAP authentication via IEEE 802.1X authentication” to “full 802.1X authentication”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4286 in <this document>, which

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4394  Mark RISON | There are ~11 instances of "current ESS", but this is not defined | As it says in the comment |
| CID 4395  Mark RISON | There are ~11 instances of "current ESS", but this is not defined | Change each to "ESS of which the STA is a member" (if you accept STAs can be members of an ESS, not just of a BSS) |

Discussion:

Mark HAMILTON has confirmed that:

I think the one thing that ARC has agreed in this area, is that an ESS is a set of BSSs. That is pretty black-and-white in the definitions, and is consistent with all our discussions about “What is an ESS?”

So, since a STA is a member of a BSS, it is by inheritance, also a member of an ESS.

Proposed resolution for CID 4394 and 4395:

REVISED

Change “current ESS” to “ESS of which the transmitting STA is a member” in 9.6.6.6 Neighbor Report Request frame format, 11.22.2.2 Transition event request and report, 11.22.2.3 RSNA event request and report.

Delete “current” in “current ESS” in 11.10.10.3 Responding to a neighbor report request.

Change “current ESS or IBSS” to “ESS or IBSS of which the transmitting STA is a member” in 11.22.2.1 Event request and event report, 11.22.2.4 Peer-to-peer link event request and report.

In 11.22.3.2 Configuration Profile report change “The Configuration Profile report enables an AP to discover the current profile in use for an associated device, and additional profiles for the current ESS.” to “The Configuration Profile report enables an AP to discover the current profile in use for an associated STA, and additional profiles for the ESS of which the STA is a member.” and change “Devices that support multiple configuration profiles for an ESS may include multiple Diagnostic Report elements in a single Diagnostic Report frame (or multiple frames if required). Each Diagnostic Report element shall contain a Profile ID element that uniquely identifies the configuration profile(s) for the current ESS that are available on the device.” to “STAs that support multiple configuration profiles for an ESS may include multiple Diagnostic Report elements in a single Diagnostic Report frame (or multiple frames if required). Each Diagnostic Report element shall contain a Profile ID element that uniquely identifies the configuration profile(s) for the ESS of which the STA is a member that are available on the device.”

In 11.22.7.3 BSS transition management request change “any BSSID in the current ESS” to “any BSSID in the ESS of which it is a member”.

In 12.6.10.1 General change “the current ESS” to “the ESS of which the STA is a member” (2x).

In 11.22.3.3 Manufacturer information STA report change “STA device” to “STA”.

In 23.3.18.5.2 Type 1 and type 2 channelization for CCA levels change “the AP and non-AP STA devices” to “STAs” (2x).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4696  Mark RISON  9 | Do not duplicate length information given in figures in text (e.g. "is x bits/octets in length", "is an x-bit/octet field") | As it says in the comment |

Discussion:

The figures in Clause 9 are normative. There is no value in duplicating the information they provide in text; this is waffle that merely presents an opportunity for spec rot.

Proposed resolution:

REVISED

In D3.3:

Delete “is 1 bit in length and ” in 9.2.4.1.5 More Fragments subfield, 9.2.4.1.6 Retry subfield, 9.2.4.1.7 Power Management subfield, 9.2.4.1.8 More Data subfield, 9.2.4.5.3 EOSP (end of service period) subfield, 9.2.4.5.9 A-MSDU Present subfield, 9.2.4.5.11 Mesh Power Save Level subfield, 9.2.4.5.13 A-MSDU Type subfield, 9.2.4.6.2 HT variant, 9.4.1.17 QoS Info field, 9.4.2.120 Intra-Access Category Priority element.

Delete “is 1 bit in length, and ” in 9.2.4.5.10 Mesh Control Present subfield.

Delete “is 1 bit in length. It ” in 9.4.2.108.2 MCCAOP Advertisement Element Information field (3x).

Delete “is 3 bits in length and ” in 9.4.2.243 MSCS Descriptor element.

Delete “is 1 octet in length and ” in 9.2.4.7.3 Mesh Control field (2x), 9.4.1.17 QoS Info field, 9.4.1.23 SM Power Control field, 9.4.1.30 Antenna Selection Indices field, 9.4.1.45 Band ID field, 9.4.2.5.2 Block Bitmap mode, 9.4.2.5.4 OLB mode, 9.4.2.30 TCLAS element, 9.4.2.34 QoS Capability element, 9.4.2.105.2 MCCAOP Reservation field (2x), 9.4.2.107 MCCAOP Advertisement Overview element, 9.4.2.108.1 General (2x), 9.4.2.119 Quality-of-Service Management Frame Policy element, 9.4.2.170.2 Neighbor AP Information field (4x), 9.4.2.177 FILS Request Parameters element (2x), 9.6.7.22 HCCA TXOP Advertisement frame (2x), 9.6.7.36 FILS Discovery frame format (2x).

Delete “is 1 octet in length. It ” in 9.6.7.36 FILS Discovery frame format.

Delete “is 2 octets in length and ” in 9.4.2.107 MCCAOP Advertisement Overview element, 9.4.2.137 Awake Window element, 9.6.7.36 FILS Discovery frame format.

Delete “is 2 octets in length, and ” in 9.4.2.55.2 HT Capability Information field.

Delete “is 4 octets in length and ” in 9.2.4.7.3 Mesh Control field, 9.4.1.32 Rate Identification field, 9.4.2.36 Neighbor Report element.

Delete “is 4 octets in length, and ” in 9.4.2.243 MSCS Descriptor element.

Delete “is 6 octets in length and ” in 9.4.1.26 MIMO Control field.

Delete “is 6 or 12 octets in length and ” in 9.2.4.7.3 Mesh Control field.

Delete “is 8 octets in length and ” in 9.3.1.8.2 Compressed BlockAck variant, 9.3.1.8.4 Extended Compressed BlockAck variant, 9.3.1.8.5 GCR Block Ack variant, 9.3.1.8.6 GLK-GCR BlockAck variant.

Delete “is 3–255 octets in length and ” in 9.4.2.30 TCLAS element.

Delete “and is 1 octet in length” in 9.4.1.19 Max Transmit Power field, 9.4.1.20 Transmit Power Used field.

Delete “and is 1 octet in length,” in 9.6.6.4 Link Measurement Request frame format.

Delete “The Protected Frame subfield is 1 bit in length.” in 9.2.4.1.9 Protected Frame subfield.

In 9.2.4.1.10 +HTC(#66) subfield change “The +HTC(#66) subfield is 1 bit in length. The setting of the (Ed)subfield is as follows(11ah):” to “The +HTC subfield is set as follows:”.

In 9.2.4.5.12 Receiver Service Period Initiated (RSPI) subfield change “The Receiver Service Period Initiated (RSPI) subfield is 1 bit in length. The subfield is set to 0 to indicate” to “The Receiver Service Period Initiated (RSPI) subfield is set to 0 to indicate”.

Delete “The PSMP Parameter Set field is 2 octets in length.” in 9.4.1.24 PSMP Parameter Set field, and change the size of the middle field in Figure 9-108—PSMP Parameter Set (#2401)field format(#2607) from 6 to 1.

Delete “The Block Bitmap subfield is 1 octet in length.” in 9.4.2.5.2 Block Bitmap mode.

In 9.4.2.8 Country element change “The Country String field is 3 octets in length. The AP and mesh STA set this field to” to “The AP and mesh STA set the Country String field to”, delete “The Number of Channels subfield of the subelement is 1 octet in length.”, change “The Maximum Transmit Power Level field is a signed number and is 1 octet in length” to “The Maximum Transmit Power Level field is a 2s complement signed integer”, delete “The Operating Class field is 1 octet in length.”, delete “The Coverage Class field is 1 octet in length.”, delete “The Padding field is 0 or 1 octet in length.”.

Delete “(1)” in Figure 9-334—QoS Capability element format.

In 9.4.2.108.3 MCCAOP Reservation Report field change “Each MCCAOP Reservation field is 5 octets in length and its format is shown” to “The format of each MCCAOP Reservation field is shown”.

In 9.4.2.119 Quality-of-Service Management Frame Policy element change:

The Individually Addressed subfield (I) is 1 bit in length. When the QACM applies to individually addressed Management frames, (MDR2)the Individually Addressed subfield is set to 1. Otherwise, it is 0.

The Group Addressed subfield (G) is 1 bit in length. When the QACM applies to group addressed Management frames, (MDR2)the Group Addressed subfield is set to 1. Otherwise, it is 0.

to

When the QACM applies to individually addressed Management frames, (MDR2)the Individually Addressed (I) subfield is set to 1. Otherwise, it is 0.

When the QACM applies to group addressed Management frames, (MDR2)the Group Addressed (G) subfield is set to 1. Otherwise, it is 0.

In 9.4.2.170.2 Neighbor AP Information field change “The Filtered Neighbor AP subfield is 1 bit in length. (11ai)When included in a Probe Response frame, it is” to “When included in a Probe Response frame, the Filtered Neighbor AP subfield is”.

In 9.4.2.181 AP Configuration Sequence Number (AP-CSN) element change “The AP-CSN field is 1 octet in length and is defined as an unsigned integer. The AP-CSN contains” to “The AP-CSN field contains”.

In 9.4.2.186 DILS element change “The MAC Address Filter field is 1 octet in length as shown in” to “The MAC Address Filter field is defined in”.

In 9.4.2.243 MSCS Descriptor element change “The User Priority Bitmap subfield is (Ed)1 octet in length. Each bit in the bitmap corresponds” to “Each bit in the User Priority Bitmap subfield corresponds”.

In 9.4.5.24 Query AP List ANQP-element change “The BSSID field is 6 octets in length” to “Each BSSID field is 6 octets in length”.

In 9.7.1 A-MPDU format delete “The MPDU delimiter is 4 octets in length.”

In 12.3.2.2 WEP MPDU format delete “The WEP ICV field shall be 32 bits in length. The expanded frame body shall start with a 32-bit IV field. This field shall contain three subfields: a 3-octet subfield that contains the IV, a 2-bit Key ID subfield, and a 6-bit Pad subfield.”

In 12.7.2 EAPOL-Key frames delete “is 1 octet and”, “is 2 octets and”, “2 octets in length,”, “is 8 octets,”, “is 32 octets. It”, “is 16 octets. It”, “is 8 octets in length. It”, “2 octets in length, taken to represent”.

In 9.2.4.3.4 BSSID field delete “a 48-bit field”.

In 9.2.4.4.2 Sequence Number field change “is a 12-bit field indicating” (2x) and “is a 10-bit subfield indicating” and “is a 2-bit subfield indicating” to “indicates”.

In 9.2.4.4.3 Fragment Number field change “is a 4-bit field indicating” to “indicates”.

In 9.2.4.5.1 QoS Control field structure delete “is a 16-bit field that”.

In 9.2.4.5.5 TXOP Limit subfield, 9.2.4.5.6 Queue Size subfield, 9.2.4.5.7 TXOP Duration Requested subfield, 9.2.4.5.8 AP PS Buffer State subfield delete “is an 8-bit field that”.

In 9.2.4.8 FCS field change “is a 32-bit field containing” to “contains”.

In 9.4.2.21.10 LCI report (Location configuration information report) delete “a 2-bit field”.

In 9.4.2.51 DSE Registered Location element delete “a 3-bit field” and “a 2-bit field” and “a 16-bit field with”.

In 9.4.5.10 NAI Realm ANQP-element delete “is a 1-bit subfield. It”.

In 15.3.3.2 PHY SYNC field, 16.2.3.2 Long PHY SYNC field delete “128 bits of”.

In 15.3.3.3 PHY SFD, 16.2.3.3 Long PHY SFD delete “a 16-bit field,”.

In 15.3.3.4 PHY SIGNAL field, 15.3.3.5 PHY SERVICE field, 16.2.3.4 Long PHY SIGNAL field, 16.2.3.11 Short PHY SIGNAL field (shortSIGNAL) delete “8-bit”.

In 15.3.3.6 PHY LENGTH field, 16.2.3.6 Long PHY LENGTH field delete “16-bit”.

In 16.2.3.9 Short PHY synchronization (shortSYNC) delete “56 bits of”.

In 16.2.3.10 Short PHY SFD field (shortSFD) delete “a 16-bit field and be”.

In 9.4.5.10 NAI Realm ANQP-element delete “is a 2-octet subfield whose value”, delete “is a 1-octet subfield whose format”, delete “a 1-octet subfield whose value is”, delete “a 1-octet subfield whose value is equal to”, delete “a 1-octet subfield that is”, delete “is a 1-octet subfield that”, change “is a 1-octet subfield whose value is set to” to “indicates”.

In 9.4.5.15 Domain Name ANQP-element change “is a 1-octet subfield whose value is set to” to “indicates”.

In M.3 A-MSDU subframes change “that 2-octet” to “that”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4229  Mark RISON  11.1.4.6  2174.49 | "A STA is not required to include all mandatory rates in its operational rate set, and a STA starting a BSS is  not required to include all mandatory rates in the basic rate set." -- there should be equivalent statements for MCSes | Change the cited text to "A STA is not required to include all mandatory rates/MCSes in its operational rate/MCS set, and a STA starting a BSS is  not required to include all mandatory rates/MCSs in the basic rate/MCS set." |

Discussion:

These comments are about the interplay between operational, basic and mandatory rates.

The operational rate set is the set of rates that a STA supports on rx, and the basic rate set is the set of rates that all STAs in the BSS are required to be able to rx and tx. A STA advertises the former in elements such as the Supported Rates and BSS Membership Selectors element and the HT Capabilities element, and the latter in elements such as the Supported Rates and BSS Membership Selectors element again and the HT Operation element.

[Oddly, only the former has a Clause 3 definition:

**operational rate set:** The set of data rates that a station (STA) is capable of receiving. The operational rate set is defined locally by the OperationalRateSet parameter of the MLME-START.request or MLME-JOIN.request primitive. The operational rate set of a peer is defined by the data rates (i.e., excluding the MSB of each octet of the (Extended) Supported Rates field) from the peer’s Supported Rates and BSS Membership Selectors element and, if present, the Extended Supported Rates and BSS Membership Selectors element.

This definition is a bit wonky, in fact, because if it’s a BSS membership selector you have to ignore it, you can’t just lop the MSB off. There’s a bit too much detail in this definition. The key (the “what”) is just the first sentence; the rest (the “how”) is not so important, though linking to WM observables is helpful.]

The point of

NOTE 1—A STA is not required to include all mandatory rates in its operational rate set, and a STA starting a BSS is not required to include all mandatory rates in the basic rate set.

is that in some situations devices might choose not to require a particular rate in a BSS, e.g. 1 Mbps might not be in the basic rate set if the AP wants to encourage use of higher data rates (e.g. it only wants OFDM modulations to be used).

Having said that, in 10.3.1 General of 10.3 DCF we also have:

NOTE—A STA’s operational rate set does not necessarily contain all the mandatory rates. However a STA has to be capable of receiving using a mandatory rate (as required by the rules in 10.6 (Multirate support)) even if it is not present in this set.

The second sentence is there because the multirate rules can in principle yield any rate, and if they do, the STA had better be able to cope! But there may be deployments in which a STA can be assured that it will not be required to receive a particular rate, e.g. ones where lower rates are deliberately excluded.

