IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **11bk Spec text for NDP Announcement** | | | | |
| **Date:** 2023-04-18 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yanjun Sun | Qualcomm |  |  |  |
| Ali Raissinia |  |  |  |  |
| Steve Shellhammer |  |  |  |  |
| George Cherian |  |  |  |  |
|  |  |  |  |  |

Abstract

We propose the draft specification skeleton for NDP Announcement to help the creation of TGbk draft D0.1.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: updated the text base on feedback during March meeting and updates in 11be spec text
* Rev 2: updated the text from page 3 to the end based on inputs from the Apr 4th call

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbk 0.1 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbk D0.1 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbk Editor: Editing instructions preceded by “TGbk Editor” are instructions to the TGbk editor to modify existing material in the TGbk draft. As a result of adopting the changes, the TGbk editor will execute the instructions rather than copy them to the TGbk Draft.***

**Discussion:**

The text is prepared for the following motion:

The Ranging NDP Announcement frame of 802.11bk will use the existing 320MHz indication of 802.11be:

* There is no change to the 802.11az Ranging NDP Announcement MAC content
* For a non-HT dup PPDU: set B7 in SERVICE field to 1 to indicate 320 MHz
* For an EHT MU PPDU: use the Bandwidth field in the U-SIG field to indicate 320 MHz

(11-23-48: 202301-12)

**Proposed spec text:**

***Discussion****: in 11be D3.1, the spec text on 320 MHz indication for NDP Announcement frame is made general and covers Ranging NDP Announcement frame in a 320 MHz non-HT Duplicate PPDU based on the following text:*

*9.3.1.19 NDP Announcement frame format*

*9.3.1.19.1 General description*

*The TA field is set to the address of the STA transmitting the NDP Announcement frame or the bandwidth signaling TA of the STA transmitting the NDP Announcement frame (see 9.2.4.3.8 (TA field) and 10.6.6.6 (Channel Width selection for Control frames)).*

*10.6.6.6 Channel Width selection for Control frames*

*NOTE 3—The TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT is carried in the scrambling sequence and the SERVICE field (see 17.3.5.2 (SERVICE field)). The allowed values for these TXVECTOR parameters are also specified in 17.3.5.2 (SERVICE field).*

*17.3.5.2 SERVICE field (CONTEXT: part of 17.3 OFDMA PHY)*

*If the CH\_BANDWIDTH\_IN\_NON\_HT parameter in the TXVECTOR primitive is not present or is present and is equal to CBW20, CBW40, CBW80, CBW160, or CBW80+80, then bit 7 of the SERVICE field is set to 0. If the CH\_BANDWIDTH\_IN\_NON\_HT parameter in the TXVECTOR primitive is present and is equal to CBW320, then bit 7 of the SERVICE field is set to 1.*

*and the following for EHT MU PPDU:*

Table

Description automatically generated

*so similar text is added below for 320 MHz Ranging NDPA*

***TGbk editor: Please note Baseline is REVme\_D2.1, IEEE 802.11az-2022 and IEEE 802.11be D3.1***

**35. Extremely high throughput (EHT) MAC specification**

**35.14 PPDU format, BW, MCS, NSS, and DCM selection rules**

**35.14.2 PPDU format selection**

***TGbk editor: Please add the following paragraph for NDPA (track changes enabled):***

A Ranging NDP Announcement frame for 320 MHz mode shall be transmitted in a non-HT Duplicate PPDU or EHT MU PPDU.

***TGbk editor: Please update 11.21.6.4 as follows (track changes enabled):***

**11.21.6.4 Measurement exchange**

**11.21.6.4.3 TB ranging measurement exchange**

**11.21.6.4.3.1 General**

TB ranging is the dynamic trigger-based variant of the FTM procedure. The TB ranging measurement exchange consists of one or more scheduled availability windows. The TB ranging measurement exchange is dynamic, as the actual number of ISTAs participating in the measurement exchange can vary across availability windows. Each ISTA that is assigned to the scheduled availability window may participate in or skip the corresponding measurement exchange. The availability windows are scheduled periodic time windows assigned to ISTAs during negotiation (see [11.21.6.3.3](#H11o21o6o3o3) Negotiation for TB ranging measurement exchange).

Within each availability window the RSTA and ISTAs shall not transmit or trigger transmission of any Data frames; they shall only perform ranging activities related to Polling, Measurement Sounding and Measurement Reporting phases, as well as signaling of modification of availability window parameters; see [11.21.6.5.1](#H11o21o6o5o1) (Availability window parameter modification), and TB ranging session termination, see [11.21.6.6.2](#H11o21o6o6o2) (TB ranging and non-TB ranging session termination) . Each availability window by default consists of a single TXOP and may be extended to multiple TXOPs by announcement, if a single TXOP is insufficient to accommodate all ISTAs that responded to the poll; see [11.21.6.4.3.2](#H11o21o6o4o3o2) (Polling phase of TB ranging), and [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement sounding phase of TB ranging). Each availability window of the TB ranging measurement exchange consists of one or more triplets of sequential phases: Polling phase, Measurement Sounding phase and Measurement Reporting phase. Figure [11-37a](#F11o37a) (TB ranging availability windows each with one instance of a polling/sounding/reporting triplet) shows an example of two availability windows, each composed of a single triplet of Polling, Measurement Sounding and Measurement Reporting phases. An RSTA and ISTA participating in TB ranging shall perform any Polling, Measurement Sounding, and Measurement Reporting phases only within the availability windows. 

**Figure 11-37a—TB ranging availability windows each with one instance of a polling/sounding/reporting triplet**

Each availability window typically contains a single poll, where the RSTA should poll all the ISTAs assigned to that availability window. If the available bandwidth is insufficient to allow for the polling of all ISTAs assigned to the availability window with one poll, the RSTA shall indicate that one or more extra polling/sounding/reporting triplets can be expected within the availability window (see example in Figure [11-37b](#F11o37b) (TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP), and Figure [[11-37c](#F11o37c)](#F11o36c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs). All instances of polling/sounding/reporting triplets shall be completed before the end of the availability window.

During the availability window, measurement resources and results shall be made available to each ISTA whose poll response was received at the RSTA; see [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement Sounding phase of TB ranging) and [11.21.6.4.3.4](#H11o21o6o4o3o4) (Reporting Phase of TB ranging Measurement). This may also lead to extra instances of polling/sounding/reporting triplets, even if all ISTAs assigned to this availability window were polled in the first Polling phase instance (e.g., if the RSTA is not able to accommodate all ISTAs that responded in a single measurement sounding phase instance; see [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement sounding phase of TB ranging).

The timestamps reported within each measurement sounding phase shall be derived from a clock that runs continuously during the measurement sounding phase.

If there is a discontinuity in the clock for the FTM timestamping between two reported TOD timestamps, then the TOD Not Continuous subfield in the TOD Error field of LMR frame shall be set to 1. Otherwise it shall be set to 0.

NOTE - In some use cases it is of interest to have a clock that runs continuously across subsequent ranging availability windows. For this reason it is desirable for the clock for the FTM timestamping to run continuously.

Within each availability window, an RSTA shall use an AID or Ranging Session ID (RSID) to identify an associated or unassociated ISTA respectively. The AID and RSID assignment shall be nonconflicting and shall have the same size and valid address space (as defined in 9.4.1.8 and 26.17.4). The RSID usage shall follow the same rules as that of AIDs for HE operations. The RSIDs are assigned to unassociated ISTAs during the FTM negotiation; see [11.21.6.3](#H11o21o6o3) (FTM procedure negotiation).

An RSTA shall follow the rules defined in [26.5.2](#H26o5o2) (UL MU Operation) when transmitting any Trigger frames of variant Location for TB ranging with the following rules:

* A Ranging Trigger frame shall be carried in an S-MPDU if the Ranging Trigger frame is carried in a VHT PPDU or HE PPDU
* An RSTA shall not transmit a Ranging Trigger frame in a VHT MU PPDU or HE MU PPDU.

An RSTA shall not transmit a Sounding Ranging Trigger frame soliciting an HE TB Ranging NDP that uses UL MU-MIMO, i.e., where the same RU is allocated to multiple ISTAs, to any ISTA from which it has not received a TB specific subelement in the Ranging Parameters element with the Full Bandwidth UL MU-MIMO field equal to 1.

If required, an ISTA shall transmit any FTM Request frames outside of Availability Windows allocated to itself. Inside Availability Windows allocated to itself, an ISTA shall not transmit any frame except when assigned UL resources by a TF transmitted by the RSTA.

An RSTA, in which dot11MultiBSSIDImplemented is true, and that transmits a Ranging Trigger frame or a Ranging NDP Announcement frame to a set of ISTAs, in which at least two ISTAs have a TB ranging measurement exchange with different BSSIDs in the Multiple BSSID set of the RSTA shall set the TA field of these frames to the transmitted BSSID. Any ISTA that negotiates a TB ranging measurement exchange session with a nontransmitted BSSID of an RSTA shall support the reception of a Control frame with TA equal to the transmitted BSSID.

