IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| REVme CIDs assigned to Hamilton | | | | |
| Date: 2024-05-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java Dr  Sunnyvale, CA, 94089 | +1 303 818 8472 | [Mark.hamilton@commscope.com](mailto:Mark.hamilton@commscope.com) |

Abstract

This document contains discussion and proposed resolutions for the following comments from TGme 2nd SA ballot, on IEEE P802.11-REVme/D5.0:

7188, 7105, 7106, 7108, 7113, 7114, 7107, 7115, 7103, 7116, 7187, 7067 (partial)

All references are to D5.0 numbering.

**Revision Notes**

R0 – initial version, with proposed resolutions for CIDs 7188, 7113 (and 7202?), 7114 and 7107.

R1 – Added CID 7187, with same resolution as CID 7188

R2 – Reviewed CIDs that were ready, at San Diego CRC F2F

R3 – Added CID 7067 (partially, only one 11az aspect). Moved some CIDs to “Completed”: 7188, 7187, 7113, 7114, 7107, 7106

R4 – CID 7067 resolution agreed at May session. Corrected the discussion for CID 7067 to not claim that this is the last 802.11az roll-in issue in clause 6.

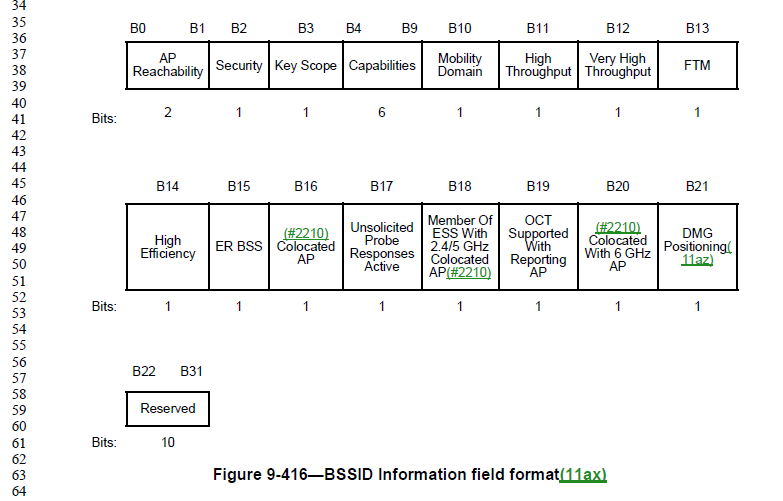
**Ready for Review:**

**CID 7108:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7108 | 9.4.2.35 | 1067.64 | What exactly is the meaning of "DMG positioning". This should be a defined term or better description of when to set this bit. | Define "DMG positioning" term. |

**Discussion:**

**Context,** from 9.4.2.35**:**





The issue is that “the AP supports DMG positioning” is not clear, as this term is never used except in this sentence.

Consulting with 11az SMEs, it seems that what is meant is “the AP is a DMG AP and supports FTM measurement.” and that this is explained in the appropriate subclause(s) of 11.21.6.4, Measurement exchange. Also, “the AP” is ambiguous, as this is a Neighbor Report, so is it the reporting AP, or the AP that is being reported? Other paragraphs in this subclause are clear to say “the reported AP”, or “the AP represented by this BSSID”.

**Proposed Resolution:**

Replace “the AP supports DMG positioning” with “the reported AP is a DMG AP and supports FTM measurement (see 11.21.6.4.2.2 (DMG general measurement exchange)).”