[Mandatory rates/MCSs are a reference to PHY statements, e.g.:

* DSSS: two mandatory modulation services […] 1 Mb/s DBPSK […] 2 Mb/s DQPSK
* HR/DSSS: the mandatory supported long preamble and header […] four mandatory rates […] 1 Mb/s […] 2 Mb/s […] 5.5 Mb/s […] 11 Mb/s
* OFDM: support of transmitting and receiving at data rates of 6, 12, and 24 Mb/s is mandatory
* ERP: transmission and reception capability for 1, 2, 5.5, 6, 11, 12, and 24 Mb/s data rates is mandatory
* HT: MCS 0–7 for 20 MHz mandatory at non-AP STA and at AP that is a VHT AP;  
   MCS 0–15 for 20 MHz mandatory at AP that is not a VHT AP

]

The first comment is about making similar statements about MCSes, since similar arguments apply, and “rates” is understood to be something only PHYs that don’t use MCSes have.

The second comment is pointing out that the basic rate/MCS set is fixed. They have to be fixed, because members of the BSS cannot suddenly be required to be able to transmit or receive at new rates.

Note that a non-VHT HT AP has 20M MCS 0-15 mandatory. However, this is not the case for an HT non-AP STA, which only has 20M MCS 0-7 mandatory. This demonstrates that the basic MCS set need not contain all the AP’s mandatory MCSes, otherwise HT non-AP STAs that only supported their mandatory MCSes would in fact be unable to join a non-VHT HT AP’s BSS. Similarly for the basic rate set: if it were required to include all the AP’s mandatory rates an ERP AP would not be able to support non-ERP DSSS non-AP STAs.

Sean COFFEY has pointed out that we need to be careful to make a distinction between the rates/MCSes that are mandatory for a STA (from the word “mandatory” in the PHY clauses and/or “shall”s in the PHY clauses) and the rates/MCSes that are advertised by a STA.

Sean COFFEY has further pointed out that “that all STAs in a BSS are capable of receiving and transmitting” is ambiguous as to whether it’s about the intersection of the capabilities of the current members of the BSS or the requirements on any members of the BSS, present or future. The answer is the latter.

Proposed changes:

In D3.4:

In Clause 3 change the definition of operational rate set and add definitions for operational MCS set and basic rate and MCS set (in the correct alphabetic position):

**operational rate set:** The set of data rates that a station (STA) is capable of receiving. ~~The operational rate set is defined locally by the OperationalRateSet parameter of the MLME-START.request or MLME-JOIN.request primitive. The operational rate set of a peer is defined by the data rates (i.e., excluding the MSB of each octet of the (Extended) Supported Rates field) from the peer’s Supported Rates and BSS Membership Selectors element and, if present, the Extended Supported Rates and BSS Membership Selectors element.~~

**operational modulation and coding scheme (MCS) set:** The set of MCSs that a station (STA) is capable of receiving.

**basic rate set:** The set of data rates that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic rate set is fixed for the lifetime of the BSS.

**basic modulation and coding scheme (MCS) set:** The set of MCSs that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic MCS set is fixed for the lifetime of the BSS.

OR (to tie the sets to specific over-the-air behaviour)

**operational rate set:** The set of data rates that a station (STA) is capable of receiving. ~~The operational rate set is defined locally by the OperationalRateSet parameter of the MLME-START.request or MLME-JOIN.request primitive.~~ The operational rate set of a peer is ~~defined by the data rates (i.e., excluding the MSB of each octet of the (Extended) Supported Rates field) from~~ advertised in the peer’s Supported Rates and BSS Membership Selectors element and, if present, ~~the~~ Extended Supported Rates and BSS Membership Selectors element.

**operational modulation and coding scheme (MCS) set:** The set of MCSs that a station (STA) is capable of receiving. The operational MCS set of a peer is typically advertised in the peer’s physical layer (PHY) capabilities element(s), e.g. HT and VHT Capabilities elements.

**basic rate set:** The set of data rates that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic rate set is fixed for the lifetime of the BSS. The basic rate set is advertised in the Supported Rates and BSS Membership Selectors element and, if present, the Extended Supported Rates and BSS Membership Selectors element.

**basic modulation and coding scheme (MCS) set:** The set of MCSs that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic MCS set is fixed for the lifetime of the BSS. The basic MCS set is typically advertised in the physical layer (PHY) operation element(s), e.g. HT and VHT Operation elements.

Change 10.3.1 General of 10.3 DCF as follows:

NOTE—~~A STA’s~~The operational rate or MCS set that a STA advertises does not necessarily contain all the mandatory rates or MCSs, respectively. However, a STA has to be capable of receiving using a mandatory rate or MCS (as required by the rules in 10.6 (Multirate support)) even if it is not present in this set.

Change 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and

Extended Supported Rates and BSS Membership Selectors element as follows:

NOTE 1—A STA is not required to include all mandatory rates or MCSs in ~~its~~the operational rate or MCS set, respectively, that it advertises, and a STA starting a BSS is not required to include all mandatory rates or MCSs in the basic rate or MCS set, respectively, that it advertises . In this context, “mandatory” describes rates or MCSs that are so described, or described using “shall support”, in the PHY clauses applicable to the STA.

OR instead of the two changes above (to put it all in one place).

Change 10.3.1 General of 10.3 DCF as follows:

NOTE—~~A STA’s~~The operational rate or MCS set that a STA advertises does not necessarily contain all the mandatory rates or MCSs, respectively. The basic rate or MCS set that a STA starting a BSS advertises does not necessarily contain all the mandatory rates or MCSs, respectively. However, a STA has to be capable of receiving using a mandatory rate or MCS (~~as~~when required by the rules in 10.6 (Multirate support)) even if it is not present in th~~is~~e operational rate or MCS set, respectively, that the STA advertises, and similarly has to be capable of transmitting using a mandatory rate or MCS (when required by the rules in 10.6 (Multirate support)) even if it is not present in the basic rate or MCS set, respectively. In this context, “mandatory” describes rates or MCSs that are so described, or described using “shall support”, in the PHY clause applicable to the STA.

Delete NOTE 1 in 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element.

[ENDOR]

Change 10.3.7 DCF timing relations as follows:

(11ah)In a non-S1G STA, when dot11DynamicEIFSActivated is false or not defined, the EIFS is derived from the SIFS and the DIFS and the length of time it takes to transmit an Ack frame at the lowest PHY mandatory rate or MCS by Equation (10-7).

EIFS = aSIFSTime + AckTxTime + DIFS (10-7)

where

AckTxTime is the time expressed in microseconds required to transmit an Ack frame, including preamble, PHY header and any additional PHY dependent information, at the lowest PHY mandatory rate or MCS.

=== previous

Change 10.3.1 General of 10.3 DCF as follows:

NOTE—A STA’s operational rate or MCS set does not necessarily contain all the mandatory rates or MCSs, respectively. However a STA has to be capable of receiving using a mandatory rate or MCS (as required by the rules in 10.6 (Multirate support)) even if it is not present in this set.

Change 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and

Extended Supported Rates and BSS Membership Selectors element as follows:

NOTE 1—A STA is not required to include all mandatory rates or MCSs in its operational rate or MCS set, respectively, and a STA starting a BSS is not required to include all mandatory rates or MCSs in the basic rate or MCS set, respectively.

Change 10.3.7 DCF timing relations as follows:

(11ah)In a non-S1G STA, when dot11DynamicEIFSActivated is false or not defined, the EIFS is derived from the SIFS and the DIFS and the length of time it takes to transmit an Ack frame at the lowest PHY mandatory rate or MCS by Equation (10-7).

EIFS = aSIFSTime + AckTxTime + DIFS (10-7)

where

AckTxTime is the time expressed in microseconds required to transmit an Ack frame, including preamble, PHY header and any additional PHY dependent information, at the lowest PHY mandatory rate or MCS.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4229 in <this document>, which make changes in the direction suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4266  Mark RISON | It should be clearer that it is not possible to change the basic rate/MCS set for the lifetime of the BSS | As it says in the comment |

Discussion:

The basic rate set is the set of rates that all STAs in the BSS are required to be able to rx and tx, and similarly for the basic MCS set. A STA advertises this in elements such as the Supported Rates and BSS Membership Selectors element and the HT Operation element. The existing text about this is e.g.:

**6.3.3.3.2 Semantics of the service primitive**

Non-DMG BSS: The set of

data rates (in units of 500 kb/s)

that all STAs in the BSS are

able to use for communication.

All STAs in the BSS are able to

receive and transmit at each of

the data rates listed in the set.

**6.3.11.2.2 Semantics of the service primitive**

Non-DMG BSS: The set of data rates (in

units of 500 kb/s) that all STAs in the BSS

are able to use for communication. All STAs

in the BSS including the STA that is creating

the BSS, are able to receive and transmit at

each of the data rates listed in the set.

**10.3.1 General**

All non-DMG STAs that are members of a BSS are able to receive and transmit at all of the data rates in the BSSBasicRateSet parameter of the MLME-START.request primitive or BSSBasicRateSet parameter of the SelectedBSS parameter of the MLME-JOIN.request primitive; see 6.3.4.2.4 (Effect of receipt) and 6.3.11.2.4 (Effect of receipt).

**11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element(#1370)**

The Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element in Beacon and Probe Response frames is used by STAs in order to avoid associating with a BSS if they do not support all of the data rates in the BSSBasicRateSet parameter

**11.3.5.3 AP or PCP association receipt procedures**

The SME shall refuse an association request from a STA that does not support all of the rates in the BSSBasicRateSet parameter

The point of the second half of

NOTE 1—A STA is not required to include all mandatory rates in its operational rate set, and a STA starting a BSS is not required to include all mandatory rates in the basic rate set.

is that (a) in general including all mandatory rates in the basic rate set would prevent legacy STAs from joining (see below) and additionally (b) in some situations devices might choose not to require a particular rate in a BSS, e.g. 1 Mbps might not be in the basic rate set if the AP wants to encourage use of higher data rates (e.g. it only wants OFDM modulations to be used).

Mandatory rates/MCSs are a reference to PHY statements, e.g.:

* DSSS: two mandatory modulation services […] 1 Mb/s DBPSK […] 2 Mb/s DQPSK
* HR/DSSS: the mandatory supported long preamble and header […] four mandatory rates […] 1 Mb/s […] 2 Mb/s […] 5.5 Mb/s […] 11 Mb/s
* OFDM: support of transmitting and receiving at data rates of 6, 12, and 24 Mb/s is mandatory
* ERP: transmission and reception capability for 1, 2, 5.5, 6, 11, 12, and 24 Mb/s data rates is mandatory
* HT: MCS 0–7 for 20 MHz mandatory at non-AP STA and at AP that is a VHT AP;  
   MCS 0–15 for 20 MHz mandatory at AP that is not a VHT AP

The basic rate/MCS sets are fixed. They have to be fixed, because members of the BSS cannot suddenly be required to be able to transmit or receive at new rates.

Note that a non-VHT HT AP has 20M MCS 0-15 “mandatory”. However, this is not the case for an HT non-AP STA, which only has 20M MCS 0-7 mandatory. This demonstrates that the basic MCS set need not contain all the AP’s mandatory MCSes, otherwise HT non-AP STAs that only supported their mandatory MCSes would in fact be unable to join a non-VHT HT AP’s BSS (because these STAs would not support MCS 8-15, which are mandatory for the AP). Similarly for the basic rate set: if it were required to include all the AP’s mandatory rates an ERP AP would not be able to support non-ERP DSSS non-AP STAs (because these STAs would not support 6, 12 and 24 Mbps, which are mandatory for the AP).

Sean COFFEY has pointed out that we need to be careful to make a distinction between the rates/MCSes that are mandatory for a STA (from the word “mandatory” in the PHY clauses and/or “shall”s in the PHY clauses) and the basic rates/MCSes that are advertised by a STA.

Sean COFFEY has further pointed out that “that all STAs in a BSS are capable of receiving and transmitting” is ambiguous as to whether it’s about the intersection of the capabilities of the current members of the BSS or the requirements on any members of the BSS, present or future. The answer is the latter.

Proposed changes:

In D3.4:

In Clause 3 add definitions for operational MCS set and basic rate and MCS set (in the correct alphabetic position):

**basic rate set:** The set of data rates that all stations (STAs) in a basic service set (BSS) shall be capable of receiving and transmitting. The basic rate set is fixed for the lifetime of the BSS. The basic rate set is advertised in the Supported Rates and BSS Membership Selectors element and, if present, the Extended Supported Rates and BSS Membership Selectors element.

**basic modulation and coding scheme (MCS) set:** The set of MCSs that all stations (STAs) in a basic service set (BSS) shall be capable of receiving and transmitting. The basic MCS set is fixed for the lifetime of the BSS. The basic MCS set is typically advertised in the physical layer (PHY) operation element(s), e.g. HT and VHT Operation elements.

In 6.3.3.3.2 Semantics of the service primitive (2x), 6.3.11.2.2 Semantics of the service primitive (2x) change “are able” to “shall be able”.

In 10.3.1 General change “All non-DMG STAs that are members of a BSS are able to receive and transmit” to “All non-DMG STAs that are members of a BSS shall be able to receive and transmit”

Change 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and

Extended Supported Rates and BSS Membership Selectors element as follows:

NOTE 1—A STA is not required to include all mandatory rates in its operational rate set, and a STA starting a BSS is not required to include all ~~mandatory~~ rates or MCSs that are mandatory for it in the basic rate or MCS set, respectively, that it advertises. In this context, “mandatory” describes rates or MCSs that are so described, or described using “shall support”, in the PHY clauses applicable to the STA.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4266 in <this document>, which make it clear that the basic rates and MCS sets are immutable characteristics of the BSS, rather than a potentially varying characteristic of the STAs that are members of the BSS.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4266  Mark RISON | It should be clearer that it is not possible to change the basic rate/MCS set for the lifetime of the BSS | As it says in the comment |

Discussion:

The operational rate/MCS set is the set of rates/MCSes that a STA supports on rx, and the basic rate/MCS set is the set of rates/MCSes that all STAs in the BSS are required to be able to rx and tx. A STA advertises the former in elements such as the Supported Rates and BSS Membership Selectors element and the HT Capabilities element, and the latter in elements such as the Supported Rates and BSS Membership Selectors element again and the HT Operation element. Only the former has a Clause 3 definition, though.

Mandatory rates/MCSes are a reference to PHY statements, e.g.:

* DSSS: two mandatory modulation services […] 1 Mb/s DBPSK […] 2 Mb/s DQPSK
* HR/DSSS: the mandatory supported long preamble and header […] four mandatory rates […] 1 Mb/s […] 2 Mb/s […] 5.5 Mb/s […] 11 Mb/s
* OFDM: support of transmitting and receiving at data rates of 6, 12, and 24 Mb/s is mandatory
* ERP: transmission and reception capability for 1, 2, 5.5, 6, 11, 12, and 24 Mb/s data rates is mandatory
* HT: MCS 0–7 for 20 MHz mandatory at non-AP STA and at AP that is a VHT AP;  
   MCS 0–15 for 20 MHz mandatory at AP that is not a VHT AP
* VHT: A VHT STA shall support the following features: […]

— Single spatial stream VHT-MCSs 0 to 7 (transmit and receive) in all supported channel widths

Note that a non-VHT HT AP has 20M MCS 0-15 mandatory a VHT AP has 20-80M MCS 0-7 mandatory. However, this is not the case for a non-VHT HT non-AP STA, which only has 20M MCS 0-7 mandatory. This means that the basic MCS set need not contain all the AP’s mandatory MCSes, otherwise HT non-AP STAs that only supported their mandatory MCSes would in fact be unable to join a non-VHT HT AP’s BSS or a VHT AP’s BSS. Similarly for the basic rate set: if it were required to include all the AP’s mandatory rates an ERP AP would not be able to support DSSS non-AP STAs. This is captured in:

NOTE 1—[…] a STA starting a BSS is not required to include all mandatory rates in the basic rate set.

in 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element, although this is missing the basic MCS set.