An ISTA shall follow the rules defined in Subclause [26.5.2](#H26o5o2) (UL MU Operation) when transmitting any HE TB PPDUs for TB ranging with the exceptions defined in [11.21.6.4.3.2](#H11o21o6o4o3o2) (Polling Phase of TB ranging), [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement Sounding phase of TB ranging) and [11.21.6.4.3.4](#H11o21o6o4o3o4) (Reporting phase of TB ranging measurement).



**Figure 11-37b—TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP**



**Figure 11-37c—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs**

**11.21.6.4.3.2 Polling phase of TB ranging**

The Polling phase is the first phase of each polling/sounding/reporting triplet.

Each Polling phase instance includes at least one Poll Ranging Trigger frame, see [9.3.1.22.10](#H09o3o1o22o10) (Ranging Trigger variant), and no more than one which it receives a response from at least one ISTA ; The Ranging variant Trigger frame of poll is called the TF Ranging Poll frame . The RSTA shall allocate each RU in the TF Ranging poll to only one ISTA. Any ISTA addressed by a User Info field in a TF Ranging Poll frame that intends to participate in the measurement sequence within this availability window shall send a CTS-to-self in an S-MPDU within an HE TB PPDU in its designated RU allocation as identified in the TF Ranging Poll frame, otherwise shall not send a CTS-to-self to avoid resource allocation in this measurement sequence; see Figure [11-37c](#F11o37c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs).

If the available bandwidth does not allow for the polling of all ISTAs assigned to this availability window using a single TF Ranging Poll frame, the RSTA shall attempt to schedule one or more extra polling/sounding/reporting triplets within the availability window. The RSTA shall indicate the extra polling/sounding/reporting triplets by setting the More TF subfield in the Common Info field to 1 and the RA field to the broadcast address in the TF Ranging Poll frame, and in TFs in subsequent Polling, Measurement Sounding and Measurement Reporting phases in the same availability window. If the RSTA had set the More TF subfield to 1 in the preceding Ranging Trigger frame, and if there are no additional polling/sounding/reporting triplets in the same availability window, the RSTA shall set the More TF subfield in the Common Info field to 0 and the RA field to the broadcast address in the next Ranging Trigger frame within that availability window. On receipt of such a frame, an ISTA that has not been addressed by a User Info field in the TF, may enter doze state, if no other condition requires this STA to remain awake. Any extra polling/sounding/reporting triplets can either be transmitted in the same TXOP: see example in Figure [11-37b](#F11o37b) (TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP); or a new TXOP, see example in Figure [[11-37c](#F11o37c)](#F11o36c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs) depending on the maximum allowed TXOP duration and the predicted length of the extra instances of polling/sounding/reporting triplets.



**Figure 11-37d—TB ranging availability window with two ISTAs**

**11.21.6.4.3.3 Measurement sounding phase of TB ranging**

The measurement-sounding phase commences SIFS time after the Polling phase and is the second phase of each polling/sounding/reporting triplet; see Figure [11-37d](#F11o37d) (TB ranging availability window with two ISTAs). The measurement sounding phase consists of one or more Sounding Ranging Trigger frames; see [9.3.1.22.10](#H09o3o1o22o10) (Ranging Trigger variant) allocating uplink resources to one or more ISTAs; see Figure [11-37a](#F11o37a) (TB ranging availability windows each with one instance of a polling/sounding/reporting triplet), and Figure [[11-37c](#F11o37c)](#F11o36c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs). The Ranging variant Trigger frame of sounding subvariant is called the TF Ranging Sounding frame. Each TF Ranging Sounding frame shall allocate uplink resources for one or more ISTAs’ I2R NDP multiplexed in the spatial stream domain covering the full bandwidth. The format of the I2R NDP is either an HE TB Ranging NDP; see [[27.3.18a.2](#H27o3o18ao2)](#H27o3o18b) (HE TB Ranging NDP) or an EHT TB Ranging NDP; see [TBD](#H27o3o18b) (EHT TB Ranging NDP). SIFS time after receiving the last I2R NDP, the RSTA shall transmit an NDP Announcement frame followed by a R2I NDP ; the Ranging NDP Announcement frame is described in [9.3.1.19](#H09o3o1o19) and the R2I NDP is an HE Ranging NDP as described in  [[27.3.18a.1](#H27o3o18ao1)](#H27o3o18a) (HE Ranging NDP) or an EHT Ranging NDP as described in TBD (EHT Ranging NDP). Figure [[11-37d](#F11o37d)](#F11o36d) shows an availability window with an RSTA and two ISTAs (ISTA 1 and ISTA 4) responding to the poll. The Ranging NDP Announcement frame’s STA Info fields specify all the ISTAs that will use the R2I NDP, which shall include the ISTAs that were allocated uplink resources in the measurement sounding phase.

NOTE--The 320 MHz bandwidth of the Ranging NDP Announcement frame is indicated based on rules in 17.3.5.2 (SERVICE field) if the frame is transmitted in a non-HT Duplicate PPDU or based on rules in Table 36-28 (U-SIG field of an EHT MU PPDU) if the frame is transmitted in an EHT MU PPDU.

The RSTA shall select a bandwidth value for the measurement sounding phase that is less than or equal to the RSTA Assigned Max Bandwidth of each of the ISTAs that are being allocated resources during this measurement instance. It may be different from the bandwidth used in the Polling phase, but shall adhere to the rules of multiple frame transmission in an EDCA TXOP; see 10.23.2.8 (Multiple frame transmission in an EDCA TXOP).

The RSTA shall set the TXVECTOR parameter CH\_BANDWIDTH of the Trigger frame Ranging Sounding to that same bandwidth and use the same value for the UL BW subfield of the Common Info field of said Trigger frame. When transmitting the Ranging NDP Announcement frame and R2I NDP, the RSTA shall set the TXVECTOR parameter CH\_BANDWIDTH to that same bandwidth.

If the TF Ranging Sounding frame is transmitted in a 320 MHz PPDU, the I2R NDP shall be an EHT TB Ranging NDP. If the TF Ranging Sounding frame is transmitted in a PPDU of 160 MHz or less, the I2R NDP shall be an HE TB Ranging NDP.In the TF Ranging Sounding, the RSTA shall set the SS Allocation subfield and the I2R Rep subfield of the User Info fields corresponding to each of the ISTAs triggered by the Trigger frame in the following way:

* The Number of Spatial Streams in each SS Allocation subfield shall not exceed the *RSTA Assigned I2R STS ≤ 80 MHz* for the corresponding ISTA, if the UL BW subfield in the Common Info field indicated a bandwidth less than or equal to 80 MHz, and not exceed the *RSTA Assigned I2R STS > 80 MHz* for the corresponding ISTA otherwise
* All the I2R Rep subfields in the User Info fields of the TF Ranging Sounding shall be set to the same value. This value indicates the number of LTF repetitions in the I2R NDP preamble and shall not exceed any of the *RSTA Assigned I2R Rep* corresponding to the ISTA triggered by this Trigger frame.
* The product of the number of LTF repetitions, indicated in each of the I2R Rep subfields of the User Info fields, and the number of HE-LTF symbols, indicated in the Number Of HE-LTF Symbols And Midamble Periodicity subfield in the Common Info field, shall not exceed the *RSTA Assigned I2R LTF Total* for any of the ISTA triggered by this Trigger frame.

After transmission of the TF Ranging Sounding, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 0, and
* the LTF\_NSTS and LTF\_REP parameter vectors set to the same values as indicated, respectively, by the SS Allocation and I2R Rep subfields of all the User Info fields

Similarly, in the Ranging NDP Announcement frame, the RSTA shall set the R2I NSTS subfield and R2I Rep subfield of the STA Info fields corresponding to each of the ISTAs, addressed by that frame in the following way

* The R2I NSTS subfield value shall not exceed the *RSTA assigned R2I* *STS ≤ 80 MHz* for the corresponding ISTA, if the TXVECTOR parameter CH\_BANDWIDTH for this Ranging NDP Announcement frame is less than or equal to 80 MH, and not exceed *RSTA assigned R2I STS > 80 MHz* for the corresponding ISTA otherwise.
* The number of LTF repetitions in the R2I Rep subfield shall be set to a value not to exceed the *RSTA Assigned R2I Rep*, for the corresponding ISTA.
* The combination of the values of the R2I NSTS and the R2I Rep shall not lead to a total number of LTF that exceeds the *RSTA Assigned R2I LTF Total* for each corresponding ISTA.

After reception of the Ranging NDP Announcement frame, the ISTAs’ MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 0, and
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the R2I NSTS and R2I Rep subfields of the STA Info field addressed to it.

The RSTA shall set a different value than the previous transmission in the Sounding Dialog Token Number field in its transmitted Ranging NDP Announcement frame as part of each Measurement Sounding phase. Measurement instances are associated with the Sounding Dialog Token Number field value.

The R2I NDP is transmitted SIFS after the Ranging NDP Announcement frame; if the bandwidth is equal to 320 MHz, the R2I NDP shall be an EHT Ranging NDP, as described in TBD (EHT Ranging NDP), otherwise the R2I NDP shall be an HE Ranging NDP.