**Not ready yet:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7105 | 9.3.3.5 | 738.20 | What does "ought" mean in this context? "Should"?? "Shall"?? Something non-normative?? Yes, clause 9 is generally not supposed to use normative verbs, but here the intent is now entirely unclear. | Replace "ought" with understandable phrasing. Same thing at P738.31, P741.57, P742.11, P746.48, P746.59, P752.17, P752.28, P757.16, P757.29, P760.16, and P761.11. |
| 7115 | C.1 | 5252.24 | Which attributes only apply to the link with the AP? Do some atrributes only apply to the direct link then (and not the link with the AP), or even not to non-TDLS operation? This information should be in the DESCRIPTION of the affected attributes, not a hand-wave at the start of Annex C. | As in comment.  Attributes are: dot11TDLSPeerUAPSDBufferSTAActivated,  dot11TDLSPeerPSMActivated,  dot11TDLSPeerUAPSDIndicationWindow,  dot11TDLSChannelSwitchingActivated,  dot11TDLSPeerSTAMissingAckRetryLimit,  dot11TDLSResponseTimeout,  dot11OCBActivated,  dot11TDLSNavSync,  dot11TDLSACDeterminationInterval |
| 7103 | M.1 | 6103.19 | "As specified in IEEE Std 802, EPD encoding always starts with a Length/Type field…" IEEE Std 802 doesn't say that. In fact, IEEE Std 802's subclause on encoding is being re-written to clarify all the options for both EPD and LPD. This text needs to align. | (As IEEE Std 802 language stabilitzes) re-write this text to align. |
| 7116 | R.3.2. | 6135.8 | Figure R-1 and text in R.3.2 is very confusing with respect to multiple BSSs served by "the same physical AP". This seems to be referencing an "AP device", perhaps? But the BSS(s?) in the figure are not separated, with a separate Portal for each. | As in comment.  Emailed Stephen, May 9. No history on this, yet?? |

**Completed:**

**CIDs 7188 and 7187 (GEN):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7188 | 4.3.1 | 274.1 | Is the BSA "The area containing the members of a basic service set (BSS)." per Clause 3 or is it "the coverage area within which all the member STAs of the BSS can remain in communication" per Clause 4? The latter is typically bigger than the former, since if a STA moves a little further away it will typically still be able to be heard. | Change the Clause 3 definition to be the Clause 4 definition |
| 7187 | 4.3.1 | 274.3 | "If a STA moves out of the BSA, it can no longer directly communicate with all the other STAs present in the BSA." -- in a infra BSS it doesn't need to, it only needs to communicate with the AP | Not sure how to express this |

**Discussion:**

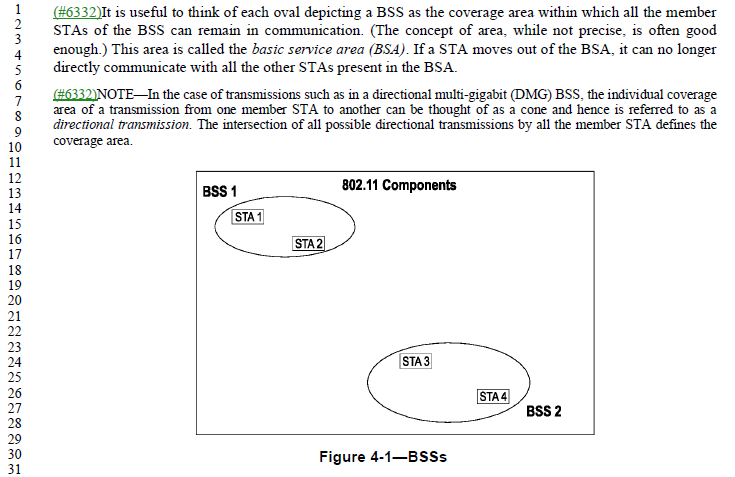
P195.1 (clause 3.1):



Thus, a strict read of this says that the BSA is dynamically resizing, as it just (exactly) surrounds all the members of the BSS. For example, if no non-AP STA is very far from an AP (in an infrastructure BSA), then the BSA is fairly small.

In fact, an AP that has no associated non-AP STAs has an ill-defined BSA, because it is just the area that contains the AP. Is that just a few square centimeters? Or, is the BSA supposed to be the area covered by the AP’s transmissions (Beacons) – if so, to what signal level/SNR/etc?

But, in clause 4, we have (P274.1):



This has text saying it is “the coverage area within which all the members STAs can remain in communication.” That seems like a more useful definition, or at least closer to how we think about it.