Finally, it is further the case that the basic rate/MCS set is fixed. This has to be the case, because members of the BSS cannot suddenly be required to be able to transmit or receive at new rates/MCSes.

Proposed changes:

In D3.4:

In Clause 3 add definitions for basic rate and MCS set (in the correct alphabetic position):

**basic rate set:** The set of data rates that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic rate set is fixed for the lifetime of the BSS.

**basic modulation and coding scheme (MCS) set:** The set of MCSs that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic MCS set is fixed for the lifetime of the BSS.

OR (to tie the sets to specific over-the-air behaviour, like for the existing operational rate set definition)

**basic rate set:** The set of data rates that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic rate set is fixed for the lifetime of the BSS. The basic rate set is advertised in the Supported Rates and BSS Membership Selectors element and, if present, the Extended Supported Rates and BSS Membership Selectors element.

**basic modulation and coding scheme (MCS) set:** The set of MCSs that all stations (STAs) in a basic service set (BSS) are capable of receiving and transmitting. The basic MCS set is fixed for the lifetime of the BSS. The basic MCS set is typically advertised in the physical layer (PHY) operation element(s), e.g. HT and VHT Operation elements.

Change 11.1.4.6 Operation of Supported Rates and BSS Membership Selectors element and

Extended Supported Rates and BSS Membership Selectors element as follows:

NOTE 1—A STA is not required to include all mandatory rates in its operational rate set, and a STA starting a BSS is not required to include all mandatory rates or MCSs in the basic rate or MCS set, respectively, that it advertises. In this context, “mandatory” describes rates or MCSs that are so described, or described using “shall support”, in the PHY clauses applicable to the STA.

Change 10.3.7 DCF timing relations as follows:

(11ah)In a non-S1G STA, when dot11DynamicEIFSActivated is false or not defined, the EIFS is derived from the SIFS and the DIFS and the length of time it takes to transmit an Ack frame at the lowest PHY mandatory rate or MCS by Equation (10-7).

EIFS = aSIFSTime + AckTxTime + DIFS (10-7)

where

AckTxTime is the time expressed in microseconds required to transmit an Ack frame, including preamble, PHY header and any additional PHY dependent information, at the lowest PHY mandatory rate or MCS.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4266 in <this document>, which make changes in the direction suggested by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4220  Mark RISON | The Timestamp field rule ("value of the STA's TSF timer at the time that the data symbol containing the first bit of the Timestamp field appears at the transmit antenna connector" or similar) is mentioned for S1G beacon (twice), PV1 probe rsp, probe rsp, beacon, DMG beacon, announce, timing advertisement but not for TIM frames | Add something to give the same rule for TIM frames as for (normal) beacons (and also for any other frames with a Timestamp field whose contents are not clearly specified) |

Discussion:

There is a Timestamp field (or similar field that is precisely synchronised to the TSF at the point the symbol containing the start of it is transmitted) in the following frames; the places where the contents are specified is shown:

|  |  |
| --- | --- |
| Figure 9-63—TACK frame format | 9.3.1.21 TACK frame format “the least significant 5 octets of the TSF timer value of the transmitting STA  at the time that the data symbol containing the first bit of the Pentapartial field  is transmitted to the PHY plus the transmitting STA’s delays through the local PHY from the MAC-PHY interface to its interface with the WM” |
| Table 9-34—Beacon frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” |
| Table 9-41—Probe Response frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” [non-DMG] “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” [DMG] |
| Table 9-46—Timing Advertisement frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” [non-DMG] “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” [DMG] |
| Table 9-47—DMG Beacon frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” |
| Figure 9-80—S1G Beacon frame format | 9.3.4.3 S1G Beacon frame format “the 4 least significant octets of the transmitting STA’s TSF timer  at the time that the start of the data symbol, containing the first bit of the Timestamp (Ed)field, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM”  11.1.3.10.1 General S1G synchronization “the 4 least significant octets of the transmitting STA’s TSF timer  at the time that the start of the data symbol, containing the first bit of the Timestamp field, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM” |
| Figure 9-899—FILS Discovery Information field format | 9.6.7.36 FILS Discovery frame format “the value of the TSF timer  at the frame source” |
| Figure 9-952—TIM frame Action field(#2568) format | 11.2.3.15 TIM Broadcast “An AP transmitting a TIM frame with a valid TSF timestamp shall set the value of the TIM frame timestamp as defined in 11.1.3 (Maintaining synchronization), for the Beacon frame timestamp.” |
| Table 9-488—Announce frame Action field format | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” |
| Figure 9-982—STACK frame format | 9.8.4.2 STACK frame format “the least significant 4 octets of the value of the transmitting STA’s TSF timer  at the time that the start of the data symbol, containing the first bit of the Tetrapartial Timestamp field, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM” |
| Figure 9-983—BAT frame format | 9.8.4.3 BAT frame format “the least significant 5 octets of the value of the transmitting STA’s TSF timer  at the time that the start of the data symbol, containing the first bit of the Pentapartial Timestamp field, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM” |
| Figure 9-986—PV1 Probe Response frame format. | 9.8.5.3 PV1 Probe Response frame format “the 4 least significant octets of the transmitting STA’s TSF timer  at the time that the start of the data symbol, containing the first bit of the Timestamp, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM” |

Proposed changes:

In D3.4:

Make the changes indicated:

|  |  |
| --- | --- |
| Figure 9-63—TACK frame format | 9.3.1.21 TACK frame format “the value of the 5 least significant ~~5~~ octets of the STA’s TSF timer ~~value of the transmitting STA~~  at the time that the data symbol containing the first bit of the Pentapartial Timestamp field  ~~is transmitted to the PHY plus the transmitting STA’s delays through the local PHY from the MAC-PHY interface to its interface with the WM~~  appears at the transmit antenna connector” |
| Table 9-34—Beacon frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” *[no change]* |
| Table 9-41—Probe Response frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” [non-DMG] “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” [DMG] *[no change]* |
| Table 9-46—Timing Advertisement frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” [non-DMG] “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” [DMG] *[no change]* |
| Table 9-47—DMG Beacon frame body | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” *[no change]* |
| Figure 9-80—S1G Beacon frame format | 9.3.4.3 S1G Beacon frame format “the value of the 4 least significant octets of the ~~transmitting~~ STA’s TSF timer  at the time that the ~~start of the~~ data symbol~~,~~ containing the first bit of the Timestamp (Ed)field~~,~~ ~~is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM~~  appears at the transmit antenna connector”  11.1.3.10.1 General S1G synchronization “~~The Timestamp~~  ~~field of the S1G Beacon frame shall be set to the 4 least significant octets of the transmitting STA’s TSF timer~~  ~~at the time that the start of the data symbol, containing the first bit of the Timestamp field, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM.~~” |
| Figure 9-899—FILS Discovery Information field format | 9.6.7.36 FILS Discovery frame format “the value of the TSF timer  ~~at the frame source~~  at the time that the data symbol containing the first bit of the Timestamp field  appears at the transmit antenna connector” |
| Figure 9-952—TIM frame Action field(#2568) format | 11.2.3.15 TIM Broadcast “~~An AP transmitting a TIM frame with a valid TSF timestamp shall set the value of the TIM frame timestamp as defined in 11.1.3 (Maintaining synchronization), for the Beacon frame timestamp.~~”  11.1.3.1 General “A non-DMG STA sending a Beacon, Timing Advertisement, TIM frame with a TSF timestamp, or Probe Response frame shall set (M101)the frame’s Timestamp field so that”  11.1.3.1 General “A DMG STA sending a DMG Beacon, Announce, Timing Advertisement, TIM frame with a TSF timestamp, or Probe Response frame shall set (M101)the frame’s (#2588)Timestamp field so that” |
| Table 9-488—Announce frame Action field format | 11.1.3.1 General “the value of the STA’s TSF timer  at the time that the data symbol containing the first bit of the frame  appears at the transmit antenna connector” *[no change]* |
| Figure 9-982—STACK frame format | 9.8.4.2 STACK frame format “the value of the 4 least significant ~~4~~ octets of the ~~value of the transmitting~~ STA’s TSF timer  at the time that the ~~start of the~~ data symbol~~,~~ containing the first bit of the Tetrapartial Timestamp field~~, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM~~  appears at the transmit antenna connector” and “the value of the 4 least significant ~~lowest 4~~ octets of the TSF timer for a next TWT” |
| Figure 9-983—BAT frame format | 9.8.4.3 BAT frame format “the value of the 5 least significant ~~5~~ octets of the ~~value of the transmitting~~ STA’s TSF timer  at the time that the ~~start of the~~ data symbol~~,~~ containing the first bit of the Pentapartial Timestamp field~~, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM~~  appears at the transmit antenna connector” amd “the value of the 6 least significant ~~lowest 6~~ octets of the TSF timer for the next TWT” |
| Figure 9-986—PV1 Probe Response frame format. | 9.8.5.3 PV1 Probe Response frame format “the value of the 4 least significant octets of the ~~transmitting~~ STA’s TSF timer  at the time that the ~~start of the~~ data symbol~~,~~ containing the first bit of the Timestamp~~, is transmitted by the PHY plus the transmitting STA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM~~  appears at the transmit antenna connector” |

At 845.46 change “the Pentapartial field” to “the Pentapartial Timestamp field”.

At 2001.38 change “the Reference timestamp field” to “the Reference Timestamp field”.

At 2166.64 change “All Beacon, (11ah)S1G Beacon, Probe Response(11ah), PV1 Probe Response, DMG Beacon, and Announce frames carry a Timestamp field. A STA receiving such a frame” to “A STA receiving a Beacon, (11ah)S1G Beacon, Probe Response(11ah), PV1 Probe Response, DMG Beacon, or Announce frame”.

Change “Event timestamp field” to “Event TSF field” at 3927.64, 4060.9, 4064.32, 4067.45, 4071.8.

Change “TSF timer value” to “TSF timer” in Table 9-57—Subfields of the MIMO Control field, Table 9-87—Subfields of the CMMG MIMO Control field.

Change “station” to “STA” at 485.35.

In 9.4.2.21.7 Beacon report change “The Parent TSF field contains the lower 4 octets of the measuring STA’s TSF timer value” to “The Parent TSF field contains the value of the 4 least significant octets of the measuring STA’s TSF timer”.

In 9.6.7.9 DSE Measurement Report frame format change “The Actual Measurement Start Time field is set to the measuring STA’s TSF timer” to “The Actual Measurement Start Time field is set to the value of the measuring STA’s TSF timer”.

In 11.30.5 Recommending DMG BSS parameters to the AP or PCP change “the lower order 4 octets of the non-AP and non-PCP STA’s TSF timer” to “the value of the 4 least significant octets of the non-AP and non-PCP STA’s TSF timer”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4220 in <this document>, which make the description of the setting of Timestamp fields consistent.

Note to the commenter: the setting for TIM frames was specified indirectly, by cross-reference from 11.2.3.15 TIM Broadcast to 11.1.3.1 General.

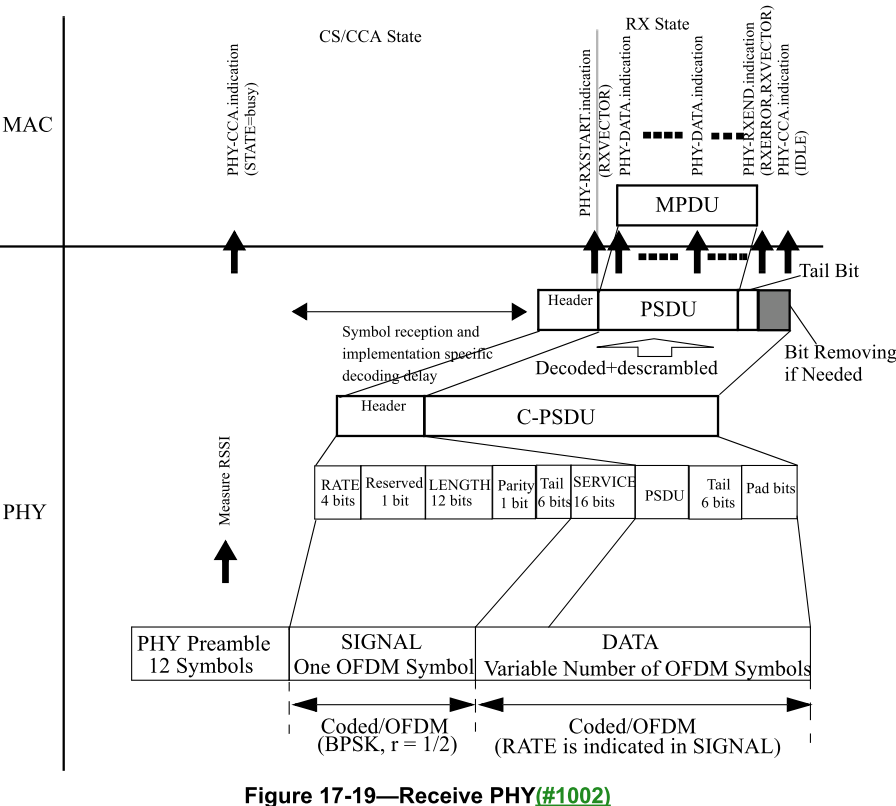
|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4477  Mark RISON | PHY-RXEND.ind is defined to be sent after any signal extension (" When a Signal Extension is present, the primitive is  generated at the end of the Signal Extension."; "When receiving a signal extended PPDU, the PHY-  RXEND.indication primitive shall be emitted a period of aSignalExtension after the end of the last symbol  of the PPDU."). So the PHY receive procedures need to show the PHY-RXEND.ind as being after the SE | As it says in the comment |

Discussion:

Signal extension applies to ERP-OFDM and HT PPDUs transmitted in the 2.4 GHz band, and delays the PHY-RXEND.indication by 6 µs. As 10.3.8 explains, “The purpose of this signal extension is to enable the NAV value of Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) STAs to be set correctly.”

This is shown in Figure 19-25—PHY receive procedure for HT-mixed format PPDU format and Figure 19-26—PHY receive procedure for HT-greenfield format PPDU. However, there is no equivalent format in Clause 18, and instead there is a cross-reference to Clause 17, whose Figure 17-19—Receive PHY does not show a signal extension (since it doesn’t apply to the OFDM PHY, since this only operates in the 5 GHz band):

In the case where the preamble is an ERP-OFDM preamble, the PHY receive procedure shall follow the procedure described in 17.3.12 (Receive PHY).



In principle, there should be a similar issue on transmit. However, it appears that there is no description of the Clause 18 transmit PHY! A different comment for another round…

Proposed resolution:

REVISED

In 18.3.5 PHY receive procedure after “In the case where the preamble is an ERP-OFDM preamble, the PHY receive procedure shall follow the procedure described in 17.3.12 (Receive PHY)” add “, except that the issuance of the PHY-RXEND.indication (and the following PHY-CCA.indication) is delayed by the signal extension”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4523  Mark RISON | Text about "channel starting frequency" sometimes does not give the units (e.g. in 20.3.1), and is inconsistent as to case of channel, italicisation (e.g. none in 17.3.8.4.2), and presence of article | As it says in the comment |

Discussion:

Yes, it’s a mess.

Proposed changes:

In D3.4:

In **17.3.8.4.2 Channel numbering**:

Channel center frequencies are defined at every integer multiple of 5 MHz above the channel starting frequency. The relationship between center frequency and channel number is given by Equation (17-27):

Channel center frequency = Channel starting frequency + 5 × *nch* (MHz) (17-27)

where

Channel starting frequency is defined as dot11ChannelStartingFactor × 500 kHz or

is defined as 5 GHz ~~for systems~~ where dot11OperatingClassesRequired is

false or not defined.