**Figure 11-37e—TB ranging availability window with multiple TF Ranging Sounding frames**

The RSTA may schedule some ISTAs that replied during the Polling phase to the first measurement sounding phase instance and other ISTAs to one of possibly multiple extra measurement sounding phase instances; see Figure [[11-37b](#F11o37b)](#F11o36b) (TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP), and Figure [[11-37c](#F11o37c)](#F11o36c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs). The RSTA shall only schedule measurement sounding resources to an ISTA in a measurement sounding instance, if a valid poll response was received from that ISTA in the corresponding Polling phase instance. This may require an RSTA to poll an ISTA multiple times. This is necessary, for example, if different ISTAs have varying, incompatible RSTA Assigned Max Bandwidth values or if the RSTA wants to limit the time duration of each range measurement sounding instance.

Both RSTA and ISTA perform RTT measurements by capturing the timestamps of the NDP. The ISTA shall record the time at which the I2R NDP is transmitted (t1). The RSTA shall then capture the time at which the I2R NDP arrives (t2) and shall record the time at which the R2I NDP is transmitted (t3). The ISTA shall finally captures the time at which the R2I NDP arrives (t4); see Figure [11-37f](#F11o37f) (Timing diagram of a Measurement Sounding phase in TB ranging). The timestamp values t2 and t3 shall be measured according to the RSTA’s clock (i.e., without applying any frequency offset correction to the time basis).



**Figure 11-37f—Timing diagram of a measurement sounding phase in TB ranging**

The Round Trip Time (RTT\_ISTA) observed by ISTA is defined as:

RTTISTA = [(t4-t1) – (t3’-t2’)]

where t3’ and t2’ are the time at which the R2I NDP was transmitted and the time at which the I2R NDP was received, respectively, as converted by the ISTA from the RSTA’s time basis to its own time basis.

The mechanism by which the ISTA derives t3’ and t2’ from the TOD and TOA fields of the relevant R2I LMR; (see [11.21.6.4.3.4](#H11o21o6o4o3o4) (Reporting phase of TB ranging measurement) are implementation dependent.

When the I2R LMR Feedback is negotiated, the RSTA can compute the RTT as:

RTTRSTA = [(t4’-t1’) – (t3-t2)]

where t1’ and t4’ are the time at which the I2R NDP was transmitted and the time at which the R2I NDP was received, respectively, as converted by the RSTA from the ISTA’s time basis to its own time basis. The mechanism by which the RSTA derives t4’ and t1’ from the TOD and TOA fields of the relevant I2R LMR are implementation dependent; see [11.21.6.4.3.4](#H11o21o6o4o3o4) (Reporting phase of TB ranging measurement).

NOTE—When using CFO in the conversion from the ISTA’s time basis to the RSTA’s, the RSTA uses the CFO reported in the CFO Parameter field of the I2R LMR.

NOTE—Refer to Subclause 27.3.15.3 (Precorrection accuracy requirements for carrier frequency offset (CFO) correction requirement for HE TB PPDU transmission).

In an LMR, the TOA field contains a timestamp that represents the time, with respect to a time base, at which the start of the preamble of the corresponding NDP arrived at the receive antenna connector. The TOD field contains a timestamp that represents the time, with respect to the same time base, at which the start of the preamble of the corresponding NDP appeared at the transmit antenna connector.

If the measurement sounding phase includes more than a single TF Ranging Sounding frame, see Figure [11-37e](#F11o37e) (TB ranging availability window with multiple TF Ranging Sounding frames), each ISTA and RSTA pair shall refer to the t1 and t2 of the I2R NDP transmitted by that ISTA, while t3 and t4 shall be based on the single R2I NDP received by all ISTAs; see Figure [[11-37g](#F11o37g)](#F11o36g) (Measurement Sounding phase with I2R time-division multiplexing). )

If due to retransmission an ISTA receives multiple TF Ranging Sounding frames and transmits multiple I2R NDPs, the ISTA and RSTA shall refer to the t1 and t2 of the I2R NDP last transmitted.



**Figure 11-37g—Measurement sounding phase with I2R time-division multiplexing**

The uplink power control, timing and frequency synchronization requirements of unassociated STAs performing TB ranging shall follow the same rules as those of associated HE STAs.

To aid in synchronizing the TSF time at the ISTAs, the RSTA maintains a trigger poll counter. Before transmitting a TF Ranging Poll, the RSTA shall increase the trigger poll counter by one (modulo 8) and set the Token subfield of the Trigger Dependent Common Info subfield to the value of the trigger poll counter.

When transmitting a Ranging NDP Announcement frame as part of the TB ranging measurement exchange, an RSTA shall include a value in the Partial TSF subfield in the STA Info field with the AID11 subfield equal to 2044, that is equal to the RSTA’s TSF[21:6] at the time of transmission of the preceding TF Ranging Poll. Specifically the time that the first data symbol of the PSDU of said frame was transmitted to the PHY plus the RSTA’s delays through its local PHY from the MAC-PHY interface to its interface with the WM.

Additionally, the RSTA shall set the Token subfield in the STA Info field with the AID11 subfield equal to 2044 to the same trigger poll counter value as the Token subfield in the TF Ranging Poll whose partial TSF time is carried in the Ranging NDP Announcement frame.

NOTE—An ISTA that tries to synchronize to the RSTA’s TSF time will need to keep track of the difference between its local TSF[63:22] and the RSTA’s TSF[63:22] when updating the TSF[21:6]. When receiving a partial TSF value in a received Ranging NDP Announcement frame from the RSTA, to synchronize its TSF time with the RSTA’s TSF time in order to determine the start of a subsequent TB ranging availability window:

* The ISTA should check if its TSF[21:6] at the reception of a TF Ranging Poll was larger than the received Partial TSF and the absolute difference is more than 216-1, then the ISTA should increase the RSTA’s tracked TSF [53:32] value by 1.
* If the ISTA’s TSF [21:6] at the reception of the TF Ranging Poll is less than the Partial TSF and the absolute difference is more than 216-1, the ISTA should decrease the RSTA’s tracked TSF [63:22] value by 1.

**11.21.6.4.3.4 Reporting phase of TB ranging measurement**

The last phase of each polling/sounding/reporting triplet is the measurement reporting phase, which is transmitted a SIFS time after the measurement sounding phase; see Figure [[11-37c](#F11o37c)](#F11o36c) (TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs). The measurement results shall be carried in LMR frames; see [9.6.7.49](#H09o6o7o49) (LMR frame format). LMR frames shall carry measurement results from the RSTA to the ISTA, and if negotiated also from the ISTA to the RSTA; see Figure [11-37h](#F11o37h) (TB ranging measurement reporting phase with Bidirectional LMR Feedback for n ISTAs). If the Range Reporting is performed in the context of a Secure FTM Session, see [11.21.6.3](#H11o21o6o3) (FTM procedure negotiation), the corresponding LMR and FTM; see [11.21.6.5.1](#H11o21o6o5o1) (Availability Window parameter modification); frames shall be transmitted using Protected Fine Timing Action frames, and see [9.6.34](#H09o6o34) (Protected Fine Timing Frame details).

The feedback type of the I2R and R2I LMRs may be either immediate (i.e., from the current availability window) or delayed (i.e., from the last availability window in which the ISTA responded to the TF Ranging Poll frame and the RSTA allocated resources to that ISTA during the measurement sounding phase). The LMR feedback (immediate/delayed) is indicated by the RSTA during the negotiation (see [11.21.6.3.3](#H11o21o6o3o3) Negotiation for TB and Non-TB ranging measurement exchange).

The Dialog Token field in the LMR frame shall be identical to the Sounding Dialog Token field in the corresponding Ranging NDP Announcement frame in the Measurement Sounding phase from which the reported TOA and TOD values were measured; see [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement sounding phase of TB ranging).

NOTE—LMR feedback is carried in Action No-Ack frames and is therefore neither acknowledged nor retransmitted; see [[9.6.7.49](#H09o6o7o49)](#H09o6o7o48) (Location Measurement Report (LMR) frame format).

The RSTA shall transmit an R2I LMR to all ISTAs that were allocated resources in the preceding measurement sounding phase. All the R2I LMR frames shall be carried in one HE MU PPDU or one EHT MU PPDU, where each RU contains only one user. If there is only one R2I LMR it may be carried instead in an HE SU PPDU. If the R2I LMR is transmitted in a bandwidth of 160 MHz or less, the PPDU shall be an HE MU PPDU or an HE SU PPDU.

NOTE--if there is only one R2I LMR, the frame is carried in an HE SU PPDU, HE MU PPDU or EHT MU PPDU (including EHT SU transmission) and this does not include VHT/HT/non-HT PPDUs.

If I2R LMR was negotiated, the RSTA shall assign uplink resources to the ISTAs using a Report Ranging Trigger frame; see [9.3.1.22.10](#H09o3o1o22o10) (Ranging Trigger variant). The Ranging variant Trigger frame of report subvariant is called the TF Ranging LMR.

A TB ranging measurement reporting phase including the optional I2R LMR is illustrated in Figure [11-37h](#F11o37h) (TB ranging measurement reporting phase with Bidirectional LMR Feedback for n ISTAs). If the I2R LMR was negotiated by one or more ISTAs, then SIFS time after transmitting out the R2I LMR, the RSTA transmits a TF Ranging LMR to solicit the I2R LMR frame(s). This TF shall allocate uplink resources to ISTAs that negotiated I2R LMR and were allocated resources in the preceding measurement sounding phase. The RSTA shall allocate each RU in the TF Ranging LMR to only one ISTA. In response to the TF Ranging LMR, each addressed ISTA shall respond by transmitting an I2R LMR frame.