Of course, this phrasing leaves some open questions:

1. What is “the coverage area” – again, to what signal strength (or other measure) does the “coverage area” extend? And, in 4.3.6, there is a tidy statement: “For wireless PHYs, well-defined coverage areas simply do not exist.” Which points out that propagation is both dynamic and unpredictable.
2. To which peer devices does a STA have to “remain in communication”? For an infrastructure BSS, that is probably each non-AP STA is in communication with the AP. But, they might not be “in communication” (within range) of each other. In an IBSS or PBSS, the STAs need only talk to the peer STAs of interest. Although, we then get into DMG clusters and PCPs…

Subclause 4.3.6 attempts to put human understandable concepts to this, in defining “area concepts” that are of interest to 802.11. That subclause is pretty clear that a strict definition will be both not accurate and not useful. The point of these terms (that use “area”) are to provide a useful human concept.

**Proposed Resolution:**

CIDs 7188 and 7187:

Revised.

At P195.1, change the definition of BSA to:

“The area in which the members of a basic service set (BSS) are able to communicate with eachother such that necessary services of the BSS can be provided, such as synchronization and data transfer.

NOTE—The extent of a given BSA is unlikely to be strictly definable, nor static. See 4.3.6 for further discussion.”

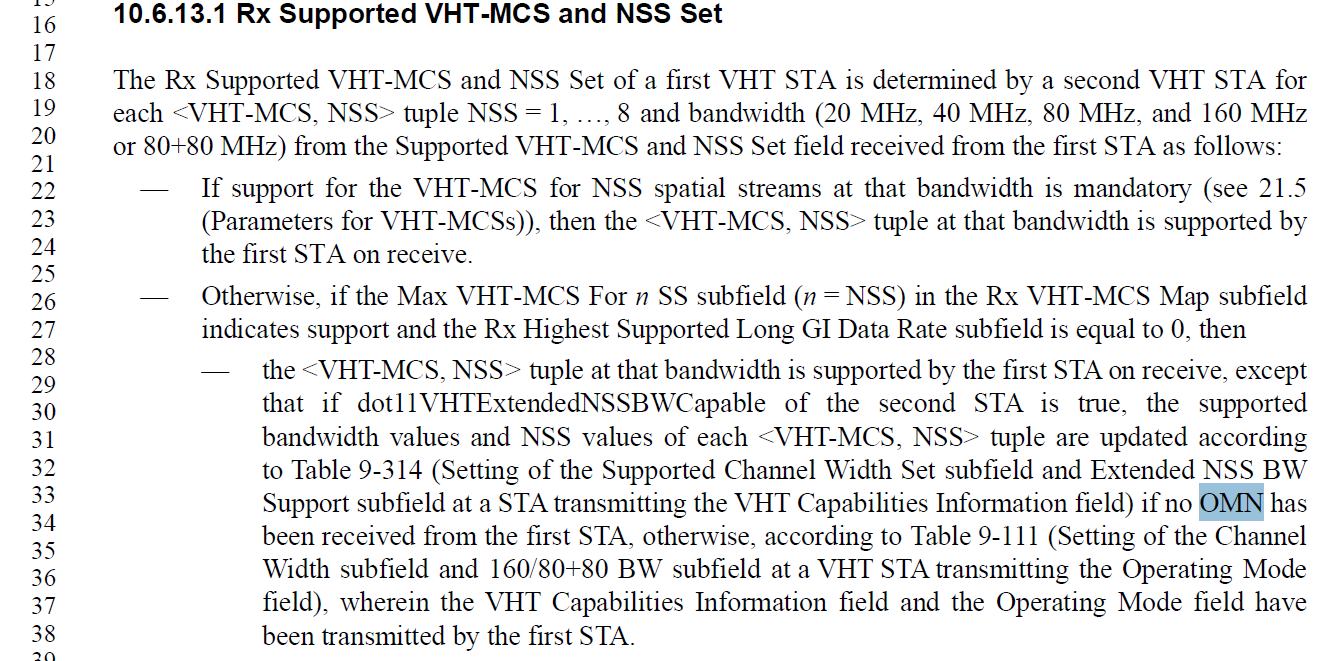
**CID 7113 (MAC):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7113 | 10.6.13.1 | 1971.33 | What is "OMN"? This term/acronym is not defined anywhere (and is used 6 times, including once claiming it is a type of frame). | Define OMN term/acronym in clause 3. |

