IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolutions for some comments on 11md/D3.0 (SB1) |
| Date: 2020-05-13 |
| 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 4393Mark 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 4432Mark RISON11 | "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 4451Mark RISON10.23.2.71834.13 | "When an AP supports DL-MU-MIMO, frames from a higher or lower priority AC may be includedin a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 whenthese frames do not increase the duration of the VHT or S1G MU PPDU beyond that required for thetransmissions 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 includedin a VHT or S1G MU PPDU with the TXVECTOR parameter(#2639) NUM\_USERS > 1 whenthe TXOP limit for the primary AC is nonzero." |

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 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) 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 in <this document>, which xx

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4433Mark RISON10.27.3.11902.28 | 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 PPDUwith the TXECTOR FORMAT parameter set to VHT may be substituted for a PPDU with the TXVECTORFORMAT 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) PHYspecification)" to "40 MHz, 80 MHz, 160 MHz and 80+80 MHz transmissions use non-HT duplicate frames defined in Clause 19 (High-throughput (HT) PHYspecification) 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 PPDUPPDUs 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 4582Mark 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 4284Mark RISON9.4.2.20.181043.59 | 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 4204Mark RISON9.4.2.24.31101.29 | 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 authenticationnegotiated over IEEEStd 802.1X is a type of Authenticationnegotiated over IEEEStd 802.1X). Similarly :8 and :9, etc. | Add a column to the table with heading something like "Can be used with PMKSA caching" and then state that this means that the AKM can also be used for the use of a cached PMKSA for a previous AKM of that type, and cross-reference from there to 12.6.10.3 Cached PMKSAs and RSNA key management |
| CID 4205Mark RISON9.4.2.24.31101.29 | 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 authenticationnegotiated over IEEEStd 802.1X is a type of Authenticationnegotiated over IEEEStd 802.1X). Similarly :8 and :9, etc. | Make sure each suite selector has no overlap with other suite selectors |

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).

Proposed changes:

Proposed resolution:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4499Mark 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 4715Mark RISON6.3.68576.10 | 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 4716Mark RISON6.3.68576.10 | 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 4591Mark 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 accordancewith IETF RFC 3986” to “The Public Identifier URI/FQDN field contains a URI as a UTF-8 string, formatted in accordancewith 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 4679Mark RISON9.3.3.1854.23 | "a) The Address 1 field of the Management frame is the RA (=DA) and is determined as the destinationof the frame.b) The Address 2 field of the Management frame is the TA (=SA) and is determined as the address ofthe 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 4689Mark RISON9.4.3 | "The optionalsubelements 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 4809Mark HAMILTON9.6.12.31589.40 | 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 4767Mark HAMILTON5.2.3.2312.7 | 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 4625Mark 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*.

Proposed additional changes:

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**?

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4245Mark RISON10.2.3.21717.62 | 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 4087Rojan Chitrakar12.5.3.4.12608.25 | 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).

Proposed changes:

In D3.0:

In Figure 12-23—CCMP decapsulation block diagram:

* change "MIC" to "Encrypted MIC"
* change "Data" to "Encrypted data" on the left
* lowercase "Nonce"

In Figure 12-18—CCMP encapsulation block diagram:

* change "Data" to "Plaintext data" on the left
* in the arrow out of CCM encryption change label to put "Encrypted data" above the arrow and “Encrypted MIC” below the arrow
* lowercase "Nonce"

In Figure 12-29—GCMP decapsulation block diagram:

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

In Figure 12-27—GCMP encapsulation block diagram:

* change "Data" to "Plaintext data" on the left
* in the arrow out of GCM encryption change label to put "Encrypted data" above the arrow and “MIC” below the arrow
* lowercase "Nonce" and "Header"

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

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

In Figure 12-23—CCMP decapsulation block diagram:

* Change PN ’ to Replay counter

In Figure 12-29—GCMP decapsulation block diagram:

* Change PN\* to Replay counter

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)).

 […]

— 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 12.5.5.4.2 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).

[…]

— 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”.

TBC: the CCMP test vectors with 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.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4087 in <this document>, which tidy up the description of encryption decapsulation and recipient processing.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4612Mark RISON122609.5 | "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!) |

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.