If an ISTA negotiated delayed I2R LMR reporting, and if the TOA measurement for the previous availability window is not ready, then the ISTA shall not respond to the TF Ranging Poll frame in the Polling phase of any availability window until the I2R LMR is ready.

For delayed reporting, the first instance of the R2I LMR and the optional I2R LMR do not have valid TOA/TOD timestamps to include, in this case the RSTA and the ISTA shall set the Invalid Measurement subfield in the TOA Error field of the respective LMR to 1.



**Figure 11-37h—TB ranging measurement reporting phase with bidirectional LMR feedback for n ISTAs**

In TB ranging, the PHY shall issue the PHY-RXEND.indication primitive with error condition IntegrityCheckError, if the PHY detects the integrity check error in the reception of the corresponding HE Ranging NDP or HE TB Ranging NDP. If the PHY of an RSTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the RSTA shall set the Invalid Measurement field in the R2I LMR frame carrying the TOA measured from the I2R NDP to 1. Correspondingly, if I2R LMR was negotiated between the ISTA and RSTA and the PHY of the ISTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the ISTA shall set the Invalid Measurement field in the I2R LMR carrying the TOA measured from the R2I NDP to 1.

NOTE—When a STA detects that the transmit center frequency offset (CFO) between the ISTA and the RSTA exceeds the allowed tolerance from the values specified in 27.3.19.3 and 27.3.15.3, this can be an indication of a security attack.

If I2R LMR reporting was negotiated, then the ISTA shall include a CFO parameter in the I2R LMR; see [[9.6.7.49](#H09o6o7o49)](#H09o6o7o48) (Location Measurement Report (LMR) frame format). The ISTA shall estimate the CFO parameter based on the PPDU carrying the TF Ranging Sounding frame that solicits the I2R NDP from the ISTA. The RSTA may account for clock rate differences between ISTA and RSTA based on the CFO parameter included in the received I2R LMR. The mechanism by which t4 and t1 are adjusted by the RSTA is implementation specific. The CFO parameter refers to the t1 and t4 indicated in the same I2R LMR.

If the Invalid Measurement field in an R2I LMR or I2R LMR is equal to 1, the RSTA or ISTA receiving the LMR should discard the TOA carried in the LMR.

In TB ranging measurement reporting phase, if R2I LMR reporting or I2R LMR reporting carries phase shift feedback, then the R2I LMR reporting or the I2R LMR reporting shall be immediate feedback.

In TB ranging measurement reporting phase, if R2I AOA feedback was negotiated the RSTA shall include the optional AOA feedback subfield in the R2I LMR frame and if I2R LMR reporting was negotiated in addition to I2R AOA Feedback reporting then the ISTA shall include the optional AOA feedback subfield in the I2R LMR frame. The AOA field contains the Direction Measurement Results element described in 9.4.2.300.

**11.21.6.4.4 Non-TB ranging measurement exchange**

**11.21.6.4.4.1 General**

In Non-TB ranging, the protocol operates in an ISTA centric scheduling FTM mode; whenever the medium is available, an ISTA may initiate the measurement. The RSTA can only limit the frequency with which the ISTA can initiate measurements, by setting a minimum time interval between subsequent range measurements.



**Figure 11-37i—Non-TB ranging measurement exchange sequence**

**11.21.6.4.4.2 Measurement sounding phase of non-TB ranging**

An ISTA shall initiate a non-TB ranging measurement instance by transmitting a Ranging NDP Announcement frame addressed to the RSTA, followed by an I2R NDP SIFS after. In response to the correctly received Ranging NDP Announcement frame addressed to itself, the RSTA shall transmit an R2I NDP; see Figure [11-37i](#F11o37i) (Non-TB ranging measurement exchange sequence). I2R NDP and R2I NDP, are HE Ranging NDPs or EHT Ranging NDPs. The measurement-reporting phase consists of an LMR frame, which is a Location Measurement Report as defined in [[9.6.7.49](#H09o6o7o49)](#H09o6o7o48) (Location Measurement Report (LMR) frame format).

For immediate feedback the LMR carries measurement results of the current measurement exchange, while for delayed feedback the LMR carries measurement results of the previous measurement exchange; see [11.21.6.4.4.3](#H11o21o6o4o4o3) (Non-TB ranging measurement reporting phase).

An ISTA shall set the Min Time Between Measurements field and the Max Time Between Measurements field in the Non-TB Specific subelement in the Ranging Parameters element in the IFTMR frame, where Max Time Between Measurements shall be larger than Min Time Between Measurements and takes into account the measurement exchange duration. An RSTA shall assign the value of the Min Time Between Measurements and Max Time Between Measurements in the Non-TB Specific subelement in the Ranging Parameters element in the initial FTM frame, where Max Time Between Measurements shall be larger than Min Time Between Measurements and takes into account of the measurement exchange duration.

An ISTA shall not initiate a new measurement exchange sequence until the assigned minimum time interval between subsequent range measurements has elapsed; see Figure [11-37k](#F11o37k) (Non-TB ranging with immediate reporting). An ISTA should complete the measurement sequence before the assigned maximum time interval between subsequent range measurements has elapsed.

An ISTA may use any AC to transmit the Ranging NDP Announcement frame.

The ISTA maintains a sounding dialog token counter modulo 64 for each FTM session. When transmitting a Ranging NDP announcement frame to an RSTA, the Sounding Dialog Token Number subfield in the Sounding Dialog field shall be set to the value of the corresponding counter; after which the counter shall be incremented by 1.

After transmitting the Ranging NDP Announcement frame and I2R NDP, the ISTA shall wait for a time interval of aSIFSTime + aSlotTime + aRxPHYStartDelay. This interval begins when the MAC receives a PHY-TXEND.confirm primitive for I2R NDP. If a PHY-RXSTART.indication primitive does not occur during the time interval, the ISTA shall conclude that the transmission of the Ranging NDP Announcement frame + I2R NDP has failed and abort the current measurement exchange. If a PHY-RXSTART.indication primitive occurred during the time interval, the ISTA tries to receive the R2I NDP and the LMR frame from the RSTA addressed by the Ranging NDP Announcement frame. If the LMR is received from the RSTA, the frame exchange initiated by the Ranging NDP Announcement frame is complete, otherwise the ISTA shall conclude that the current measurement exchange has failed.

The ISTA may invoke the backoff procedure by an EDCAF when the last frame of the measurement exchange initiated by the Ranging NDP Announcement frame has completed, the TXNAV timer has expired.

In the Non-TB ranging measurement exchange sequence, the ISTA shall transmit the Ranging NDP Announcement frame with the same bandwidth as the I2R NDP to reserve the medium. The Ranging NDP Announcement frame shall be unicast with the RA field set to the address of the RSTA, and contain one STA Info field with the AID11 subfield set to 0. If negotiated, the NPD Announcement frame shall contain another STA Info field with AID11 subfield set to 2045, and the I2R Tx Power subfield shall be set to indicate the TX power of the following I2R NDP. If the STA Info field with AID11 subfield set to 2045 is included, the ISTA shall set the R2I NDP Target RSSI subfield to either its preferred receive signal power or a reserved value.

The RSTA shall transmit the R2I NDP with the same bandwidth as the Ranging NDP Announcement frame, while the LMR may be transmitted at a different bandwidth, according to the rules of multiple frame transmission in an EDCA TXOP, see 10.23.2.8 (Multiple frame transmission in an EDCA TXOP). The allowed bandwidths for the Ranging NDP Announcements, I2R NDP and R2I NDP, shall be less than or equal the RSTA Assigned Max Bandwidth.

Accordingly:

* An ISTA transmitting an I2R NDP shall set the TXVECTOR parameter CH\_BANDWIDTH to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame.
* If the CH\_BANDWIDTH of the I2R NDP is equal to 320 MHz, the I2R NDP shall be an EHT Ranging NDP, otherwise it shall be an HE Ranging NDP.
* An RSTA transmitting a R2I NDP shall set the TXVECTOR parameter CH\_BANDWIDTH to the bandwidth of the Ranging NDP Announcement frame and/or the I2R NDP; which are obtained from the RXVECTOR parameter CH\_BANDWIDTH of the Ranging NDP Announcement frame or I2R NDP respectively. For the Ranging NDP Announcement frame, when not received in an EHT/HE/VHT/HT PPDU: from the RXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT when the Ranging NDP Announcement frame is received in a non-HT duplicate PPDU and is 20 MHz when the Ranging NDP Announcement frame is received in a non-HT PPDU.

If the CH\_BANDWIDTH of the R2I NDP is equal to 320 MHz, the R2I NDP shall be an EHT Ranging NDP and the LMR(s) in the corresponding measurement exchange sequence shall be transmitted in an EHT SU transmission. Otherwise, the R2I NDP shall be an HE Ranging NDP and the LMR(s) shall be transmitted in an HE SU PPDU. If the bandwidth is less than or equal to 80 MHz, the ISTA shall set the I2R NSTS subfield and the R2I NSTS subfield in the STA Info field of the Ranging NDP Announcement frame each to a value not to exceed the *RSTA assigned I2R* *STS ≤ 80 MHz* and *RSTA assigned R2I* *STS ≤ 80 MHz* respectively. If the bandwidth is greater than 80 MHz, the ISTA shall set these same subfields to values not to exceed the *RSTA assigned I2R* *STS > 80 MHz* and *RSTA assigned R2I* *STS > 80 MHz* respectively.