**Discussion:**

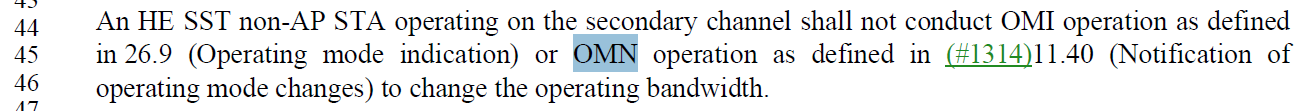
Examples of the 6 uses are:

P1971.34:

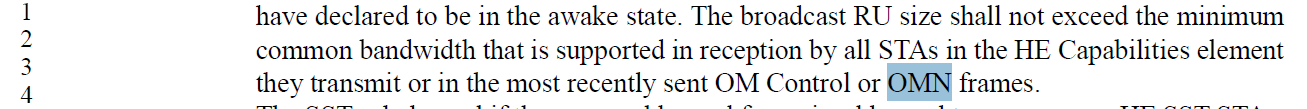


And, same thing in the next bullet, and in two bullets in TX Supported VHT-MCS and NSS Set.

P4148.44 (in 26.8.7.2 SST operation):



And P4190.3 (within the rules for Broadcast RU in HE MU PPDU):



Note that this CID overlaps with CID 7202 (which is in “Review”):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7202 | 26.15.7 | 4190.3 | "OMN frames" -- no such frames | Change to "Operating Mode Notification frames" |

In this last location, the expansion of “OMN” and referencing “frames” seems appropriate.

At P4148.44, it also works to expand “OMN” to “Operating Mode Notification” as it applies to that ‘operation’.

However, at the P1971.34 location, there is no noun to go with an expanded “Operating Mode Notification” adjective. Suggest, from context, that since it talking about “no OMN has been received”, it seems to also be a reference to the frame.

**Proposed Resolution (CID 7113):**

Revised.

At P1971.34, P1971.49, P1972.26, and P1972.43, replace “OMN” with “Operating Mode Notification frame”

At P4148.44, replace “OMN” with “operating mode notification”

At P4190.3, replace “OMN” with “Operating Mode Notification”

Note to Editor: This is aligned with “Accepted” for CID 7202.

**CID 7114(MAC):**

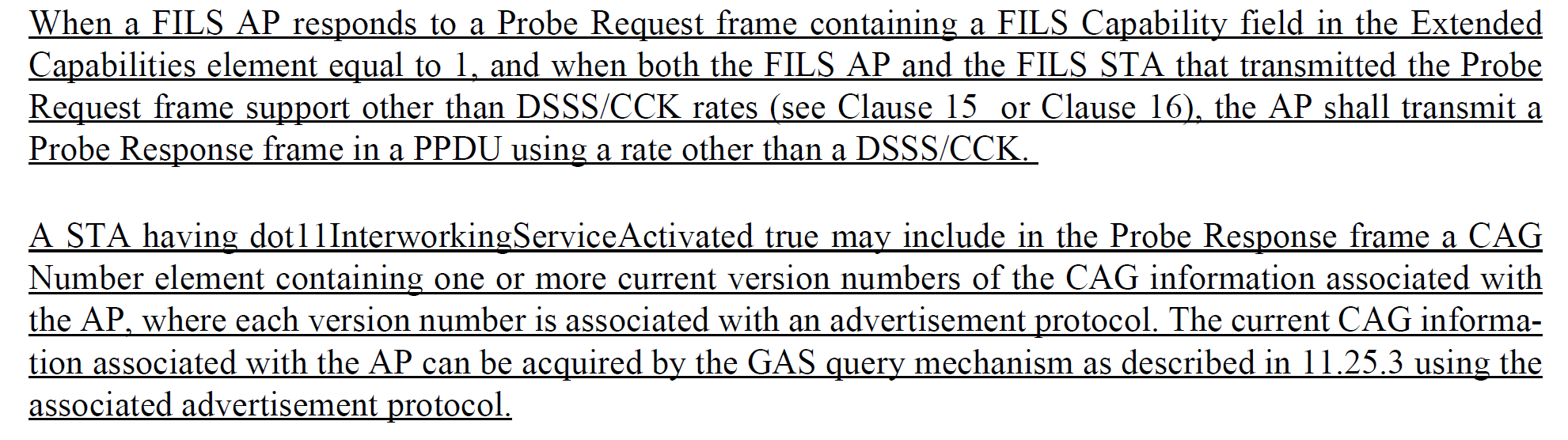
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7114 | 11.1.4.3.9 | 2479.51 | This isn't a sentence. Fix it to be something about the transmitting STA shall do something with the Number element. I don't know what it's supposed to say, sorry. | As in comment. |