~~For example, dot11ChannelStartingFactor = 10 000(M101) indicates that Channel 0 center frequency is 5.000 GHz.~~ A channel center frequency of 5.000 GHz shall be indicated by dot11ChannelStartingFactor = 8000 and *nch* = 200. ~~An SME managing multiple channel sets can change the channel set being managed by changing dot11ChannelStartingFactor.~~

In **19.3.15.3 Channel allocation in the 5 GHz band**:

Channel center frequencies are defined at every integer multiple of 5 MHz above ~~5 GHz~~ the channel starting frequency. The relationship between center frequency and channel number is given in Equation (19-88).

Channel center frequency = Channel starting frequency + 5 × *nch* (MHz) (19-88)

where

***[Editor: indent the next sentence, as in 17.3.8.4.2. Leave the last sentence as it is, not indented.]***

Channel starting frequency is defined as dot11ChannelStartingFactor × 500 kHz or is defined as 5~~.000~~ GHz ~~for systems~~ where dot11OperatingClassesRequired is false or not defined. A channel center frequency of 5.000 GHz shall be indicated by dot11ChannelStartingFactor = 8000 and *nch* = 200.

In **20.3.1 Channelization**:

The channel center frequency is defined as:

***[Editor: deitalicise the following equation]***

*Channel center frequency = Channel starting frequency + Channel spacing × Channel number*

(M31)(#2017)where the channel starting frequency is equal to 56.16 GHz, and the channel spacing is (#4316)defined in Annex E.

In **21.3.14 Channelization**:

Given dot11CurrentChannelCenterFrequencyIndex0 and dot11CurrentChannelCenterFrequencyIndex1, the

respective channel center frequency is given by Equation (21-102).

Channel center frequency [MHz] (21-102)

= Channel starting frequency + 5 × dot11CurrentChannelCenterFrequencyIndex

where

Channel starting frequency is given by the operating class (Annex E)

dot11CurrentChannelCenterFrequencyIndex is either dot11CurrentChannelCenterFrequencyIndex0 or

dot11CurrentChannelCenterFrequencyIndex1

The center frequency of the primary 20 MHz channel is given by Equation (21-103).

Primary 20 MHz channel center frequency [MHz] (21-103)

= Channel starting frequency + 5 × dot11CurrentPrimaryChannel

***[Editor: indent the sentence after the “where”. Leave the sentence afterwards as it is, not indented.]***

where

~~The c~~Channel starting frequency is defined as dot11ChannelStartingFactor × 500 kHz. ~~If a~~

A channel center frequency ~~is~~of 5.000 GHz~~, it~~ shall be indicated by dot11ChannelStartingFactor = 8000 and

dot11CurrentPrimaryChannel = 200.

~~c~~Channel starting frequency = 5000 MHz

~~c~~Channel starting frequency = 5000 MHz

~~c~~Channel starting frequency = 5000 MHz

In **22.3.14 Channelization**:

***[Editor: make the same changes as in 21.3.14 Channelization]***

In **23.3.14 Channelization**:

The channel center frequency, *f*c, is defined as

*f*c [MHz] = *ChannelStartingFrequency* + *f*separation × *ChannelCenterFrequencyIndex*

where

*f*separation is the frequency separation between channels, and has the value of 0.5 MHz

*ChannelStartingFrequency* and *ChannelCenterFrequencyIndex* are region and operating class specific

and given in Annex E. The Channel spacing column(#2290) in Annex E denotes the corresponding bandwidth for S1G operation.

The center frequency of the primary 1 MHz or primary 2 MHz channel, *f*c, primary, is defined as:

*f*c, primary [MHz] = *ChannelStartingFrequency* + *f*separation × *PrimaryChannelNumber*

where

*f*separation is the frequency separation between channels, and has the value of 0.5 MHz

*PrimaryChannelNumber* is the subchannel index of the primary 1 or 2 MHz channel within the overall

bandwidth for S1G operation

In **24.3.1 Channelization**:

The channel center frequency is defined as:

***[Editor: deitalicise the following equation]***

*Channel center frequency* = *Channel starting frequency* + *Channel spacing* × (*Channel number mod* 32)

(#4578)where the channel starting frequency is equal to 56.16 GHz, and the channel spacing is defined in Table E-6 (Operating classes in China) in Annex E.

In **25.10 Channelization**:

~~Given dot11CMMGCurrentChannelCenterFrequencyIndex~~If dot11CMMGCurrentChannelWidth indicates a 540 MHz channel, the channel center frequency is given by Equation (25-75): ~~for 540 MHz channel.~~

*f*(*n*) [GHz] = blahblahblah (25-75)

***[Editor: in Equation (25-75) change all instances of*** *n* ***to*** dot11CMMGCurrentChannelCenterFrequencyIndex ***]***

~~where (#4580)channel starting frequencies of channel numbers 1 to 8 and channel numbers 9 to 10 are 42.66~~

~~GHz and 47.52 GHz, respectively, and~~ *~~n~~* ~~denotes the channel index decided by~~

~~dot11CMMGCurrentChannelCenterFrequencyIndex.~~

***[Editor: make the same changes for the text immediately below re a 1080 MHz channel]***

In **C.3**:

dot11CMMGCurrentChannelCenterFrequencyIndex OBJECT-TYPE

SYNTAX Unsigned32 (~~0~~1..~~200~~15)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

Written by the PHY.(MDR2)

~~For a 540 MHz, 1080 MHz, denotes the channel center frequency.~~

If dot11CMMGCurrentChannelWidth is cbw540(0) then contains the channel number (between 1 and 10).

If dot11CMMGCurrentChannelWidth is cbw1080(1) then contains the channel number (between 1 and 5) plus 10.

See 25.10 (Channelization)."

DEFVAL { 0 }

::= { dot11PHYCMMGEntry(M101) 2 }

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4523 in <this document>, which tidy things up, and fix a few bugs along the way.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4685  Mark RISON  6.3.4.2.4  344.63 | "If the MLME of an S1G STA receives an MLME-JOIN.request primitive with a SelectedBSS  parameter containing a BSSDescription with a Basic S1G-MCS and NSS Set field in the S1G Operation element that contains any unsupported <S1G-MCS, NSS> tuple, the ResultCode parameter in the MLME's  responding invocation of the MLMEJOIN.confirm primitive shall contain a value that is not SUCCESS." -- wording does not parallel that for other PHYs. Ditto last para of 6.3.11.2.4 | As it says in the comment |

Discussion:

The wording for other PHYs is e.g.:

If the MLME of an HT STA receives an MLME-JOIN.request primitive with the SelectedBSS parameter containing a Basic HT-MCS Set field in the HT Operation parameter that contains any unsupported MCSs, the MLME response in the resulting MLME-JOIN.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.

If the MLME of a VHT STA receives an MLME-JOIN.request primitive with a SelectedBSS parameter containing a Basic VHT-MCS And NSS Set field in the VHT Operation parameter that contains any unsupported <VHT-MCS, NSS> tuple, the MLME response in the resulting MLME-JOIN.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.

Cf.:

If the MLME of an S1G STA receives an MLME-JOIN.request primitive with a SelectedBSS parameter containing a BSSDescription with a Basic S1G-MCS and NSS Set field in the S1G Operation element that contains any unsupported <S1G-MCS, NSS> tuple, the ResultCode parameter in the MLME's responding invocation of the MLME-JOIN.confirm primitive shall contain a value that is not SUCCESS.

Proposed resolution:

REVISED

Change the cited text to (note: no space in “S1GOperation”):

If the MLME of an S1G STA receives an MLME-JOIN.request primitive with a SelectedBSS parameter containing a Basic S1G-MCS and NSS Set field in the S1GOperation parameter that contains any unsupported <S1G-MCS, NSS> tuple, the MLME response in the resulting MLME-JOIN.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.

Change the last para of 6.3.11.2.4 Effect of receipt to (ditto):

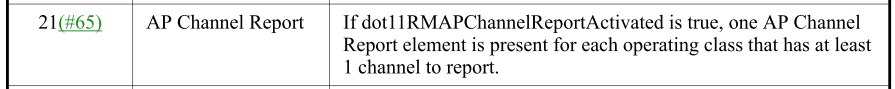
If the MLME of an S1G STA receives an MLME-START.request primitive with a Basic S1G-MCS and NSS Set field in the S1GOperation parameter containing any unsupported <S1G-MCS, NSS> tuple, the MLME response in the resulting MLME-START.confirm primitive shall contain a ResultCode parameter that is not set to the value SUCCESS.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4583  Mark RISON 6.3.3.3.2  330.44 | The AP Channel Report in a BSSDesdcription should allow for the possible of multiple reports | As it says in the comment |

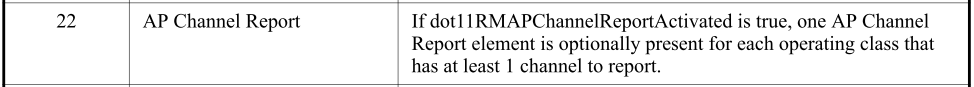
Discussion:

As the beacon and probe response format tables indicate (and also the text on Beacon requests), you can have more than one AP Channel Report element:

Beacon:



Probe response:



Beacon request:

The Request, Extended Request, AP Channel Report, and Vendor Specific subelements have the same format as their corresponding elements (see 9.4.2.9 (Request element), 9.4.2.10 (Extended Request element), 9.4.2.35 (AP Channel Report element), and 9.4.2.25 (Vendor Specific element), respectively). (#2606)Zero or more AP Channel Report subelements and zero or more Vendor Specific subelements are included in the list of optional subelements.

[…]

If one or more AP Channel Report elements are included, they indicate that iterative measurements are requested first on the channel(s) indicated by the Operating Class and Channel Number fields included in the Beacon request, and second on the channel(s) indicated by the Operating Class and Channel List fields of each AP Channel Report element included in the Beacon request.

Proposed resolution:

REVISED

Change the second and fourth cells of the AP Channel Report row in the second table in 6.3.3.3.2 Semantics of the service primitive (329.44 in D3.4) to “Set of AP Channel Report elements” and “The values from the AP

Channel Report element(s) if present in the Probe Response(#18) or Beacon frame, else null.” respectively.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4515  Mark RISON 8.3.5.6.2  769.43 | TXSTATUS in PHY-TXSTART.confirm isn't actually a transission status, it's ancillary info on the tx | As it says in the comment |

Discussion:

The description of the parameter is:

**8.3.5.6.2 Semantics of the service primitive**

The semantics of the primitive are as follows:

PHY-TXSTART.confirm(

TXSTATUS

)

The TXSTATUS represents a list of parameters that the local PHY entity provides to the MAC sublayer related to the transmission of an MPDU. The required PHY parameters are listed in 8.3.4.3 (PHY SAP service primitives parameters).

This is a bit weird because a PHY doesn’t know about MPDUs so can’t really provide info related to their transmission. Also, 8.3.4.3 doesn’t actually list the parameters at all:

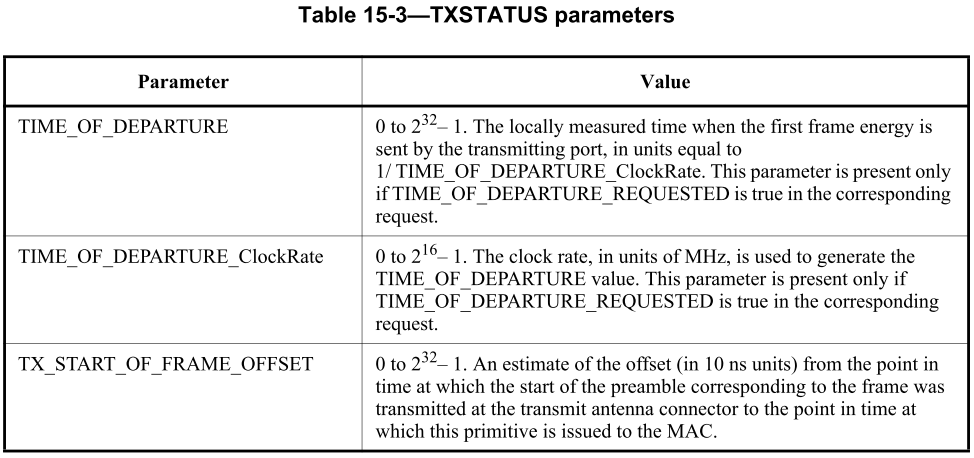


There’s a bit more info in 8.3.5.6.4 Effect of receipt:

Parameters in the TXSTATUS vector may be included in transmitted frames so that recipients on multiple channels can compensate for differences in the transmit time of the frames, and so to determine the time differences of air propagation times between transmitter and pairs of recipients and hence to compute the location of the transmitter via multilateration. See Annex P. In addition, the TXSTATUS vector may include the TX\_START\_OF\_FRAME\_OFFSET.

but this implies the TXSTATUS is just for timing stuff.

The actual TXSTATUS parameters are PHY-dependent, e.g.:



Similar information is in in Table 16-5—Parameter vectors, Table 17-3—TXSTATUS parameters, Table 18-2—TXSTATUS parameters (but also piggybacks on Clause 17), Table 19-4—TXSTATUS parameter, Table 20-2—TXSTATUS parameters (also used by Clause 21 -- must be wrong!), Table 24-2—TXSTATUS parameters. There appears to be no TXSTATUS parameters for Clauses 22, 23 or 25.

Proposed changes:

In D3.4:

Change 8.3.5.6.2 to 8.5.6.4 as follows:

**8.3.5.6.2 Semantics of the service primitive**

The semantics of the primitive are as follows:

PHY-TXSTART.confirm(

TXSTATUS

)

The TXSTATUS represents a list of parameters that the local PHY entity provides to the MAC sublayer related to the transmission of ~~an MPDU~~a PPDU. The ~~required PHY~~ list of parameters ~~are listed in 8.3.4.3 (PHY SAP service primitives parameters)~~ is PHY-dependent.

**8.3.5.6.3 When generated**

[…]

If dot11TODImplemented and dot11TODActivated are both true or dot11TimingMsmtActivated is true; and the parameter TIME\_OF\_DEPARTURE\_REQUESTED in the TXVECTOR specified in the PHY-TXSTART.request primitive(MDR2) is true, then the PHY shall include the TIME\_OF\_DEPARTURE corresponding to the time when the first frame energy is sent by the transmitting port and TIME\_OF\_DEPARTURE\_ClockRate parameters in the TXSTATUS ~~vector (See Table 15-3 (TXSTATUS parameters))~~, if the PHY includes these parameters in the TXSTATUS.

If dot11TimingMsmtActivated is true, then the PHY shall include TX\_START\_OF\_FRAME\_OFFSET in the TXSTATUS ~~vector (See Table 15-3 (TXSTATUS parameters))~~, if the PHY includes this parameter in the TXSTATUS.

**8.3.5.6.4 Effect of receipt**

The receipt of this primitive by the MAC entity causes the MAC to start the transfer of data octets. Parameters in the TXSTATUS ~~vector may~~ can be included in transmitted ~~frames~~MPDUs ~~so that recipients on multiple channels can compensate for differences in the transmit time of the frames, and so to determine the time differences of air propagation times between transmitter and pairs of recipients and hence to compute the location of the transmitter via multilateration~~. See Annex P for use of TXSTATUS parameters for timing. ~~In addition, the TXSTATUS vector may include the TX\_START\_OF\_FRAME\_OFFSET~~.

In 18.2 PHY-specific service parameter list delete “The service parameters for TXVECTOR, TXSTATUS, and RXVECTOR shall follow 17.2.2 (TXVECTOR parameters), 17.2.4 (TXSTATUS parameters), and 17.2.3 (RXVECTOR parameters), respectively.”.