The ISTA shall set the I2R Rep subfield and R2I Rep subfield in the STA Info field of the Ranging NDP Announcement frame each to a value not to exceed the *RSTA assigned I2R rep* and *RSTA assigned R2I rep* respectively. Furthermore, the total number of LTF in the I2R NDP and R2I NDP, based on the number of spatial streams and repetitions, shall not exceed the *RSTA assigned I2R LTF Total* and *RSTA assigned R2I LTF Total* respectively.

After transmission of the Ranging NDP Announcement frame, the ISTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 0, and
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the R2I NSTS and R2I Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007.

After reception of the Ranging NDP Announcement frame, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 0, and
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the I2R NSTS and I2R Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007.

Both RSTA and ISTA perform RTT measurements by capturing the timestamps of the NDP. The ISTA shall record the time at which the I2R NDP is transmitted (t1). The RSTA shall then capture the time at which the I2R NDP arrives (t2) and shall record the time at which the R2I NDP is transmitted (t3). The ISTA shall finally capture the time at which the R2I NDP arrives (t4); see Figure [11-37j](#F11o37j) (Timing diagram of a Measurement Sounding phase in non-TB ranging). The timestamp values t2 and t3 shall be measured according to the RSTA’s clock (i.e., without applying any frequency offset correction to the time basis).



**Figure 11-37j—Timing diagram of a measurement sounding phase in non-TB ranging**

The Round Trip Time (RTTISTA) based on first path reporting is defined as:

RTTISTA = [(t4 – t1) – (t3’ – t2’)]

where t3’ and t2’ are the time at which the R2I NDP was transmitted and the time at which the I2R NDP was received, respectively, as converted by the ISTA from the RSTA’s time basis to its own time basis.

The mechanism by which the ISTA derives t3’ and t2’ from the TOD and TOA fields of the relevant LMR are implementation dependent.

The Round Trip Time (RTTRSTA) based on first path reporting is defined as:

RTTRSTA = [(t4’– t1’) – (t3 – t2)]

where t1’ and t4’ are the time at which the I2R NDP was transmitted and the time at which the R2I NDP was received, respectively, as converted by the RSTA from the ISTA’s time basis to its own time basis.

The mechanism by which the RSTA derives t1’ and t4’ from the TOD and TOA fields of the relevant LMR are implementation dependent.

In an LMR, the TOA field contains a timestamp that represents the time, with respect to a time base, at which the start of the preamble of the corresponding NDP arrived at the receive antenna connector. The TOD field contains a timestamp that represents the time, with respect to the same time base, at which the start of the preamble of the corresponding NDP appeared at the transmit antenna connector.

**11.21.6.4.4.3 Non-TB ranging measurement reporting phase**

In non-TB ranging, the ranging protocol supports both immediate and delayed reporting.

An RSTA or ISTA indicates immediate reporting by setting the immediate R2I Or I2R Feedback subfield in the Ranging Parameters field of the FTM session frames that enable the measurement exchange, to 1. In immediate reporting, the TOA feedback corresponding to the current measurement exchange sequence shall be reported in the current measurement exchange; see Figure [[11-37k](#F11o37k)](#F11o36j) (Non-TB ranging with immediate reporting).



**Figure 11-37k—Non-TB ranging with immediate reporting**

An RSTA or ISTA indicates delayed reporting by setting the Immediate R2I Or I2R Feedback subfield in the Ranging Parameters field to 0. In delayed reporting, the TOA and TOD values in the current LMR shall carry the measurement results of the previous round. In this case, the first instance of the R2I LMR and the optional I2R LMR do not have valid TOA/TOD timestamps to include, and the RSTA and the ISTA shall set the Invalid Measurement subfield in the TOA Error field of the corresponding LMR to 1; see Figure [11-37l](#F11o37l) (Non-TB ranging with delayed reporting).



**Figure 11-37l—Non-TB ranging with delayed reporting**

An RSTA that indicated delayed reporting shall provide TOA feedback to the ISTA when the ISTA initiates another measurement sequence after Min Time Between Measurements, but before Max Time Between Measurements; see Figure [11-37m](#F11o37m) (Illustration of Min Time Between Measurements and Max Time Between Measurements with delayed reporting). This TOA feedback is carried in the LMR frame of this new measurement sequence and can be either valid or invalid as indicated by the invalid Measurement field in the LMR frame.

TheDialog Token field of the LMR frame shall be copied from the Sounding Dialog Token Number subfield in the Ranging NDP Announcement frame that preceded the NDP which is used for the reported measurement.

If negotiated, the RSTA shall set the R2I TX Power field in the R2I LMR to report the TX power of the preceding R2I NDP; otherwise the R2I Tx Power field shall be set to a reserved value. The RSTA shall set the I2R NDP Target RSSI field to its preferred receive signal power or a reserved value.



**Figure 11-37m—Illustration of min time between measurements and max time between measurements with delayed reporting**

If I2R LMR feedback is negotiated, the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) sequence shall follow the sequence shown in Figure [11-37n](#F11o37n) (Non-TB ranging measurement exchange sequence with bidirectional LMR feedback). After SIFS time of receiving the R2I LMR frame, the ISTA shall transmit the I2R LMR frame to the RSTA. The feedback type of I2R LMR could be either immediate or delayed.

NOTE—LMR feedback is carried in an Action No-Ack frame and is therefore neither acknowledged nor retransmitted; see [[9.6.7.49](#H09o6o7o49)](#H09o6o7o48) (Location Measurement Report (LMR) frame format).



**Figure 11-37n—Non-TB ranging measurement exchange sequence with bidirectional LMR feedback**

The data rate or MCS used for transmitting the R2I and I2R LMR frames is solely decided by the transmitter of each of the frames. The bandwidth used to transmit the R2I LMR frame shall be no greater than that of the soliciting NDP Announcement frame, and the transmit bandwidth of the I2R LMR frame shall be no greater than the bandwidth of the preceding R2I LMR frame.

In non-TB ranging, the PHY shall issue the PHY-RXEND.indication primitive with error condition IntegrityCheckError, if the PHY detects the integrity check error in the reception of the corresponding HE/EHT Ranging NDP. If the PHY of an RSTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the RSTA shall set the Invalid Measurement field in the R2I LMR frame carrying the TOA measured from the I2R NDP to 1. Similarly, if I2R LMR was negotiated between the ISTA and RSTA and the PHY of an ISTA issues a PHY-RXEND. Indication primitive with error condition IntegrityCheckError, the ISTA shall set the Invalid Measurement field in the I2R LMR carrying the TOA measured from the R2I NDP to 1.

NOTE—When a STA detects that the transmit center frequency offset (CFO) between the ISTA and the RSTA exceeds the allowed tolerance from the values specified in 27.3.19.3 and 27.3.15.3, this can be an indication of a security attack.

In the non-TB ranging, both RSTA and ISTA should measure the CFO value based on reception of I2R NDP and R2I NDP respectively. Therefore, the CFO parameter field in the I2R LMR, if negotiated, and R2I LMR are reserved. The RSTA and ISTA may account for clock rate differences between ISTA and RSTA respectively based on their own measured CFO value. The mechanism by which t4 and t1 are adjusted by the RSTA, and t2 and t3 are adjusted by the ISTA is implementation specific.

If the Invalid Measurement field in R2I LMR or I2R LMR is equal to 1, the RSTA or ISTA receiving the LMR should discard the TOA carried in the LMR.

In non-TB ranging measurement reporting phase, if R2I LMR reporting or I2R LMR reporting carries phase shift feedback, then the R2I LMR reporting or the I2R LMR reporting shall be immediate feedback.

In non-TB ranging measurement reporting phase, if R2I AOA feedback was negotiated the RSTA shall include the optional AOA feedback subfield in the R2I LMR frame and if R2I LMR reporting was negotiated in addition to I2R AOA Feedback reporting then the ISTA shall include the optional AOA feedback subfield (see 9.4.2.300, Direction Measurement Results element) in the I2R LMR frame. The AOA field contains the Direction Measurement Results element described in 9.4.2.300.