**Discussion:**

From 11.1.4.3.9 Contents of a probe response, on P2479.51:



These paragraphs came from 802.11ai-2016, P102:



It appears that a line of text got lost, in IEEE Std 802.11-2020.

**Proposed Resolution:**

Revised.

At P2479.51, Add to the start of this paragraph:

“A STA having dot11InternetworkingServiceActivated true may include in the Probe Response frame a CAG”

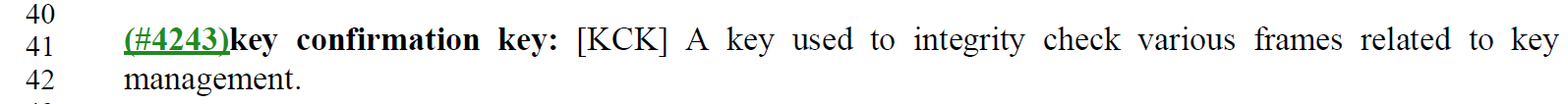
**CID 7107 (SEC);**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7107 | 12.7.8.2 | 3118.8 | The terms "TPK-KCK" and "TPK-TK" need to be understood in numerous places. Finding the definition (only) here is very awkward. | Add definitions for these terms in clause 3, and acronyms in 3.4. |

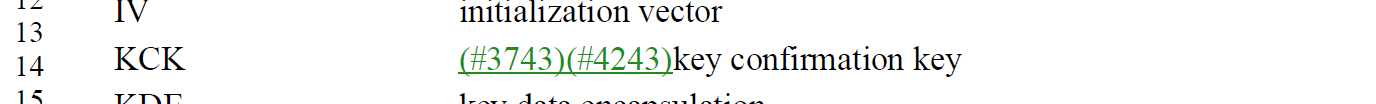
**Discussion:**

The KCK (key confirmation key) concept, in general, is well defined in the definitions and acronyms.

P231.41:



P263.14:



There are KCKs for many keys, PTK, SAE, and PASN PTKSA, in addition to TPK. Each of these, is defined locally within their respective specifying subclauses. There appears no reason to make the TPK-KCK and TPK-TK different, by defining these terms differently and introducing more duplication in the Standard.

**Proposed Resolution:**

Rejected. There are KCKs for many keys, PTK, SAE, and PASN PTKSA, in addition to TPK. There is a formal definition (and acronym expansion) for “KCK” as a general concept. Each of the specific KCKs, are defined locally within their respective specifying subclauses. There appears no reason to make the TPK-KCK and TPK-TK different, by defining these terms differently and introducing more duplication in the Standard.

**CID 7106 (MAC):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7106 | 9.4.2.23.3 | 1023.46 | There are "Editor's Note"s still in the draft | Clean up the "Editor's Note"s |

**Discussion:**

Per discussion on April 17 (at San Diego F2F ad hoc), it is believed that all the Editor’s Notes have specific CIDs already filed on this ballot. Thus, there is no further work to do on this “blanket” comment. The easiest disposition is just to note that the commenter was not sufficiently specific.