In 21.2.6 TXSTATUS parameters change “Table 20-2 (TXSTATUS parameters)” to “Table 19-4 (TXSTATUS parameters)”.

Change the caption of Table 19-4 from “TXSTATUS parameter” to “TXSTATUS parameters”.

At 2360.49 change “via the TXSTATUS parameter of the PHY-TXSTART.confirm primitive.” to “via the TXSTATUS parameter list in the PHY-TXSTART.confirm primitive.”

Delete “(TXSTATUS)” in “PHY-TXSTART (TXSTATUS)” in the table in 6.5.4.3 When generated (2x), 15.2.2.6 TXVECTOR TIME\_OF\_DEPARTURE\_REQUESTED (2x), 17.2.2.6 TXVECTOR TIME\_OF\_DEPARTURE\_REQUESTED (2x), Table 17-3—TXSTATUS parameters (3x), 19.2.6 TXSTATUS parameters, 20.2.4 TXSTATUS parameters, 21.2.6 TXSTATUS parameters, 21.3.19 PHY transmit procedure, 23.3.19 PHY transmit procedure, 24.2.3 TXSTATUS parameters.

Change any remaining instances of “TXSTATUS vector” to “TXSTATUS”.

Proposed resolution:

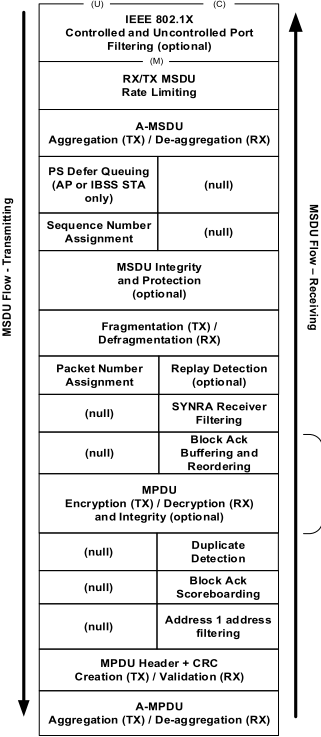
REVISED

Make the changes shown under “Proposed changes” for CID 4515 in <this document>, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4272  Mark RISON  5 | Figures 5-1, 5-2 and 5-7 talk of "MSDU flow", but a large part of what they show applies to MMPDUs, and some applies to Control frames | Show the portions of the figures that pertain to MMPDU and Control frame flows |

Discussion:

Figure 5-1 is as follows:



Things like PS Defer Queueing, Sequence Number Assignment, Fragmentation/Defragmentation, PN Assignment, Replay Detection, Integrity apply to MMPDUs too, and the bottom three rows apply to Control frames too. On the other hand this subclause is about “MAC data service architecture”; there doesn’t seem to be a MAC control service architecture subclause.

Proposed changes:

Change 5.1.5.1 as follows:

The MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 5-1 (MAC data plane architecture(11ak)(#2273)) when transparent FST is not being used and shown in Figure 5-2 (MAC data plane architecture (transparent FST)(11ak)(#2467)(#2273)) when transparent FST is being used.

The dotted line box labeled “Role-specific behaviors” is replaced by one of several options, depending on the role of the STA. See the following subclauses

During transmission, an MSDU goes through ~~some or all of~~ the ~~following~~ processes shown in the left-hand side of Figure 5-1~~: MSDU rate limiting, aggregate MSDU (A-MSDU) aggregation, frame delivery deferral during power save mode, sequence number assignment, integrity protection, fragmentation, encryption, frame formatting (11ak)(including optional SYNRA construction), and aggregate MAC protocol data unit (A-MPDU) aggregation~~. When transparent FST is used, an MSDU first goes, as shown in Figure 5-2, through an additional transparent FST entity that contains a demultiplexing process that forwards the MSDU down to the selected TX MSDU Rate Limiting process, and thence MAC data plane processing as described in the previous sentence. IEEE Std 802.1X-2010 may block the MSDU at the Controlled Port before the preceding processing occurs. Otherwise, at some point, the Data frames that contain all or part of the MSDU are queued per AC/TS.

During reception, a received Data frame goes through the processes shown in the right-hand side of Figure 5-1 ~~of possible A-MPDU deaggregation, MPDU header and cyclic redundancy code (CRC) validation, Address 1 address filtering, block ack scoreboarding(#1561), duplicate removal, decryption, possible reordering if the block ack mechanism is used, replay detection, defragmentation, integrity checking, SYNRA receive filtering when the corresponding link is a general link,(11ak) possible A-MSDU deaggregation, and possible MSDU rate limiting~~. Then, one or more MSDUs are delivered to the MAC SAP or, via the DSAF, to either the DS or an IEEE 802.1Q bridge port.(11ak) When transparent FST is used, MSDUs originating from different PHY SAPs go, as shown in Figure 5-2, through a final step of a transparent FST entity that contains a multiplexing process before delivering the MSDU. The IEEE 802.1X Controlled/Uncontrolled Ports discard any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame.

NOTE—Many of the processes shown in Figure 5-1 also apply to MMPDU flows for the MAC control plane architecture, and the processes shown at the bottom also apply to Control and Extension frames.

When transparent FST is used, the same security keys, sequence counter, and PN counter are used by the MAC data plane to encrypt the MPDU prior to and following an FST, and the same security keys are used to check the integrity and perform the protection of MSDUs. When nontransparent FST is used, independent RSNAs, security keys, sequence counters, and PN counters have to be established for each MAC data plane to be used prior to and following an FST. When transparent FST is used, a single MAC SAP at each peer is presented to the higher layers of that peer for all of the frequency bands/channels that are identified by the same MAC address at that peer. When nontransparent FST is used, different MAC SAPs are presented to higher layers since different MAC addresses are used prior to and following an FST.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4272 in <this document>, which add a NOTE to clarify that MMPDUs share a lot of the processes with MSDUs, and that Control (and Extension) frames share the lowest-level ones.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4550  Mark RISON  C.3  4214.42 | dot11Class2CapabilitiesOptionImplemented -- should this really be a capability variable, if it's something a STA might not do if it's operating in the 5G band? | As it says in the comment |

Discussion:

Class 2 ERP and HT STAs only operate in the 2.4 GHz band, so it is desirable to be clearer that the capability must be false outside that band.

Proposed resolution:

REVISED

In D3.4 add a new sentence to the end of the last para of the DESCRIPTION for dot11Class2CapabilitiesOptionImplemented (4221.65): “This attribute is false if the STA is not operating in the 2.4 GHz band.”. Also at the start of the existing sentence change “value” to “attribute”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4458  Mark RISON | Re Supported Operating Classes, in the MLME SAP, it's sometimes "This parameter is present if  dot11ExtendedChannelSwitchAct  ivated is true; otherwise not  present." but sometimes "This parameter is  present if  dot11ExtendedChannelSwitchActivated  is true.". In the Beacon/Probe Request/Response frame, though, it's "The Supported Operating Classes element is present if  dot11ExtendedChannelSwitchActivated is true.  The Supported Operating Classes element is optionally present if  dot11TVHTOptionImplemented is true." [why in Response?] and in the (Re)Association Request frame it's "The Supported Operating Classes element is present if  dot11ExtendedChannelSwitchActivated is true." | As it says in the comment |

Discussion:

As it says in the comment, but some observations:

* Some places have the explicit “otherwise not present”, others not. Presumably for .inds and .cfms it won’t be present if the peer hasn’t provided a list of supported operating classes
* Some places have a dependency on dot11OperatingClassesImplemented, some on dot11ExtendedChanneSwitchActivated (but both must be true for an HT STA); also an ECS STA sets both dot11OperatingClassesRequired (which presumably implies dot11OperatingClassesImplemented) and dot11ExtendedChannelSwitchActivated
* Maybe mesh STAs are required to do extended channel switching? 11.8.8.4 MBSS channel switching suggests this

[In 11.9.1 General:

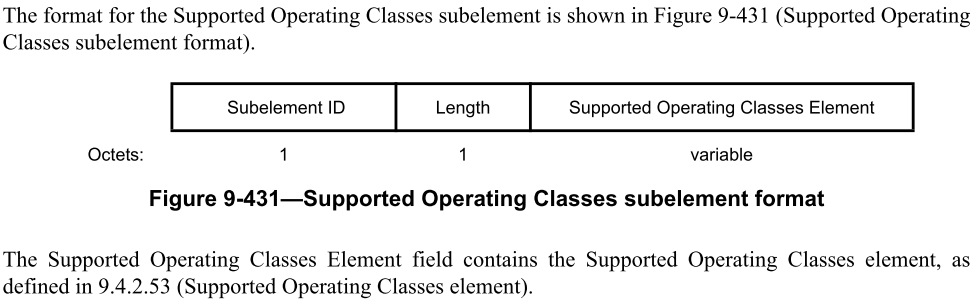
A STA shall use the ECS procedures defined in this subclause if dot11ExtendedChannelSwitchActivated is true. To indicate that it can perform ECS procedures, a STA shall set dot11ExtendedChannelSwitchActivated, dot11MultiDomainCapabilityActivated and dot11OperatingClassesRequired to true

In 11.15.3.1 General:

An HT STA shall set the following (M101)to true: dot11OperatingClassesImplemented, dot11OperatingClassesRequired, and dot11ExtendedChanneSwitchActivated.

]

[Incidentally: really? The Information field of the subelement contains the whole element?!



]

Proposed changes:

In D3.4:

In the table in 6.3.7.2.2 Semantics of the service primitive [assoc.req]:

Specifies the supported operating classes ~~capabilities~~ of the STA. This parameter is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.8.2.2 Semantics of the service primitive [reassoc.req]:

Specifies the supported operating classes of the STA. This parameter is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.7.3.2 Semantics of the service primitive [assoc.cfm]:

~~Specifies~~Indicates the supported operating classes ~~capabilities~~ of the ~~STA~~AP or PCP. This parameter is optionally present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.8.3.2 Semantics of the service primitive [reassoc.cfm]:

~~Specifies~~Indicates the supported operating classes of the ~~STA~~AP or PCP. This parameter is optionally present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.7.4.2 Semantics of the service primitive [assoc.ind]:

Indicates the supported operating classes ~~capabilities~~ of the ~~AP or PCP~~STA. This parameter is optionally present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.8.4.2 Semantics of the service primitive [reassoc.ind]:

~~Specifies~~Indicates the supported operating classes of the STA. This parameter is optionally present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.7.5.2 Semantics of the service primitive [assoc.rsp]:

~~Indicates~~Specifies the supported operating classes ~~capabilities~~ of the AP or PCP. This parameter is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.8.5.2 Semantics of the service primitive [reassoc.rsp]:

Specifies the supported operating classes of the ~~STA~~AP or PCP. This parameter is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true; otherwise not present.

In the table in 6.3.65.2.2 Semantics of the service primitive [channelusage.req]:

Specifies the ~~S~~supported ~~O~~operating ~~C~~classes ~~information for the Channel Usage Request~~.

In the table in 6.3.65.4.2 Semantics of the service primitive [channelusage.ind]:

~~Specifies~~Indicates the ~~S~~supported ~~O~~operating ~~C~~classes ~~information for the Channel Usage Request~~.

In Table 9-34—Beacon frame body and Table 9-40—Probe Request frame body and Table 9-41—Probe Response frame body:

The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true.

The Supported Operating Classes element is optionally present if dot11TVHTOptionImplemented is true.

In Table 9-36—Association Request frame body and Table 9-38—Reassociation Request frame body:

The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true.

In Table 9-375—TDLS Discovery Response frame blahblah, Table 9-415—Information for TDLS Setup Request Action field:

The Supported Operating Classes element is present if the TDLS channel switching capability field is equal to 1.

In Table 9-416—Information for TDLS Setup Response Action field:

The Supported Operating Classes element is present if the TDLS channel switching capability bit is equal to 1 and the Status Code is SUCCESS and not present otherwise.

In 9.6.13.24 Channel Usage Request frame format:

The Supported Operating Classes Element field ~~includes~~contains a Supported Operating Classes element

In Table 9-437—Mesh Peering Open frame blahblah:

The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true, or for a mesh STA if dot11OperatingClassesImplemented is true and the STA is capable of operation in more than one operating class.

In 10.22.3 Operation with operating classes:

When dot11OperatingClassesImplemented is true, the following statements apply:

When dot11OperatingClassesRequired is true, or where operating classes domain information is

present in a STA, the STA shall indicate current operating class information in the Country element and Supported Operating Classes element

When dot11OperatingClassesRequired and dot11ExtendedChannelSwitchActivated are true and a

STA is capable of operating as specified in more than one operating class, the STA shall include the Supported Operating Classes element in (Re)Association Request ~~frames~~ and ~~Reassociation~~ Response frames.

When dot11OperatingClassesRequired is true and the STA supports one or more global operating

classes, or where global operating classes domain information is present in a STA, the STA shall

indicate current operating class information in the Country element and Supported Operating

Classes element

In 11.8.8.4.4 Channel switch across an operating class:

When dot11OperatingClassesImplemented is true and the mesh STA is capable of operation in more than one operating class, the mesh STA shall include the Supported Operating Classes element within its Mesh Peering Open frames.

In 11.9.2 Advertising supported operating classes:

When dot11ExtendedChannelSwitchActivated or dot11OperatingClassesRequired is true, the Current Operating Class field in the Supported Operating Classes element shall indicate the operating class in use for transmission and reception. The Operating Classes field shall list all operating classes with which the STA is capable of operating for the country that is specified in the Country element (9.4.2.8 (Country element)).

In 11.21.6.1 General:

When a STA enables support for TDLS channel switching, it shall set dot11TDLSChannelSwitchingActivated, dot11MultiDomainCapabilityActivated and dot11ExtendedChannelSwitchActivated to true. When TDLS channel switching is enabled, the STA may set TDLS Channel Switching capability field to 1. The STA shall include a Supported Channels element and a Supported Operating Classes element in all TDLS Setup Request and TDLS Setup Response frames that have a TDLS Channel Switching capability field equal to 1.

In 11.22.15 Channel usage procedures:

A non-AP STA that supports Channel Usage and is not associated to an AP prior to using a noninfrastructure network or an off channel TDLS direct link may transmit a Probe Request frame including both Supported Operating Classes and Channel Usage elements.

Change “TDLS Channel Switching on this link” to “TDLS channel switching on this link” at 1113.35.

Change “TDLS Channel Switching capability subfield” to “TDLS Channel Switching subfield” at 1113.37.

Change “TDLS channel switching capability field” to “TDLS Channel Switching subfield” at 1545.5, 1545.27, 1588.33, 1588.59.

Change “TDLS channel switching capability bit” to “TDLS Channel Switching subfield” at 1590.28, 1590.55.

Change “TDLS Channel Switching capability field” to “TDLS Channel Switching subfield” at 2342.54, 2342.56, 2342.60.

In 11.15.3.1 change “dot11ExtendedChanneSwitchActivated” to “dot11ExtendedChannelSwitchActivated”.

In 13.9.1 Introduction, B.4 PICS proforma (3x) change “(Re)Association frames” to “(Re)Association Request and Response frames”.

In 11.22.16.3.1 Overview change “(Re)Association frame” to “(Re)Association Request and Response frame”.

In 11.27.1 General, 11.46.3.2 Higher layer protocol encapsulation change “(Re)Association frame” to “(Re)Association Request frame”.

In 11.8.2.2 Providing supported channels upon association in a DMG BSS, 11.46.5.1 General change “(Re)Association frames” to “(Re)Association Request frames”.