**11.21.6.4.5 Secure LTF in the TB and non-TB ranging measurement exchange protocol**

***Discussion****:*

*The HE-LTF Counter subfield in the Secure HE-LTF Parameters element looks reusable for EHT ranging NDP. Need group’s inputs on next step:*

1. *Rename them to “LTF Counter subfield” and “Secure LTF Parameters element” with a global replacement (assumed in this PDT, as “Secure LTF” has already been used in multiple figures in the baseline text) - - the group was supportive in this direction during the Apr 4th call, so we made change for this subclause in this direction*
2. *Keep the name as is*

*On secure EHT -LTF:*

1. *Expand the current subclauses - - the group was supportive in this direction during the Apr 4th call, so we made change for this subclause in this direction*
2. *Create separate subclauses*

***TGbk editor: please replace Secure HE-LTF Parameters element with Secure LTF Parameters element and HE-LTF Counter subfield with LTF Counter subfield throughout the spec, including Figure 9-788eu—Secure HE-LTF Parameters element format.***

**11.21.6.4.5.1 General**

Both the TB and the non-TB ranging measurement exchanges allow for the use of secure LTF for PHY security, if the ISTA and RSTA have established a secure LTF measurement setup as defined in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB measurement exchange). The frame exchange sequences stay nominally the same as described in [11.21.6.4.3](#H11o21o6o4o3) (TB ranging measurement exchange) and [11.21.6.4.4](#H11o21o6o4o4) (Non-TB ranging measurement exchange), except that the HE Ranging NDP , HE TB Ranging NDP, EHT Ranging NDP and EHT TB Ranging NDP will use secure LTF as described in  [[27.3.18a.1](#H27o3o18ao1)](#H27o3o18a) (HE Ranging NDP), [[27.3.18a.2](#H27o3o18ao2)](#H27o3o18b) (HE TB Ranging NDP), TBD (EHT Ranging NDP) and TBD (EHT TB Ranging NDP) respectively. To use the secure LTF the ISTA and RSTA need to share and communicate pseudorandom bit sequences that are used to generate and demodulate the secure LTF, the details and management thereof is described in the following.

**11.21.6.4.5.2 TB ranging measurement exchange with secure LTF**



**Figure 11-37o—Overview of the TB ranging measurement exchange with secure LTF**

An example of the negotiation and two TB Ranging Measurement Exchanges with secure LTF is shown in Figure [11-37o](#F11o37o) (Overview of TB ranging measurement exchange with secure LTF), where the LTF\_VALID\_SAC and SEC\_LTF\_CTR refer to the value of the values of the Validation SAC and Secure LTF Counter subfields. The first value of the Validation SAC and its associated Secure LTF Counter subfields shall be included in a protected IFTM frame, and thereafter any subsequent value of the Validation SAC and its corresponding Secure LTF Counter subfield shall be included in a protected R2I LMR frame. The value of the Validation SAC subfield shall also be the same value of the SAC subfield in the Trigger Dependent User Info field of the Secure Sounding Ranging Trigger frame. The description of how these fields are set in the TB ranging measurement exchange is given next.

In a TB ranging measurement exchange with secure LTF where there are multiple ISTAs involved in the measurement sequence, the RSTA shall transmit a Secure Sounding Ranging Trigger frame which includes a single User Info field to trigger a single ISTA at a time.

When an RSTA has established a secure LTF measurement exchange with an ISTA as specified in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB measurement exchange), the RSTA that sends a Secure Sounding Ranging Trigger frame to the STA shall set:

* The SAC subfield in the Trigger Dependent User Info field corresponding to the ISTA in the Secure Sounding Ranging Trigger frame to the same value as in the Validation SAC field in the Secure LTF Parameters element in the last transmitted protected IFTM, or last transmitted protected LMR frame, to the ISTA;

The RSTA shall set the I2R Rep subfield of the User Info field corresponding to the ISTA in the Secure Sounding Ranging Trigger frame equal to the value of the *RSTA Assigned I2R Rep* corresponding to the ISTA, where the value of the *RSTA Assigned I2R Rep* shall be greater than 0.

After transmission of the Secure Sounding Ranging Trigger frame to the ISTA, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values, respectively, as indicated by the SS Allocation and I2R Rep subfields of the User Info field;
* the LTF\_KEY and LTF\_IV parameters that are set to *ista-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NDP; it is set to 0 otherwise,
* the LTF\_OFFSET set to 0.

When the RSTA receives the HE/EHT TB Ranging NDP from the ISTA, the RSTA shall:

1. Send a Ranging NDP Announcement frame.
2. Send an HE/EHT Ranging NDP with the TXVECTOR parameter LTF\_KEY and LTF\_IV set to the *rsta-ltf-key* and *ltf-iv* for generating secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation).
3. Send a protected LMR frame that includes the Secure LTF Parameters element to the ISTA.

Otherwise, the RSTA shall follow the rules in 10.22.2.2 (EDCA backoff procedure) as the frame exchange is not successful.

When an RSTA sends a Ranging NDP Announcement frame, it shall set the LTF Offset subfield in the STA Info fields to values that satisfy Equations [(11-6a)](#E11o6a) and [(11-6b):](#E11o6b)

(11-6a)

(11-6b)

where,

* Offset*n* represents the LTF Offset subfield value of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *N\_STSn* represents the R2I NSTS subfield value plus 1 of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *N\_LTFn* represents the number of LTF symbols based on *N\_STSn*, see Table 21-13 (Number of VHT-LTFs required for different numbers of space-time streams), for the *nth* STA Info field in the Ranging NDP Announcement frame.
* *Repn* represents the R2I Rep subfield value plus 1 of the *nth* STA Info field in the Ranging NDP Announcement frame.
* *MinOffset* represents the set of indexes of the STA Info fields of which the LTF Offset subfield values are less than the LTF Offset subfield value of *ith* STA Info field in the Ranging NDP Announcement frame.
* *MaxOffset* represents the set of indexes of all STA Info fields excluding *ith* STA Info field.

The RSTA shall set the R2I Rep subfield in each of the STA Info field in the Ranging NDP Announcement frame equal to the *RSTA Assigned R2I Rep* for each of the corresponding ISTAs, where all of the *RSTA Assigned R2I Rep* shall be greater than 0.

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame, received from the RSTA, the ISTA shall  
send an HE/EHT TB Ranging NDP with the TXVECTOR parameters LTF\_KEY and LTF\_IV that are set to *ista-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame, received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame received from the RSTA, the ISTA shall send an HE/EHT TB Ranging NDP with the TXVECTOR parameters LTF\_KEY and LTF\_IV that are set to the *ista-ltf-key* and *ltf-iv* for generating any secure HE/EHT-LTF ;

When an ISTA receives a Ranging NDP Announcement frame from an RSTA in which the AID11 subfield in the STA Info field contains the 11 least significant bits of the AID or RSID of the ISTA, the ISTA shall issue a PHY-RXLTFSEQUENCE.request primitive with the following LTFVECTOR parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS, LTF\_REP, and LTF\_OFFSET parameters set to the same values, respectively, as indicated by the R2I NSTS, R2I Rep and LTF Offset subfields of the STA Info field addressed to it;
* the LTF\_KEY and LTF\_IV parameters that are set to the *rsta-ltf-key* and *ltf-iv* for generating the secure HE/EHT-LTFbased on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (General secure LTF octet stream generation), and;
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for R2I NDP; it is set to 0 otherwise.

When an LMR frame contains range measurement results measured from an I2R NDP or an R2I NDP, an RSTA that transmits an R2I LMR frame, or when negotiated, an ISTA that transmits an I2R LMR frame, shall include the Secure LTF Parameters element in the protected LMR frame:

* The Measurement SAC subfield in the Secure LTF Parameters element in the protected LMR frame shall be set to the same value as in the SAC subfield in the Trigger Dependent User Info field in the Secure Sounding Ranging Trigger destined to the ISTA receiving or transmitting this protected LMR frame.
* The Measurement Result LTF Offset subfield in the Secure LTF Parameters element in the protected LMR frame shall be set to the same value as in the LTF Offset subfield of the STA Info field in the Ranging NDP Announcement frame that preceded the R2I NDP destined to the ISTA for this measurement result.

When an ISTA or RSTA receives the R2I or I2R protected LMR frame, the ISTA or RSTA shall compare the value of the Measurement Result LTF Offset subfield with the value of the LTF Offset subfield in the corresponding STA Info field of the Ranging NDP Announcement frame, and if these two values don’t match, the ISTA or RSTA shall discard the measurement results carried in the protected LMR frame.

When a frame exchange that consists of receiving an HE/EHT TB Ranging NDP and transmitting HE/EHT Ranging NDP results into a Null-SAC-LTF, the RSTA shall not use the TOA and TOD value of the HE/EHT TB Ranging NDP and HE/EHT Ranging NDP respectively and shall set the Invalid Measurement Indication subfield to 1 in the TOA error field in the protected LMR carrying the TOA value of the I2R HE/EHT TB Ranging NDP.

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame received from the RSTA, the ISTA shall:

* not use the TOD value of the I2R HE/EHT TB Ranging NDP
* not use the TOA value of the R2I HE/EHT Ranging NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR carrying the TOA value of the HE/EHT Ranging NDP if the I2R LMR transmission from the ISTA was negotiated.

The STA shall discard the SAC value used in the frame exchange and shall not use the same SAC value in the current measurement exchange.

NOTE—In TB ranging measurement exchange with secure LTF, the RSTA never sends the SAC subfield with value 0 in the Trigger Dependent User Info field in the Secure Sounding Ranging Trigger frame.

When there is a transmission failure within a secure measurement exchange sequence, the recovery procedure of the LTF\_VALID\_SAC and its associated SEC\_LTF\_CTR parameters is illustrated in Figure [11-37p](#F11o37p) (Error recovery of TB ranging measurement exchange using secure LTF).