**Proposed Resolution:**

Rejected. The comment fails to provide sufficient detailed changes that would satisfy the commenter.

**Under CID 7067, the issue involving 802.11az subclause 6.3.56 merge into REVme’s clause 6 (or clause 11) structure:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page/Line** | **Comment** | **Proposed Change** |
| 7067 |  |  | Contents in Clause 6 of 11az, 11bd and 11bc cannot be rolled-in due to the Clause 6 structure changes in REVme. This can be resolved by a submission. | as in comment. |

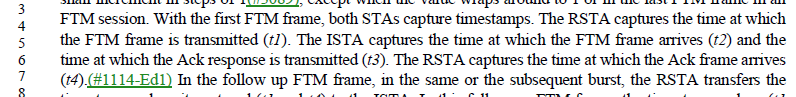
**Discussion:**

**This document only addresses one ~~(the last remaining?)~~ item for 11az, which is rolling in subclause 6.3.56.**

Subclause 6.3.35 was removed as part of the clause 6 restructuring. It was felt at that time (prior to 802.11az-2022) that the details in subclause 6.3.56 were not needed, and FINETIMINGMSMTRQ and FINETIMINGMSMT primitives were changed to entries in Table 6-1 with no further discussion in clause 6.

However, 802.11az-2022 includes changes to this subclause, and upon further review, inspired by looking at the changes to Figure 6-17 in 802.11az-2022, it seems that this figure includes information not represented anywhere else in the draft, in particular the very careful location of where the timestamps t1, t2, t3 and t4 are captured, which is to say, at the antenna connector. Thus, it seems that Figure 6-17 is still useful/necessary, to fully understand how to implement the procedures of 11.21.6.

The definitions of t1 – t4 are in 11.21.6, in the paragraph at the top of P2719 (REVme D5.0):



Thus, it is proposed to add Figure 6-17 (as modified by 802.11az-2022) into this paragraph.

Also, 802.11az-2022 added new figures in 6.3.35 which helps understand the MLME’s responsibilities and the relationship between the MLME primitives (to/from the SME) and the frame exchanges. These relationships are not obvious, this author claim, and would be good to keep in the 802.11 Draft. It seems that other subclauses of 11.21.6.4 are a good place to put this material.

**Proposed Resolution:**

Revised.

***On P2718.60 (and on to page 2719), split the paragraph, move Note 2, and insert text and Figure 6-17 (as modified by 802.11az-2022 and renumbered as Figure 11-xx), as shown:***

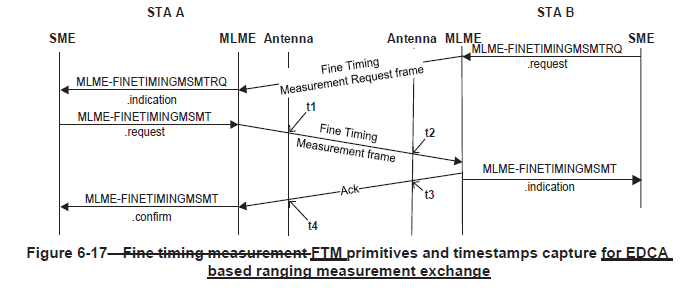
A (11az)RSTA transmits FTM frames in overlapping pairs of consecutive frames. For example, in Figure 11-45 (Example negotiation and measurement frame exchange, ASAP=1, and FTMs Per Burst = 2(#109)(11az)), FTM\_1 and FTM\_2, FTM\_2 and FTM\_3, and FTM\_3 and FTM\_4 are overlapping pairs of consecutive frames. The first FTM frame of a pair of consecutive FTM frames contains a nonzero value in the Dialog Token field. The follow up FTM frame contains a Follow Up Dialog Token field set to the value of the Dialog Token field in the first frame of the consecutive pair. Dialog Token field values of consecutive FTM frames shall increment in steps of 1(#3089), except when the value wraps around to 1 or in the last FTM frame in an FTM session. ***<insert para break here, and move NOTE 2 to follow this paragraph, as shown:>***

NOTE 2—(11az)An FTM frame can contain nonzero values in both the Dialog Token and Follow Up Dialog Token fields, meaning that the Action frame contains follow up information from a previous measurement, and new Timestamp values are captured to be sent in a future follow up FTM frame.