In 13.4.1 Overview change “Association frames, Reassociation frames” to “Association Request and Response frames, Reassociation Request and Response frames”

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4458 in <this document>, which address the issue raised by the commenter, including the interplay between dot11ExtendedChannelSwitchActivated and dot11OperatingClassesRequired.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4808  Mark HAMILTON  9.6.7.16  1543.10 | RSNE, and FTE, are not "optionally present" if security is required. They \_are\_ present if security is required. | Delete "optionally" at P1543.10 and P1543.18. |

Discussion:

A resolution to this comment has already been motioned. However, two issues have since come to light:

1. Jouni MALINEN reports, re the presence of the FTE in the TDLS Discovery Response frame:  
     
   “This looks like a mistake in IEEE Std 802.11z-2010. The FTE is reused as a convenient container of nonce and MIC fields (i.e., nothing to do with FT support) and the FTE should be included only in frames that are exchanging nonces or providing integrity protection. In the case of the TDLS design, that is only the TDLS Setup Request/Response/Confirm/Teardown frames. The discovery frames do not do either of those items that would use the FTE. The TDLS implementation in wpa\_supplicant does not add the FTE into TDLS Discovery Response frames.

I think we should fix this in REVmd by removing the FTE from the TDLS Discovery Response frame format. That change could be justified by P802.11z not describing what values would be used within the FTE and at least one example implementation of TDLS not adding that FTE (i.e., this removal is fixing the standard, not really making a technical change into the protocol).”

1. The expression “present if security is required on the direct link” in various TDLS frames is not immediately clear. Who/what determines whether security is required on the direct link? The answer is that it’s dependent on whether security is used on the link to the AP (see 12.7.8.1: “If any security method (pre-RSNA or RSNA) is enabled on the connection between a STA and the AP, the STA shall require that the TPK security protocol complete successfully before using a direct link.”).

Proposed additional changes:

In D3.4:

In Table 9-375—TDLS Discovery Response frame Action field(#2568) format delete the FTE row (order 10) and renumber the following ones.

In Table 9-418—Information for TDLS Teardown Action field delete “(optional)” in the FTE row. (Note to the reader: the context is “The FTE is present if a TPK handshake was successful for this session (optional).”.)

Make the changes indicated in the following tables:

In Table 9-375—TDLS Discovery Response frame Action field(#2568) format:

if security is required on the direct link

-> if security is required on the direct link (see 12.7.8.1)

In Table 9-415—Information for TDLS Setup Request Action field:

if security is required on the direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the TDLS direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the direct link

-> if security is required on the direct link (see 12.7.8.1)

In Table 9-416—Information for TDLS Setup Response Action field:

if security is required on the TDLS direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the TDLS direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the direct link

-> if security is required on the direct link (see 12.7.8.1)

In Table 9-417—Information for TDLS Setup Confirm Action field:

if security is required on the TDLS direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the TDLS direct link

-> if security is required on the direct link (see 12.7.8.1)

if security is required on the direct link

-> if security is required on the direct link (see 12.7.8.1)

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4662  Mark RISON | I think "when" is disfavoured w.r.t. "if" | Change "when used with" to "it used with" |

Discussion:

“if” is preferred over “when” because the former focuses on the condition while the latter focuses on the time.

Proposed changes:

Change D3.4 as follows:

**parameterized quality of service (QoS):** The treatment of the medium access control (MAC) protocol data

units (MPDUs) depends on the parameters associated with the MPDU. Parameterized QoS is primarily

provided through the hybrid coordination function (HCF) controlled channel access (HCCA) mechanism,

but is also provided by the enhanced distributed channel access (EDCA) mechanism ~~when~~if used with a

traffic specification (TSPEC) for admission control.

The following AKM operations represent an alternate operation of using a PSK. This operation has security

vulnerabilities ~~when~~if used with a low-entropy key and is recommended to be used only after taking that into

account.

~~When~~If used with the looping technique described in (#4661)12.4.4.2.2 (Generation of the password element

with ECC groups by looping(M137)) and 12.4.4.3.2 (Generation of the password element with FFC groups by

looping(M137)), H and CN are instantiated with SHA-256. ~~When~~If used with the direct hashing technique

described in 12.4.4.2.3 (Hash-to-curve generation of the password element with ECC groups(M137)) and

12.4.4.3.3 (Direct Generation of the password element with FFC groups(M137)), H and CN are instantiated

with a hash function from Table 12-1 (Hash algorithm based on length of prime(M137)) depending on the size

of the prime defining the group being used with SAE.

~~When~~If used with the looping method of PWE generation (see 12.4.4.2.2

(Generation of the password element with ECC groups by looping(M137)) and 12.4.4.3.2 (Generation of the

password element with FFC groups by looping(M137))), both the KCK and PMK shall be 256 bits in length.

~~When~~If used with AKMs 00:0F:AC-8 or 00:0F:AC-9 and the direct hashing technique of PWE generation (see

12.4.4.2.3 (Hash-to-curve generation of the password element with ECC groups(M137)) and 12.4.4.3.3 (Direct

Generation of the password element with FFC groups(M137))), the KCK shall be the length of the digest

generated by H() and the PMK shall be 256 bits in length. ~~When~~If both SAE Commit messages indicated a

status code of SAE\_HASH\_TO\_ELEMENT,

PSK PMKIDs

have security vulnerabilities ~~when~~if used with low-entropy keys and should be used only after taking this into

account.

In addition to contents for establishing a mesh peering as specified in 14.3.7.1 (Generating Mesh Peering

Confirm frames), the Mesh Peering Confirm frame, ~~when~~if used with the AMPE, shall contain the following:

NOTE: Backend protocol might allow longer NAS Client identifiers (e.g.,

RADIUS allows up to 253-octet NAS-Identifier), but ~~when~~if used with fast BSS

transition, the maximum length is limited to 48 octets.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4662 in <this document>, which make the change suggested, fixing the typo and adding one more “When”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4618  Mark RISON | "receive address" should be "received address" throughout, and "transmit address" should be "transmitter address". Also "transmitting STA address (TA), and  receiving STA address (RA)" should be "transmiter address (TA), and  receiver address (RA)" | As it says in the comment |

Discussion:

In D3.4 there are about 16 instances of “receive address” or “transmit address” and about 44 instances of “receiver address” or”transmitter address”. Also, “RA” is stated to be an abbreviation for “receiver address or receiving station address” in 3.4.

Proposed resolution:

REVISED

In D3.4:

Change “transmit address” to “transmitter address” at 218.1, 1060.12, 2144.27, 2294.1, 2578.62, 2589.10, .

Change “Receive address” to “Receiver address” at 3626.42.

Change “The Transmit Address field contains the Transmitter Address (TA) from the frames being reported.” to “The Transmitter Address field contains the transmitter address (TA) from the frames being reported.” and change “Transmit Address” to “Transmitter Address” on page 1059.

Delete “Each Frame Report Entry field contains the Transmit Address, BSSID, PHY Type, Average RCPI, Last RSNI, Last RCPI, Antenna ID, and Frame Count for the frames counted in this Frame Report Entry field.” at 2294.5.

Change “The RSNA architecture binds the transmit and receive addresses to the pairwise key.” to “The RSNA architecture binds the transmitter and receiver addresses to the pairwise key.” at 2637.14.

Change “transmitting STA address (TA), and receiving STA address (RA)” to “transmitter address (TA), and receiver address (RA)” at 794.7.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4629  Mark RISON | "The RCPI encoding is defined in 15" should be referring directly to Clause 9, as in 16.3.8.6 Received Channel Power Indicator Measurement | Fix in 17.3.10.7 Received Channel Power Indicator Measurement and 20.3.10 Received channel power indicator (RCPI) measurement |

Discussion:

In fact it’s worse than that. The following issues are present:

* Weird indirection through Clause 15
* Missing RCPI spec for VHT, TVHT and S1G
* Duplication for CMMG

Proposed changes:

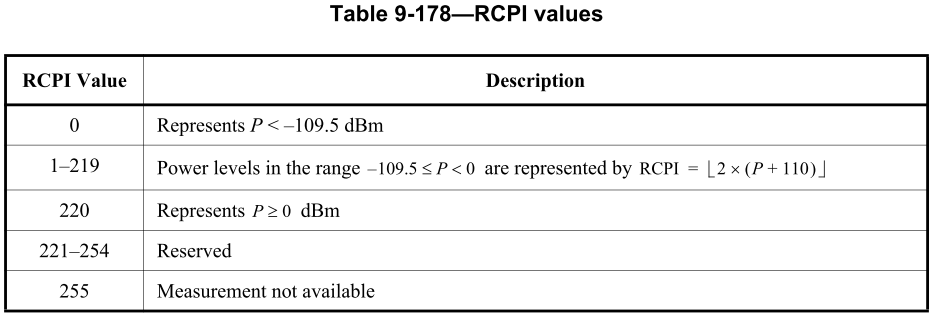
Make the following changes in D3.4:

**9.4.2.37 RCPI element**

The value of the RCPI field(M101) is a monotonically increasing, logarithmic function of the received

power level. The allowed values for the RCPI field are defined in Table 9-178 (RCPI values), where P is the

received power level in dBm.



**15.4.6.6 Received Channel Power Indicator Measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame. This parameter shall be a measure by the PHY of the received RF power in the channel measured over the entire received frame or by other equivalent means that meet the specified accuracy.

The RCPI encoding ~~of received power to RCPI~~ is defined in 9.4.2.37 (RCPI element).

RCPI shall equal the received RF power within an accuracy of ±5 dB (95% confidence interval) within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel bandwidth multiplied by 1.1.

**16.3.8.6 Received Channel Power Indicator Measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame. This parameter shall be a measure by the PHY of the received RF power in the channel measured over the entire received frame or by other equivalent means that meet the specified accuracy.

The RCPI encoding is defined in 9.4.2.37 (RCPI element).

RCPI shall equal the received RF power within an accuracy of ±5 dB (95% confidence interval) within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel bandwidth multiplied by 1.1.

**17.3.10.7 Received Channel Power Indicator Measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame. This parameter shall be a measure by the PHY of the received RF power in the channel measured over the entire received frame or by other equivalent means that meet the specified accuracy.

The RCPI encoding is defined in ~~15.4.6.6 (Received Channel Power Indicator Measurement)~~ 9.4.2.37.

RCPI shall equal the received RF power within an accuracy of ±5 dB (95% confidence interval) within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel bandwidth multiplied by 1.1.

**19.3.19.6 Received channel power indicator (RCPI) measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame. This parameter shall be a measure by the PHY of the received RF power in the channel measured over the data portion of the received frame. The received power shall be the average of the power in all active receive chains.

The RCPI encoding is defined in 9.4.2.37 (RCPI element).(#2101)

RCPI shall equal the received RF power within an accuracy of ± 5 dB (95% confidence interval) within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel width multiplied by 1.1.

**20.3.10 Received channel power indicator (RCPI) measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame ~~as measured at the DMG antenna(#2620) output~~. This parameter shall be a measure~~d~~ by the PHY of the received RF power in the channel measured over the preamble of the received frame.

The RCPI encoding is defined in ~~15.4.6.6 (Received Channel Power Indicator Measurement)~~ 9.4.2.37.

RCPI shall equal the received RF power with an accuracy of ± 5 dB with 95% confidence interval within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel width multiplied by 1.1. The relative error between RF

power measurements made within a 1 second interval should be less than ± 1 dB.

**21.3.18 VHT receiver specification**

*[nothing on RCPI]*

**22.3.18 TVHT receiver specification**

*[nothing on RCPI]*

**23.3.18 S1G receiver specification**

*[nothing on RCPI]*

**24.3.10 Received channel power indicator (RCPI) measurement**

The description for received channel power indicator (RCPI) measurement for CDMG PHY is the same as

that contained in 20.3.10 (Received channel power indicator (RCPI) measurement).

**25.3.13 Received channel power indicator (RCPI) measurement**

The RCPI is a measure of the received RF power in the selected channel for a received frame. This parameter shall be a measure~~d~~ by the PHY of the received RF power in the channel measured over the data portion of the received frame. ~~RCPI shall be a monotonically increasing, logarithmic function of the received power level defined in dBm.~~

The RCPI encoding is defined in 9.4.2.37.

~~The allowed values for the (#4627)RCPI shall be an 8 bit value in the range from 0 to 220, with indicated~~

~~values rounded to the nearest 0.5 dB as follows:~~

~~— 0: Power < –110 dBm~~

~~— 1: Power = –109.5 dBm~~

~~— 2: Power = –109.0 dBm~~

~~And so on up to:~~

~~— 220: Power > 0 dBm~~

~~— 221–254: reserved~~

~~— 255: Measurement not available~~

~~where RCPI = int{(Power in dBm +110) × 2} for 0 dBm > Power > –110 dBm.~~

RCPI shall equal the received RF power with an accuracy of ± 5 dB (95% confidence interval) within the

specified dynamic range of the receiver. The received RF power shall be determined assuming a receiver

noise equivalent bandwidth equal to the channel width multiplied by 1.1. The relative error between RF

power measurements made within a 1 second interval should be less than ± 1 dB.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4629 in <this document>, which align the descriptions of the RCPI where they are present (they are not present for the VHT, TVHT and S1G PHYs).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4602  Mark RISON  12 | There is confusion (cf. CID 2137 I think) about the general concept of a temporal key, and the temporal key (TK) in PTKs (Jouni is adamant they are not the same) | As it says in the comment |

Discussion:

We have the following definitions:

**group temporal key (GTK):** a temporal key that is used to protect information exchanged in group

addressed Data frames.(#2137)

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

(PMK) or from the PMK-R1.(#4779)

**perfect forward secrecy (PFS):** A property of a key agreement protocol that protects a session key derived

from a set of long-term public and private keys from being compromised if one of the (long-term) private

keys is compromised in the future.(11ai)

**temporal encryption key:** The portion of a pairwise transient key (PTK) or group temporal key (GTK) used

directly or indirectly to encrypt data in medium access control (MAC) protocol data units (MPDUs).

**temporal key (TK):** Temporal key integrity protocol (TKIP) only: The combination of temporal encryption

key and a message integrity code (MIC) key. Non-TKIP only: A temporal encryption key.

At the time we discussed CID 2137, which led to the addition of the GTK definition above, I suggested that the PTK should be called a temporal key too, since they both seem to me to be temporal in nature. I think Jouni, said, however, that PTKs are not temporal keys. I’m guessing this is because the GTK is just a temporal key, while the PTK is a concatenation of temporal keys (though I’m not sure how a session key differs from a temporal key -- the term in a context other than “master session key” only appears about 6 times and is not defined).

Proposed changes:

Alternative 1:

Under the definition of PTK add:

NOTE—A PTK is not a temporal key.

Change the definition of GTK to start “A” not “a”.

Alternative 2:

Under the definition of PTK add:

NOTE—A PTK is not a temporal key. It is a set of temporal keys.

Change “session key” to “temporal key” in the definition of perfect forward secrecy (PFS), in the definition of pairwise transient key (PTK), in 4.3.21.5.4 Mesh security (2x), in 12.6.1.2 TPKSA.

Change the definition of GTK to start “A” not “a”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4602 in <this document>, which add a note to explain why a PTK is not a TK[ and remove the undefined term “session key” except in the context of MSKs].

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4527  Mark RISON | The concept of a frame being "protected" is used without being defined | Define a protected frame as a frame that is authenticated and/or encrypted |

Discussion:

As it says in the comment. Some protected frames are protected by encryption, and some only by authentication/integrity-verifiability (not sure whether any are ever protected solely by encryption?).