***TGbk editor: Please delete the 2 occurances of “HE” in the figure above***

**Figure 11-37p—Error recovery of TB ranging measurement exchange using secure LTF**

**11.21.6.4.5.3 Non-TB ranging measurement exchange with secure LTF**



**Figure 11-37q—Overview of the non-TB ranging measurement exchange with secure LTF**

An overview of the negotiation and two non-TB ranging measuerment exchanges are illustrated in Figure [11-37q](#F11o37q) (Overview of non-TB ranging measurement exchange with secure LTF). The LTF\_VALID\_SAC and its associated SEC\_LTF\_CTR parameter shall be included in a protected IFTM frame and a protected R2I LMR frame. The LTF\_VALID\_SAC shall also be included in the SAC subfield in the Ranging NDP Announcement frame. The detailed description of how the fields in these frames are set follows.

When an ISTA has established a secure LTF measurement exchange with an RSTA as specified in [11.21.6.3.4](#H11o21o6o3o4) (Negotiation for secure LTF in the TB and non-TB ranging measurement exchange), this ISTA shall set the following subfields in any Ranging NDP Announcement frame addressed to that RSTA as follows:

* The SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is set to the same value contained in the Validation SAC subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected R2I LMR frame, received from the RSTA;
* Otherwise the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is set to a value of 0 to indicate that a new SEC\_LTF\_CTR and the corresponding LTF\_VALID\_SAC parameter are needed.

The ISTA shall set the I2R Rep subfield and R2I Rep subfield of the STA Info field in the Ranging NDP Announcement frame to the values of *RSTA Assigned I2R Rep* and the *RSTA Assigned R2I Rep* respectively, corresponding to the RSTA. Both values of the *RSTA Assigned R2I Rep,* and *RSTA Assigned I2R Rep,* shall begreater than 0.

An ISTA that sends an I2R NDP a SIFS after transmission of the Ranging NDP Announcement frame shall set the TXVECTOR parameters LTF\_KEY and LTF\_IV as follows:

* Either to the value of Null-SAC-LTF, if the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame, is equal to 0 ;
* Or the *ista-ltf-key* and *ltf-iv* for generating secure HE/EHT-LTF based on the value of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame or last protected LMR frame, received from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation).

After transmission of the Ranging NDP Announcement frame to the RSTA, the ISTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR containing the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the R2I NSTS and R2I Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007;
* the LTF\_KEY and LTF\_IV parameters that are set to either to the value of Null-SAC-LTF, if the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame is equal to 0; Or the *rsta-ltf-key* and *ltf-iv* for generating a secure HE/EHT-LTF based on the values of the Secure LTF Counter subfield in the Secure LTF Parameters element in the last protected IFTM frame, or last protected LMR frame received, from the RSTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for R2I NDP; it is set to 0 otherwise, and
* the LTF\_OFFSET set to 0.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the SAC subfield in the STA Info field with AID11 equal to 2043 is not equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall:

* Send an HE/EHT Ranging NDP to the ISTA with the TXVECTOR parameters r*sta-ltf-key* and *ltf-iv* for generating any secure LTF to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame;
* Send a protected LMR frame with a Secure LTF Parameters element containing the SEC\_LTF\_CTR and the corresponding LTF\_VALID\_SAC parameters to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the value of the SAC subfield in the STA Info field with AID11 equal to 2043 is equal to the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall:

* Send an HE/EHT Ranging NDP with the TXVECTOR parameters *rsta-ltf-key* and *ltf-iv* for generating a secure HE/EHT-LTF based on the values of the Secure LTF Counter in the Secure LTF Parameters element in the last transmitted protected IFTM frame, or last transmitted protected LMR frame to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (Overview of secure LTF octet stream generation);
* Send a protected LMR frame that includes the Secure LTF Parameters element to the ISTA, only if the RSTA receives an HE/EHT Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA, the RSTA shall also issue a PHY-RXLTFSEQUENCE.request primitive with an LTFVECTOR with the following parameters:

* the SECURE\_LTF\_FLAG parameter set to 1;
* the LTF\_NSTS and LTF\_REP parameters set to the same values as indicated, respectively, by the I2R NSTS and I2R Rep subfields in the STA Info field with the AID11 subfield less than or equal to 2007;
* the LTF\_KEY and LTF\_IV parameters that are set to the i*sta-ltf-key* and *ltf-iv* for receiving a secure HE/EHT-LTF based on the values of the Secure LTF Counter and corresponding Validation SAC subfields in the Secure LTF Parameters element in the last transmitted protected IFTM frame, or last transmitted protected LMR frame to the ISTA; see [11.21.6.4.5.4](#H11o21o6o4o5o4) (General secure LTF octet stream generation);
* the TX\_WINDOW\_FLAG set to 1 if the ISTA and RSTA have negotiated to use the optional frequency domain Tx window for I2R NDP; it is set to 0 otherwise, and;
* the LTF\_OFFSET set to 0.

An RSTA transmitting an R2I LMR frame, or an ISTA when negotiated to transmit LMR frame, containing range measurement results measured from an I2R NDP and a R2I NDP, shall include the Secure LTF Parameters element in the protected LMR frame and set the Measurement SAC subfield in the Secure LTF Parameters element in the protected LMR frame to the same value as in the SAC subfield in the STA Info field with AID11 equal to 2043 in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP.

When a STA sends a Null-SAC-LTF in an HE/EHT Ranging NDP**,** the STA shall not use the TOD value of the HE/EHT Ranging NDP for the secure range measurement exchange.

When a STA receives a Null-SAC-LTF in an HE/EHT Ranging NDP, the STA shall not use the TOA value of the HE/EHT Ranging NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR carrying the TOA value of the HE/EHT Ranging NDP.

When there is a transmission failure within a secure measurement exchange, the recovery procedure of the LTF\_VALID\_SAC is illustrated in Figure [11-37r](#F11o37r) (Error recovery of non-TB ranging measurement exchange using secure LTF).

A STA shall discard the LTF\_VALID\_SAC parameter used in the frame exchange and shall not use the same LTF\_VALID\_SAC parameter in the current measurement exchange.



***TGbk editor: Please delete the 2 occurances of “HE” in the figure above***

**Figure 11-37r—Error recovery non-TB ranging measurement exchange using secure LTF**

11.21.6.4.5.4 Overview of secure LTF octet stream generation

This clause describes mechanisms for generating the SAC, LTF protection keys, counters, and the pseudorandom octet stream used to randomize the input to the modulation and per stream phase rotation for constructing secure LTFs. The mechanism is illustrated in Figure [11-37s](#F11o37s) (ISTA secure LTF octet stream generation, and Figure [11-37t](#F11o37t) (RSTA secure LTF octet stream generation).

For each secure measurement (e.g. NDP exchanges), a SAC and two secret keys *ista-ltf-key* and *rsta-ltf-key* shall be derived by the ISTA and the RSTA independently as follows.

SAC-and-LTF-Keys = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure HE-LTF Expansion”, Secure-LTF-Counter)

Where

* KDF and Hash are the key derivation function and hash function determined by the AKM used to derive the PTKSA from which the Secure-LTF-Key-Seed was derived.
* Length is equal to 272 (bits)
* SAC = L(SAC-and-LTF-Keys, 0, 16)
* *ista-ltf-key* = L(SAC-and-LTF-Keys, 16, 128)
* *rsta-ltf-key* = L(SAC-and-LTF-Keys, 144, 128)

The *ista-ltf-key* shall be used to generate the pseudorandom octet stream to protect all of the LTFs in PPDUs transmitted by the ISTA. The *rsta-ltf-key* shall be used to generate the pseudorandom octet stream to protect all of the LTFs in PPDUs transmitted by the RSTA. The ISTA and RSTA shall use the same derivation and derive identical keys.

With the SAC constructed as above, an attacker not knowing the Secure-LTF-Key-Seed would not be able to predict the SAC that would be used for a given measurement.

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the value of the Secure LTF Counter subfield in the KDF as well as in the transmitted LTF sequence information. The counter shall be padded with leading (MSB) 0s to be exactly 6 octets.

The 16-octet IV input *ltf-iv* to the secure LTF bit generator shall be constructed as follows:

* First 6 octets shall be the transmitter MAC address (A2).
* Next 6 octets shall encode the value of the Secure LTF Counter subfield with the encoding convention described above.
* Final 4 octets shall be used as a 32-bit block counter. The block counter shall be initialized to 0 before the NDP with secure LTFs is transmitted or received. The counter shall be incremented by 1 each time an AES block is output by the generator.

Each time pseudorandom bits are required to protect the LTFs in an NDP, the secure LTF bit generator generates the required number of AES blocks using the AES algorithm (see FIPS PUB 197) with the corresponding 128-bit key and 128-bit IV inputs. The output of the AES-128 counter encryption is a 128-bit integer. It shall be converted using the conventions specified in 12.4.7.2.2 (Integer to octet string conversion) to obtain the octet stream used for secure LTF generation.

NOTE— A 6 octet parameter representing the value of the Secure LTF Counter subfield is sufficient because a unicast protected management frame that uses a 6 octet PN is used to convey the LTF sequence information that carries the counter.

NOTE—The pseudorandom bit generator is based on AES-128 Counter mode approved by NIST (CTR-DRBG - NIST SP 800 90Ar1 - Recommendations for Random Number Generation).