With the first FTM frame, both STAs capture timestamps. The RSTA captures the time at which the FTM frame is transmitted (*t1*). The ISTA captures the time at which the FTM frame arrives (*t2*) and the time at which the Ack response is transmitted (*t3*). The RSTA captures the time at which the Ack frame arrives (*t4*).(#1114-Ed1) In the follow up FTM frame, in the same or the subsequent burst, the RSTA transfers the timestamp values it captured (*t1* and *t4*) to the ISTA. In this follow up FTM frame, the timestamp values (*t1* and *t4*) shall be the measurement according to the RSTA’s clock (i.e., without applying any frequency offset correction to the time bases).

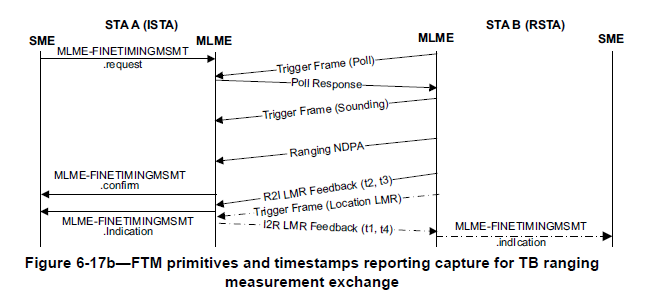
For the above timestamp captures, t1 and t3 correspond to the point in time at which the start of the preamble for the transmitted FTM frame appears at the antenna connector during transmit (see Figure 11-xx). An implementation may capture a timestamp during the transmit processing earlier or later than the point at which it actually occurs and offset the value to compensate for the time difference.

Timestamp captures t2 and t4 correspond to the point in time at which the start of the preamble for the incoming FTM frame arrives at the receive antenna connector (see Figure 11-xx). Because time is needed to detect the frame or the relevant LTF in the preamble and synchronize with its logical structure, an implementation determines when the start of the preamble or the relevant LTF in the preamble for the incoming frame arrived at the receive antenna connector by capturing a timestamp some time after it occurred and compensating for the delay by subtracting an offset from the captured value.



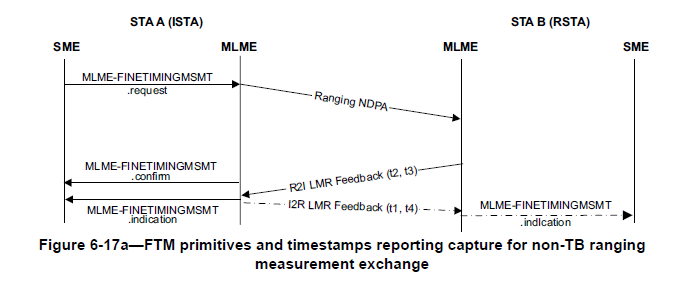
***At P2727.50, add a paragraph, and Figure 6-17b from 802.11az-2022 and renumbered as Figure 11-yy, to the end of subclause*** ***11.21.6.4.3.1:***

The structure of the FTM protocol for a TB ranging measurement exchange and its relationship with the SME and MLME interface is shown in Figure 11-yy.



***At P2735.24, add a paragraph, and Figure 6-17a from 802.11az-2022 and renumbered as Figure 11-zz, to the end of subclause 11.21.6.4.4.1:***

The structure of the FTM protocol for a non-TB ranging measurement exchange and its relationship with the SME and MLME interface is shown in Figure 11-zz.



***At P2727.50, add a paragraph, and Figure 6-17c from 802.11az-2022 and renumbered as Figure 11-qq, to the end of subclause 11.21.6.4.8.1:***

The structure of the FTM protocol for a passive TB ranging measurement exchange and its relationship with the SME and MLME interface is shown in Figure 11-qq.