The only definitions involving “protected frame” in D3.4 are:

**decapsulate:** To recover an unprotected frame from a protected one.

**encapsulate:** To construct a protected frame from an unprotected frame.

**encapsulation:** The process of generating a protected frame by encapsulating plaintext data.

**emergency services association:** A robust security network association (RSNA) between an access point (AP) and a non-AP station (STA) without security credentials; the non-AP STA is granted access to emergency services using unprotected frames via this association.

Proposed changes:

REVISED

In D3.4.

Add a definition in 3.2 (with the usual formatting):

**protected frame:** A frame that has been encrypted and/or whose integrity can be verified cryptographically.

Delete the space in the heading in 6.3.24.1 MLME- PROTECTEDFRAMEDROPPED.indication.

At 2631.40 change “Any protected frame(s) received shall be discarded, and MLME-PROTECTEDFRAMEDROPPED.indication primitive is invoked.” to “Any protected frame(s) received shall be discarded, and an MLME-PROTECTEDFRAMEDROPPED.indication primitive shall be invoked.” (changes in 2 places).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4525  Mark RISON | An ax comment said "W.r.t. dynamic defragmentation, it is mentioned that a recipient STA shall discard incomplete fragments when receiving a BlockAckReq to move the BA window. When the STA receives a DELBA to tear down the BA agreement, the STA should/shall do the same". The requirement to discard incomplete fragments on receiving a BAR that moves the window or a DELBA needs to be captured | As it says in the comment |

Proposed resolution:

REJECTED

10.2.6 says “An MSDU transmitted (#4290)under an HT-immediate or HT-delayed block ack agreement shall not be fragmented” so there can be no fragments to discard when the BA window moves or when the BA agreement is deleted.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4699  Mark RISON | "remaining TXOP duration" is not well-defined. Maybe it's just TXNAV? | As it says in the comment |

Discussion:

Ignoring dual CTS, which is obsolete, the references to “remaining TXOP duration” are:

**10.23.3.3 HCCA TXOP structure and timing**

The STA shall not initiate transmission of a frame unless the transmission and any acknowledgment or

other immediate response expected from the peer MAC entity are able to complete prior to the end of the

remaining TXOP duration.

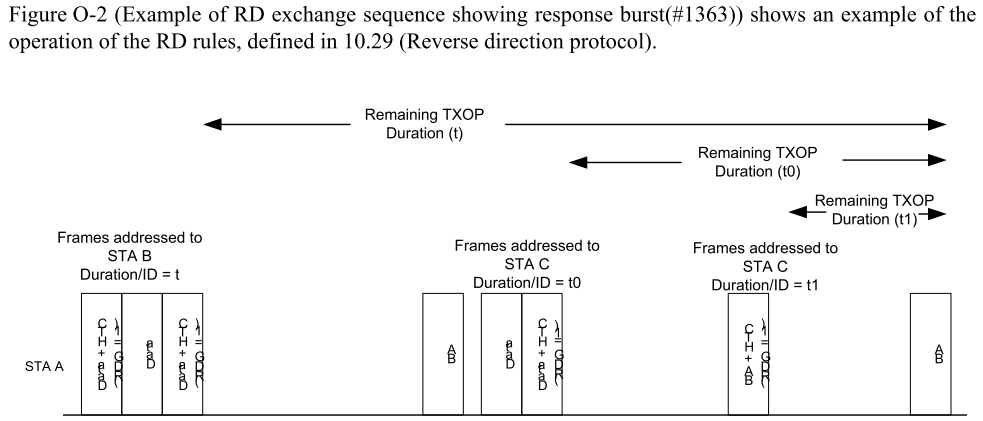
**10.54.5.4 Relay-shared TXOP protection mechanisms**

If explicit Ack procedure (see 10.54.5.2 (Explicit Ack procedure)) then the Duration field of the NDP CTS frame shall be set to a value D:

*TRTS + TPENDING − TCTS <= D <= TTXOP \_REMAINING − TPPDU*

*TTXOP\_REMAINING* is equal to any *TTXOP* as defined in 9.2.5.2 (Setting for single and multiple protection under enhanced distributed channel access (EDCA)) minus *TRTS*

**O.3 Example of an RD exchange sequence**



Proposed resolution:

REVISED

In 10.23.3.3 HCCA TXOP structure and timing change “prior to the end of the remaining TXOP duration” to “prior to the end of the TXOP”.

Fix the horror that has befallen Figure O-2.

Change “<=” to “≤” in 9.2.5.2 Setting for single and multiple protection under enhanced distributed channel

access (EDCA) (2x), 10.54.5.4 Relay-shared TXOP protection mechanisms (2x), Figure 11-35—Example negotiation and measurement exchange sequence, ASAP=0, and FTMs Per Burst = 2, Figure 11-36—Example negotiation and measurement exchange sequence, ASAP=1 FTMs Per Burst = 2 (and also add “, and” before “FTMs”), Figure 11-37—Example negotiation and measurement exchange sequence for a single burst instance, ASAP=1, and FTMs Per Burst = 3, Table 12-1—Hash algorithm based on length of prime (4x), 12.4.4.2.2 Generation of the password element with ECC groups by looping, 23.3.20 PHY receive procedure (2x), Table D-4—Maximum STA transmit power and maximum BW allowed (4x).

Change “>=” to “≥” in Figure 11-35—Example negotiation and measurement exchange sequence, ASAP=0, and

FTMs Per Burst = 2, Figure 11-36—Example negotiation and measurement exchange sequence, ASAP=1 FTMs Per Burst = 2 (and also add “, and” before “FTMs”), Figure 11-37—Example negotiation and measurement exchange sequence for a single burst instance, ASAP=1, and FTMs Per Burst = 3, 11.22.6.4 Measurement exchange body, Figure 23-5—Timing boundaries for S1G PPDU fields (and put a space after) (2x).

Change “-” to a minus glyph in the last bullet in 9.2.5.2 Setting for single and multiple protection under enhanced distributed channel access (EDCA).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4565  Mark RISON  9.3.1 | Why do some frame format figures in 9.3.1.x xxx frame format show the extent of the MAC header with arrows, and some not? | As it says in the comment |

Discussion:

Emily QI notes that:

According to Editorial Style guide (11-09-1034r16), the general rule is: “Arrows should not be used, except where labelling parts of the structure (e.g., MAC Header).”

So the question is when the MAC header needs to be labelled. It should be labelled in the figure showing the top-level frame formats, but not in the figures showing specific frames. Most specific frame figures do not label the MAC header, but a few of the oldest ones do.

Proposed resolution:

REVISED

In D3.4:

Delete the “MAC header” label and arrows in

Figure 9-30—RTS frame format

Figure 9-31—CTS frame format

Figure 9-32—Ack frame format

Figure 9-33—PS-Poll frame format

Figure 9-34—CF-End frame format

Figure 9-35—BlockAckReq frame format

Figure 9-41—BlockAck frame format

Make Figures 9-30/31/32/34 have searchable text, like Figures 9-33/35/41 (rather than being just pixels).

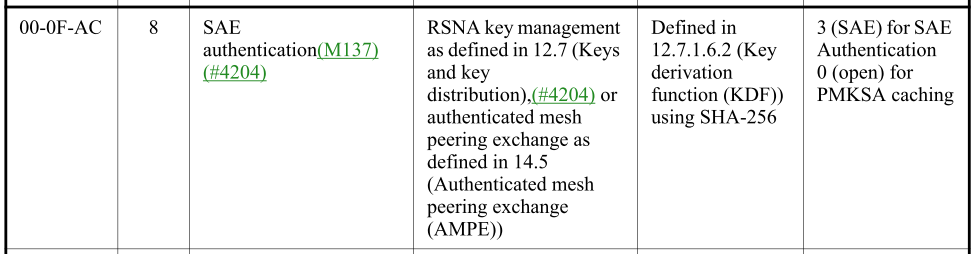
Add an arrow labelled “MAC header” to Figure 9-985—PV1 Management frame format, under the boxes, from the left of Frame Control to the right of A3.

Add “ format” to the end of the caption for Figure 9-65—Data frame and of the heading for Subclause 9.3.1.9 Control Wrapper frame.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4655  Mark RISON 9.4.2.24.3  1103.15 | "with SHA-256" was deleted from the 3rd column but is still there in the fifth, for 00-0F-AC:8 | Change "SAE  authentication" to "SAE  authentication with SHA-256" in third column |
| CID 4656  Mark RISON 9.4.2.24.3  1103.15 | "with SHA-256" was deleted from the 3rd column but is still there in the fifth, for 00-0F-AC:8 | Change "SAE  authentication" to "SAE  authentication with SHA" in third column |
| CID 4657  Mark RISON 9.4.2.24.3  1103.15 | "with SHA-256" was deleted from the 3rd column but is still there in the fifth, for 00-0F-AC:8 | Delete "using SHA\_256" in fifth column |

Discussion:

This is what the row in question looks like in D3.4:



So the question is: what selector do I use if I want to do SAE with SHA-384? It's not this one, because the fifth column explicitly requires me to use SHA-256. But there's no other row for SAE authentication. So I can't do SAE with anything other than SHA-256? That seems wrong.

Jouni MALINEN confirms this is indeed wrong:

SAE can use SHA-384 and even SHA-512. SHA-256 is hardcoded only for the case where the looping mechanism is used to derive pwe. When hash-to-curve (H2E) is used, the algorithm is determine based on the length of the prime per Table 12-1.

There seems to be a missing change in 12.4.5.4 that can make this a bit difficult to notice.. REVmd/D3.4 page 2566 line 12 describes the way this is supposed to work ("KDF using the hash algorithm defined for H()" and that H() part being defined in 12.4.2) while page 2565 line 42 covers only the pre-H2E option ("KDF shall then be used with the hash algorithm identified by the AKM suite selector"). That page 2565 line 42 text should be fixed to say "KDF shall then be used with the hash algorithm identified for H()" (and maybe add ", see 12.4.2" to make that clearer).

As far as Table 9-153 is concerned, the SAE authentication cases 00-0F-AC:8 and 00-0F-AC:9 should say something like this for Key derivation type: "Defined in 12.7.1.6.2 using the hash algorithm specified in 12.4.2".

Proposed resolution:

REVISED

Replace "Defined in 12.7.1.6.2 using SHA-256" with "Defined in 12.7.1.6.2 using the hash algorithm specified in 12.4.2" in the Key derivation type cell for the 00-0F-AC:8 and 00-0F-AC:9 rows in Table 9-153—AKM suite selectors (11md/D3.4 at 1104.15/26).

In addition, replace "The key derivation function from 12.7.1.6.2 shall then be used with the hash algorithm identified by the AKM suite selector (see Table 9-153)" with "The key derivation function from 12.7.1.6.2 shall then be used with the hash algorithm identified for H() (see 12.4.2)" in 12.4.5.4 Processing of a peer’s SAE Commit message (11md/D3.4 at 2565.42).

Change “00:0F:AC-” to “00-0F-AC:” (2x) in 12.4.5.4 Processing of a peer’s SAE Commit message (11md/D3.4 at 2565.48).

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4263  Mark RISON 11.39.1  2501.63 | "A STA that is starting a VHT BSS shall be able to receive and transmit at each of the <VHT-MCS, NSS> tuple  values indicated by the Basic VHT-MCS And NSS Set field" -- also a STA that is operating in such a BSS (cf. 11.14 -- but note that a STA that has not started the BSS it's in has not seen the MLME-START.request). There is some stuff in 10.3.1, but this is about DCF so it's not clear it applies to VHT STAs. See also 11ax CID 21270 | As it says in the comment |

Discussion:

The basic rate set applies to everyone in the BSS, not just the STA that started it.

Some PHYs state this in one place, others split it into two.

In a few places “create” is used instead of “start”, for a BSS, which makes things harder to find.

Proposed changes:

In D3.4:

Change the table in 6.3.11.2.2 Semantics of the service primitive [MLME-START.req] as follows:

Non-DMG BSS: The set of data rates (in units of 500 kb/s) that all STAs in the BSS are able to use for communication. All STAs in the BSS, including the STA that is ~~creating~~starting the BSS, are able to receive and transmit at each of the data rates listed in the set.

The set of features that are supported by all STAs ~~joining this~~in the BSS, ~~and by~~ including the STA that is ~~creating~~starting the BSS.

Change 6.3.11.1 Introduction as follows:

This mechanism supports the process of ~~creating~~starting a new BSS or becoming a member of an MBSS.

Leave 10.46.1 Basic S1G BSS functionality as follows:

An S1G STA that is starting a BSS shall be able to receive and transmit at each of the <S1G-MCS, NSS> tuple values indicated by the Basic S1G-MCS and NSS Set field of the S1G Operation parameter of the MLME-START.request primitive and shall be able to receive at each of the <S1G-MCS, NSS> tuple values indicated by the Supported S1G-MCS and NSS Set field of the S1G Capabilities parameter of the (#1270)MLME-START.request primitive.

Leave 10.46.7 BSS Basic S1G-MCS and NSS set operation as follows:

An S1G STA shall not attempt to join (MLME-JOIN.request primitive(MDR2)) a BSS unless it supports (i.e., is able to both transmit and receive using) all the <S1G-MCS, NSS> tuples in the BSS basic S1G-MCS and NSS set.

Change 11.14 HT BSS Operation as follows:

An HT STA that is ~~creating~~starting or joining a BSS shall be able to receive and transmit at each of the MCS values listed in the Basic HT-MCS Set field of the HT Operation parameter of the MLME-START.request primitive or Basic HT-MCS Set field of the HT Operation parameter of the SelectedBSS parameter of the MLME-JOIN.request primitive.

Leave 11.39.1 Basic VHT BSS functionality as follows:

A STA that is starting a VHT BSS shall be able to receive and transmit at each of the <VHT-MCS, NSS> tuple values indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the MLME-START.request primitive and shall be able to receive at each of the <VHT-MCS, NSS> tuple values indicated by the Supported VHT-MCS and NSS Set field of the VHT Capabilities parameter of the MLME-START.request primitive.

Leave 11.39.7 Basic VHT-MCS and NSS set operation as follows:

A VHT STA shall not attempt to join (MLME-JOIN.request primitive) a BSS unless it supports (i.e., is able to both transmit and receive using) all of the <VHT-MCS, NSS> tuples in the basic VHT-MCS and NSS set.

Change 11.42 Basic TVHT BSS functionality as follows:

The STA that is ~~creating~~starting a TVHT BSS shall be able to receive and transmit at each of the <VHT-MCS, NSS> tuple values indicated by the Basic VHT-MCS And NSS Set field of the VHT Operation parameter of the MLME-START.request primitive and shall be able to receive at each of the <VHT-MCS, NSS> tuple values indicated by the Supported VHT-MCS and NSS Set field of the VHT Capabilities parameter of the MLME-START.request primitive.***<insert line break>***

The basic VHT-MCS and NSS set is the set of <VHT-MCS, NSS> tuples that are supported by all TVHT STAs that are members of a TVHT BSS. It is established by the STA that starts the TVHT BSS. Other TVHT STAs determine the basic VHT-MCS and NSS set from the Basic VHT-MCS And NSS Set field of the TVHT Operation element in the BSSDescription derived through the scan mechanism (see 11.1.4.1 (General)).

A TVHT STA shall not attempt to join (MLME-JOIN.request primitive) a BSS unless it supports (i.e., is able to both transmit and receive using) all of the <VHT-MCS, NSS> tuples in the basic VHT-MCS and NSS set.

Leave 11.49.1 Basic CMMG BSS functionality as follows:

A STA that is starting a CMMG BSS shall be able to receive and transmit at each of the <(#4341)CMMG-MCS, NSS> tuple values indicated by the Basic (#4341)CMMG-MCS and NSS Set field of the CMMG Operation parameter of the MLME-START.request primitive and shall be able to receive at each of the <(#4341)CMMG-MCS, NSS> tuple values indicated by the Supported (#4341)CMMG-MCS and NSS Set field of the CMMG Capabilities parameter of the MLME-START.request primitive.