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.

[TBD: and similarly for CCMP PV1 and for GCMP]

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.

The PN subfield shall contain the packet number, with PN0 at the highest octet index.

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 at the highest octet index.

Proposed resolution:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4259Mark 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 4531Mark RISON9 | "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 4543Mark RISON9.4.2.141008.34 | "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 4549Mark RISON9.3.1.2826.15 | "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 4510Mark RISON9.3.1.1824.52 | 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 4505Mark RISON11.41 | 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 4512Mark RISON9.4.2.55.31176.10 | "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 4516Mark RISON9.6.22.4 | Should specify that OMN can be broadcast (discussion with Abhi) | As it says in the comment |

Discussion:

Abhishek PATIL suggests that it might be desirable to broadcast OMN frames in certain situations, because xxx.

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 4353Mark RISON9.3.3.1854.43 | "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 specificBSSID 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 |

Discussion:

It would be better to be clear and consistent.

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 optionally 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). Otherwise, the Address 3 field is a specific BSSID as described in item 4) below.

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, 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, the Address 3 field is the BSSID, irrespective of whether the STA is associated with that AP.

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.

Proposed resolution:

REVISED

Make the changes shown under “Proposed changes” for CID 4353 in <this document>, which address the issue raised by the commenter.

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4413Mark RISON10.2.3.21717.60 | "When communicating within a BSS, the EDCA parameters used are from the EDCA Parameter Set element orfrom the default values for the parameters when no EDCA Parameter Set element is received from the AP ofthe 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 4703Mark 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 4501Mark 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 4247Mark RISONC.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 4314Mark RISON12 | "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 in <this document>, which

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4423Mark 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” to “indicate the recovery duration by including the Recovery Duration field in the Duration field of an NDP (PS-Poll-)Ack frame”.

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 in <this document>, which

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4717Mark RISON10.23.2.71834.4 | 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 4718Mark RISON10.23.2.71834.4 | 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 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. If we’ve agreed to delete HT-delayed BA, then this is moot, but otherwise we need to cover this case
* Table 9-529—A-MPDU contents in the data enabled immediate response context is not totally clear as to whether you’re allows a mixture of TIDs all under HT-immediate BA agreements, as long as all but one are sent with Block Ack ack policy:





Probably not, but not 100% clear to me

Need group discussion

Proposed changes:

Add the figures shown in the F10-xx and F10-yy tabs in this Visio file. Caption them “Illustration of TXOP sharing and PPDU construction (non-A-MPDUs)” and “Illustration of TXOP sharing and PPDU construction (A-MPDUs)” respectively. Append “ (DL MU-MIMO)” to the caption for Figure 10-27.

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

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:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4178Mark 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 4575Mark RISON | Is it BSSID of the AP or BSSID of the AP's BSS? | As it says in the comment |
| CID 4576Mark 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 |
| CID 4177Mark RISON | "BSSID of the [something] frame" -- a frame does not have a BSSID, it has a BSSID field | Change "BSSID" to "BSSID field" in the cited text in 9.4.2.45 Multiple BSSID element, 9.3.2.1.2 Address and BSSID fields, 9.4.2.146 Cluster Report element, 10.40.4 Cluster report and rescheduling (and change "of the received DMG Beacon" to "of the received DMG Beacon frame"), 11.10.15.3 Measurement pilot usage by a STA, 11.16 20/40 BSS Coexistence Management frame usage, 11.25.1.1 Overview, C.3 (for dot11BeaconRprtBSSID) |

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”.

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”.

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”.

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).

Proposed resolution:

REVISED

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

|  |  |  |
| --- | --- | --- |
| Identifiers | Comment | Proposed change |
| CID 4746Mark RISON11.13 | "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

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

|  |  |  |
| --- | --- | --- |
| 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

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)?

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

4630: RCPI over PHY SAP

4523: on channel starting frequency

4395: "current ESS" => ESS of AP (not of STA)

4298+4299 with Sigurd: definition of "preamble"

4286: list the locations ("EAP authentication")

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

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 uplicate 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

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

**References:**

802.11md/D3.0 except where otherwise specified