Leave 11.49.7 BSS basic (#4341)CMMG-MCS and NSS set operation as follows:

A CMMG STA shall not attempt to join (MLME-JOIN.request primitive) a BSS unless it supports (i.e., is able to both transmit and receive using) all the <(#4341)CMMG-MCS, NSS> tuples in the BSS basic (#4341)CMMG-MCS and NSS set.

In 11.2.4.3 Initialization of power management within an IBSS change “A STA creating a new IBSS” to “A STA starting a new IBSS”.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4263 in <this document>, which ensure that the behaviour for TVHT STAs joining a TVHT BSS is specified, and also use the term “start” consistently in relation to a BSS (not “create”). Note to the commenter: the VHT behaviour is already specified, in 11.39.7.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4566  Mark RISON  9.4.2.21.13  1087.26 | The Map Type field value "URL Defined" indicates the Map URL field value has a file extension, defined  as a mime type and is self-descriptive." is not clear. The MAP URL field has a MIME type appended? Exactly how is this appending signalled/encoded? Also, "mime" should be "MIME" | As it says in the comment |

Discussion:

A MIME (Multipurpose Internet Mail Extensions) type is something that looks like foo/bar (with optional extra stuff). A file extension is something that looks like .ext. An extension is arbitrary, though many are de facto mappings to MIME types (e.g. extensions .jpg and .jpeg are MIME type image/jpeg).

Proposed changes:

REVISED

In D3.4:

In 9.4.2.21.13 Location Civic report change “The Map Type field value “URL Defined” indicates the Map URL field value has a file extension, defined as a mime type and is self-descriptive.” to “The Map Type field value “URL Defined” indicates the Map URL field value has a file extension, and that the type of map referred to by the Map URL field is to be determined from this.”

In Table 9-143—Map Types change “fiff” to “tiff”.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4574  Mark RISON  10.23.2.2  1828.11 | "The transmission of the MPDU in the final PPDU transmitted by the TXOP holder during the TXOP for that AC has completed" -- has a number of issues: - what does "has completed" mean (just "has been put on the air, don't care about response if needs one"?) - what is the "AC was a primary AC" about? Presumably this is the MPDU at the start of the sentence? - so you start backoff immediately, even if you then transmit a secondary AC MPDU in the TXOP? Or you don't do backoff at all if the last MPDU you transmitted in the TXOP was a secondary AC MPDU? - what does "the MPDU in the final PPDU" mean if there is more than one MPDU in the final PPDU? - what if there isn't a TXNAV (i.e. multiple protection is not being used)? - so if the TXNAV timer has not expired you need to wait until it does and then do backoff? (More plausible than "you don't do backoff at all if the TXNAV hadn't expired at the same time as the "completion" of the last transmission!) | As it says in the comment |
| CID 4364  Mark RISON  10.23.2.2  1828.11 | "The transmission of the MPDU in the final PPDU transmitted by the TXOP holder during the TXOP  for that AC has completed" -- it is not clear what "completed" means (put on air? acked?) | As it says in the comment |
| CID 4365  Mark RISON  10.23.2.2  1828.11 | "The transmission of the MPDU in the final PPDU transmitted by the TXOP holder during the TXOP  for that AC has completed" -- it is not clear what "the MPDU" refers to, since a PPDU can contain more than one MPDU | As it says in the comment |
| CID 4154  Matthew Fischer  10.23.2.2  1827.61 | The subbullets all refer to "that AC" but there is no reference for "that" | Add the words "corresponding to an AC" in the introductory phrase which immediately precedes item a), so that it reads, "The backoff procedure shall be invoked by an EDCAF corresopnding to an AC when" |

Discussion:

Definitions:

**primary access category (AC):** The AC associated with the enhanced distributed channel access function (EDCAF) that gains channel access.

**transmission opportunity (TXOP) holder:** A quality-of-service (QoS) station (STA) that has either been granted a TXOP by the hybrid coordinator (HC) or successfully contended for a TXOP.

So an EDCAF that gains the medium is the TXOP holder and the primary AC is the EDCAF’s AC, but the term “primary AC” does not apply for a transmission if the EDCAF is not the TXOP holder (even when it is e.g. sending Data frames under a RDG). And obviously during a TXOP typically at least two EDCAFs are transmitting, it’s just that only one is the TXOP holder and has an associated primary AC.

Proposed changes:

In D3.4:

Change 10.23.2.2 EDCA backoff procedure as follows:

The backoff procedure shall be invoked by an EDCAF when any of the following events occurs:

a) An MA-UNITDATA.request primitive is received that causes ~~a frame~~ an MPDU ~~with that~~ corresponding to the EDCAF’s AC to be queued for transmission such that one of the transmit queues associated with that AC has now become nonempty and any other transmit queues associated with that AC are empty; the medium is busy on the primary channel as indicated by any of the following:

— physical CS;

— virtual CS;

— a nonzero TXNAV timer value;

— a mesh STA that has dot11MCCAActivated true and a nonzero RAV timer value, (#1501)

and the backoff counter has a value of 0 for that AC.

b) For the EDCAF that is the TXOP holder, t~~T~~he transmission of ~~the MPDU in~~ the final PPDU transmitted by the TXOP holder during the TXOP ~~for that AC~~ has completed and the TXNAV timer has expired~~, and the AC was a primary AC~~. ~~(See 10.23.2.7 (Sharing an EDCA TXOP)).~~

c) For the EDCAF that is the TXOP holder, t~~T~~he transmission of an MPDU in the initial PPDU of a TXOP fails, as defined in this subclause~~, and the AC was a primary AC~~.

d) ~~The~~A transmission attempt by the EDCAF collides internally with another EDCAF of an AC that has higher priority, that is, two or more EDCAFs in the same STA are granted a TXOP at the same time.(#1507)

In addition, the backoff procedure may be invoked by an EDCAF when:

e) For the EDCAF that is the TXOP holder, t~~T~~he transmission by the TXOP holder of an MPDU in a non-initial PPDU of a TXOP fails, as defined in this subclause.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID <above> in <this document>, which are great.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4659  Mark RISON 9.4.2.246  1464.28 | "list of unsigned 16-bit integers" -- the endianness is not clear (security tends to be the other way round to the usual MAC conventions) | As it says in the comment |

Discussion:

The full sentence is:

The Rejected Groups field contains a concatenated list of unsigned 16-bit integers representing finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

So yes, the endianness is not stated explicitly, so given that sometimes things in Clause 12 are big-endian, there is some scope for doubt, but one can argue that since it’s in Clause 9 the little-endian default from 9.2.2 applies. In addition, it is not clear how the 16-bit integers represent finite cyclic groups. Fortunately, there is a 9.4.1.42 Finite Cyclic Group field that is much clearer.

Proposed resolution:

REVISED

In D3.4:

In 9.4.2.246 Rejected Groups element change:

The Rejected Groups field contains a concatenated list of unsigned 16-bit integers representing finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

to:

The Rejected Groups field contains a list of Finite Cyclic Group fields indicating finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

and change “is shown in Figure 9-786 (OCT Source element format(#2634))” to “is shown in Figure 9-787”.

Note to the commenter: the endianness of the Finite Cyclic Group fields is given in Subclause 9.2.2, since it is not explicitly identified in 9.4.1.42 Finite Cyclic Group field.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID  Mark RISON |  |  |

Discussion:

Proposed changes:

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID in <this document>, which

traffic classification (TCLAS): The specification of one of several types of matching filter to classify protocol data units (PDUs) or medium access control (MAC) service data units (MSDUs) as belonging to a particular traffic stream (TS) or traffic category (TC). Depending on the type of classification, the filter is applied within the MAC sublayer management entity (MLME),(#4810) above the MAC, or within the MAC itself.(#2224)

traffic category (TC): A label for medium access control (MAC) service data units (MSDUs) that have a distinct user priority (UP), as viewed by higher layer entities, relative to other MSDUs provided for delivery over the same link. Traffic categories are meaningful only to MAC entities that support quality of service (QoS) within the MAC data service. These MAC entities determine the UP for MSDUs belonging to a particular traffic category using the priority value provided with those MSDUs at the MAC service access point (MAC SAP) or by using traffic classification (TCLAS).

traffic stream (TS): A set of medium access control (MAC) service data units (MSDUs) to be delivered subject to the quality-of-service (QoS) parameter values provided to the MAC in a particular traffic specification (TSPEC). TSs are meaningful only to MAC entities that support QoS within the MAC data service. These MAC entities determine the TSPEC applicable for delivery of MSDUs belonging to a particular TS using the priority parameter provided with those MSDUs at the MAC service access point (MAC SAP).

traffic identifier (TID): Any of the identifiers usable by higher layer entities to distinguish medium access control (MAC) service data units (MSDUs) to MAC entities that support quality of service (QoS) within the MAC data service.

NOTE—There are 16 possible TID values; eight identify traffic categories (TCs), and the other eight identify parameterized traffic streams (TSs). ~~The TID is assigned to an MSDU in the layers above the MAC.~~

The parameters that control differentiation of ~~traffic classes~~ access categories using EDCA can be configured by the PCP in a PBSS.

All STAs support the data service, but only QoS STAs in a QoS BSS differentiate their MSDU delivery according to the designated traffic category (TC) or traffic stream (TS) of individual MSDUs.

The Transmit Stream/Category Measurement applies to TIDs for traffic streams associated with TSPECs and also to TIDs for traffic categories for QoS traffic without TSPECs or with traffic classification (TCLAS).

The Transmit Stream/Category Measurement report(M101) applies to TIDs for ~~T~~traffic ~~S~~streams associated with TSPECs and also to TIDs for ~~T~~traffic ~~C~~categories for QoS traffic without TSPECs or with traffic classification (TCLAS).

The Transmit Stream/Category Measurement applies to TIDs for ~~T~~traffic ~~S~~streams associated with TSPECs and

also to TIDs for ~~T~~traffic ~~C~~categories for QoS traffic without TSPECs or with traffic classification (TCLAS).

The backoff procedure shall be invoked by an EDCAF corresponding to a given AC when any of the following events occurs:

a) An MA-UNITDATA.request primitive is received that causes ~~a frame~~ an MPDU with that AC to be queued for transmission such that one of the transmit queues associated with that AC has now become nonempty and any other transmit queues associated with that AC are empty; the medium is busy on the primary channel as indicated by any of the following:

— physical CS;

— virtual CS;

— a nonzero TXNAV timer value;

— a mesh STA that has dot11MCCAActivated true and a nonzero RAV timer value, (#1501)and

the backoff counter has a value of 0 for that AC.

b) The transmission by the EDCAF of ~~the MPDU in~~ the final PPDU transmitted by the TXOP holder during the TXOP ~~for that AC~~ has completed, the EDCAF is the TXOP holder, and the TXNAV timer has expired~~, and the AC was a primary AC~~. (See 10.23.2.7 (Sharing an EDCA TXOP)).

c) The transmission by the EDCAF of an MPDU in the initial PPDU of a TXOP fails, as defined in this subclause, and the MPDU’s AC was ~~a~~the primary AC.

d) The transmission attempt by the EDCAF collides internally with another EDCAF of an AC that has higher priority, that is, two or more EDCAFs in the same STA are granted a TXOP at the same time.(#1507)

In addition, the backoff procedure may be invoked by an EDCAF when:

e) The transmission by the EDCAF~~by the TXOP holder~~ of an MPDU in a non-initial PPDU of a TXOP fails, as defined in this subclause, and the EDCAF is the TXOP holder ***[and the MPDU’s AC was the primary AC, to match c)?]***.

**TBD**

~~4178, 4575, 4576: BSSID is property of BSS not of AP, so should be BSSID of BSS not BSSID of AP; also missing definition of BSSID~~

~~4717, 4718: figures to illustrate higher-AC TXOP sharing~~

~~4137: fields called Reserved that are validated by the receiver~~

4756 with Solomon: unqualified “awake window” (only applies to/problem for 11.2.3.12)? -- at risk of insufficient detail rejection

4738: aRxPHYStartDelay

~~4458: Supported Operating Classes wording inconsistency~~

4760: proprietary code points

4752: \*XVECTORS in Clause 8

4736: operating class meaning flip-flopping

4732: "BSS bandwidth" v "operating channel width" v "BSS operating channel width"

~~4685: S1G join MCS rules~~

4681: “RTT”

~~4583: The AP Channel Report in a BSSDescription should allow for multiple reports~~

~~4550: dot11Class2CapabilitiesOptionImplemented is capability variable?~~

~~4515: TXSTATUS in PHY-TXSTART.confirm isn't actually a transmission status~~

~~4272: Figures 5-1, 5-2 and 5-7 talk of "MSDU flow", but also for MMPDUs and Control frames~~

~~4229: operational MCS set != mandatory MCS set~~

4720: delete SRC/LRC

4712: relay STA add S1G before

4629: RCPI xref -- by Jul 15 -- at risk of insufficient detail rejection

4630: RCPI over PHY SAP -- by Jul 15 -- at risk of insufficient detail rejection

~~4523: on channel starting frequency~~

~~4395: "current ESS" => ESS of AP (not of STA) -- By Jul 15~~

4363: “or both” removal -- at risk of insufficient detail rejection

4298+4299 with Sigurd: definition of "preamble" -- pending Sigurd -- at risk of insufficient detail rejection

4286: list the locations ("EAP authentication") -- pending Jouni

~~4277: BA session definition~~

~~4266: say can't change basic rate/MCS set~~

4402: comma before modal

4414: status/reason code magic numbers

4483: Action field inconsistency -- need direction

4537: uppercase start of caption

4565: arrows in MAC header -- need direction

~~4575: BSSID is of AP or BSS?~~

~~4576: why “BSSID of the IBSS” but not for infra~~

4588: capability bits “Support” or “Supported” -- need direction

4606: differentiate v differentiates etc. -- need direction

4616: use of “Std” -- need direction

4618: receive v. receiver address etc.

4620: case after hyphen in field names -- need direction

4623: ellipsis inconsistency for numerics -- need direction

4624: italics for “x to y” etc, and use minus or en dash

4637: subelements editorials

4662: if v when -- need direction

4676: “the structure of” not canonical ~70 instances

4690: “Beacon Report” -> “Beacon report”

4757: CID 15

4758: RSC v RC v TSC/PN/IPN counter -- need direction

4743: carrier sense terminology

4750: ps/u-apsd description etc.

4754: multirate rules

4699: "remaining txop duration"

4744: OCT to specify peer NT channels

4745: OCT not clear

~~4746: INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME move to 11.3~~

~~4696: do not duplicate length information given in figures (e.g. "is x bits/octets in length", "is an x-bit/octet field")~~

4636: subelements

4562: no A1/A2/A3 stuff in C11 if already in 9.3

~~4557: conflict in EDCA sharing wording~~

4379: “control response frame”

4343: Antenna ID field

~~4263: basic VHT-MCS set rules missing for non-starter of BSS~~

4260 "existing"/"established"

4293 binary fields ambiguous if just a number -- at risk of insufficient detail rejection

~~4365/4364 with MarkH: transmission of the MPDU in the final wotsit~~

4419 with MarkH: STA that implements X

4247 with MarkH: MIB variables default that are capability variable

4291 with Menzo: 20/0150 PCF remnants

4694 with Graham on associate w/ BSSID

BSS with which ~13

BSS to which ~4

Friday 17

4087 with Jouni

4756 with Solomon

4286

4293 todo Wed

4298/99 need Sigurd

4694 need Graham

**References:**

802.11md/D3.0 except where otherwise specified