The number of pseudorandom bits that can be generated without violating security guarantees of the scheme is 2^39 without updating the key or reseeding the generator with additional entropy.

Secure LTF measurement requires a variable number of octets from the pseud random octet stream depending on the TXVECTOR or RXVECTOR parameters for the LTFs as described in section [27.3.18b.2](#H27o3o18bo2) (Generation of a randomized secure LTF sequence). The initial block counter value used to construct the *ltf-iv* for setting the TXVECTOR and RXVECTOR parameters shall be 0.

**11.21.6.4.5.5 Secure LTF octet stream generation on an ISTA**

Figure [11-37s](#F11o37s) (ISTA secure LTF octet stream generation) illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an ISTA.

Diagram

Description automatically generated

***TGbk editor: Please replace “*Secure LTF Expansion*” with “*Secure HE-LTF Expansion*” in the figure above***

**Figure 11-37s—ISTA secure LTF octet stream generation**

For each secure measurement on an ISTA, the following parameters shall be used for generating the pseudorandom octet stream used to construct the LTFs for NDPs:

* the *ista-ltf-key* and *rsta-ltf-key* for transmitted NDP (TXVECTOR parameter LTF\_KEY) and received NDP (RXVECTOR parameter LTF\_KEY) respectively.
* the *ltf\_iv* for transmitted NDP (TXVECTOR parameter LTF-IV) and received NDP (RXVECTOR parameter LTF-IV) with corresponding ISTA MAC address and RSTA MAC address respectively together with the value of the Secure LTF Counter subfield and the block counter

**11.21.6.4.5.6 Secure LTF input octet stream generation on an RSTA**

The following Figure [11-37t](#F11o37t) (RSTA secure LTF octet stream generation) illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an RSTA.

Diagram

Description automatically generated

***TGbk editor: Please replace “*Secure LTF Expansion*” with “*Secure HE-LTF Expansion*” in the figure above***

**Figure 11-37t—RSTA secure LTF octet stream generation**

For each secure measurement on an RSTA, the following parameters are provided for generating the pseudorandom octet stream to construct the LTFs for NDPs:

* the *ista-ltf-key* and *rsta-ltf-key* for received NDP (RXVECTOR parameter LTF\_KEY) and transmitted NDP (TXVECTOR parameter LTF\_KEY) respectively.
* the *ltf\_iv* for received NDP(RXVECTOR parameter LTF-IV) and for transmitted NDP (TXVECTOR parameter LTF-IV) with corresponding ISTA MAC address and RSTA MAC address respectively together with the values of the Secure LTF Counter subfield and the block counter.

NOTE—In an R2I NDP used for range measurement, LTFs assigned to each of the recipient STAs would use their corresponding pseudorandom octet stream derived from the key material from the corresponding PTKSA for the recipient.

The values of the Secure LTF Counter subfield shall be maintained for the lifetime of a PTKSA used for secure LTF measurements. It shall not be reset between measurements and shall not be reset for multiple FTM negotiations using the same PTKSA.

The values of the Secure LTF Counter subfield used for each measurement protected bits is derived from a given Secure-LTF-Key-Seed (and its KDK and the PTKSA) and shall be unique. When the derived SAC is equal to 0, the RSTA shall increment the secure LTF counter parameter by 1 and derive the SAC until a nonzero SAC value is obtained. An RSTA shall also increment the secure LTF counter parameter by 1 each time an *ista-ltf-key* and *rsta-ltf-key* are derived.

**11.21.6.4.6 Transmission of a ranging NDP**

An RSTA transmitting an HE Ranging NDP or EHT Ranging NDP to one or more peer ISTAs shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_MU if the CH\_BANDWIDTH is equal to 320 MHz
  + Is set to HE\_SU otherwise
* The RANGING\_FLAG is present
* The UPLINK\_FLAG parameter is set to 0
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)) and non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)).
  + Is set to 1 in the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)).
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for R2I NPDs; it is set to 0 otherwise.
* In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)), the NUM\_USERS parameter is set to the number of ISTAs that the HE/EHT Ranging NDP is transmitted to.
* In the Non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)), the TXPWR\_LEVEL\_INDEX parameter is set to a value that matches the Tx Power value indicated in the R2I NDP Tx Power field in the following LMR frame, except if the value in the R2I NDP Tx Power field was set to a reserved value.
* The DOPPLER parameter is set to 0 if the FORMAT parameter is set to HE\_SU
* The NUM\_STS parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), set to the same value as the R2I NSTS subfield in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
  + In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)).
    - The NUM\_STS[*p*] is set to the same value as the R2I NSTS subfield in the STA Info field addressed to the corresponding STA *p* in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to more than one ISTA.
    - The NUM\_STS is set to the same value as the R2I NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1, when the HE/EHT Ranging NDP is transmitted to one ISTA.
  + In the Non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the R2I NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The LTF\_REP parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), set to the same value as the R2I Rep subfield in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
  + In the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)):
    - The LTF\_REP[*p*] is set to the same value as the R2I Rep subfield in the STA Info field addressed to the corresponding STA *p* in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to more than one ISTA.
    - The LTF\_REP is set to the same value as the R2I Rep subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1 when the HE/EHT Ranging NDP is transmitted to one ISTA.
  + In the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the R2I Rep subfield in the STA Info field with AID11 subfield less than or equal to 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The CH\_BANDWIDTH parameter is set as follows:
  + In the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)), and TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)), set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging Sounding Trigger frame
  + In the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)) and non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)), set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame
* In the TB and non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5](#H11o21o6o4o5)), the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF) and [11.21.6.4.5.3](#H11o21o6o4o5o3) (Non-TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present.
* In the TB ranging measurement exchange with secure LTF, the LTF\_OFFSET parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_OFFSET parameter is not present.
* If the FORMAT parameter is set to HE\_SU, the HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* If the FORMAT parameter is set to EHT\_MU the EHT\_LTF\_TYPE parameter is set to 2xEHT-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element transmitted by the RSTA
* The TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (26-3), replacing *D*HE\_NDPA by *D*Ranging\_NDP\_Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.

An ISTA transmitting an HE Ranging NDP or EHT Ranging NDP shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_MU if the CH\_BANDWIDTH is equal to 320 MHz
  + Is set to HE\_SU otherwise
* The RANGING\_FLAG is present
* The UPLINK\_FLAG parameter is set to 1
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the non-TB ranging measurement exchange ([11.21.6.4.4](#H11o21o6o4o4)).
  + Is set to 1 in the non-TB ranging measurement exchange with secure LTF ([11.21.6.4.5.3](#H11o21o6o4o5o3)),
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NPDs; it is set to 0 otherwise.
* The DOPPLER parameter is set to 0
* The NUM\_STS parameter is set to the same value as the I2R NSTS subfield in the STA Info field with AID11 subfield equal or less than 2007 in the preceding Ranging NDP Announcement frame plus 1.
* The LTF\_REP parameter is set to the same value as the I2R Rep subfield with AID11 subfield equal or less than 2007 in the STA Info field in the preceding Ranging NDP Announcement frame plus 1.
* The TXPWR\_LEVEL\_INDEX parameter is set to a value that matches the Tx Power value indicated in the I2R NDP Tx Power subfield in the STA Info field with the AID11 subfield set to 2045 in the preceding Ranging NPD Announcement frame, except if the value in the I2R NDP Tx Power subfield was set to a reserved value.
* The CH\_BANDWIDTH set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging NDP Announcement frame
* In the non-TB ranging measurement exchange with secure LTF, the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (Non-TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present
* The HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element received from the RSTA
* The TXOP\_DURATION parameter is set to either 127 or a value defined in Equation (26-3), replacing *D*HE\_NDPA by *D*Ranging NDP Announcement which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcementframe.

An ISTA transmitting an HE TB Ranging NDP or an EHT TB Ranging NDP to an RSTA shall set the TXVECTOR parameter as follows:

* The FORMAT parameter is set as follows:
  + Is set to EHT\_TB if the CH\_BANDWIDTH is equal to 320 MHz
* Is set to HE\_TB otherwiseThe RANGING\_FLAG is present
* The APEP\_LENGTH parameter is set to 0
* The SECURE\_LTF\_FLAG is set as follows:
  + Is set to 0 in the TB ranging measurement exchange ([11.21.6.4.3](#H11o21o6o4o3)).
  + Is set to 1 in the TB ranging measurement exchange with secure LTF ([11.21.6.4.5.2](#H11o21o6o4o5o2)).
* The TX\_WINDOW\_FLAG is set to 1 if the SECURE\_LTF\_FLAG is set to 1 and the RSTA and ISTA have negotiated to use the optional frequency domain Tx window for I2R NPDs; it is set to 0 otherwise.
* The DOPPLER parameter is set to 0
* The NUM\_STS parameter is set to the same value as the Number Of Spatial Streams subfield in the SS Allocation field in the User Info field in the preceding Ranging Sounding Trigger frame.
* The LTF\_REP parameter is set to the same value as the I2R Rep subfield in the User Info field in the preceding Ranging Sounding Trigger frame plus 1.
* The CH\_BANDWIDTH parameter is set to the same value as the TXVECTOR parameter CH\_BANDWIDTH in the preceding Ranging Sounding Trigger frame
* In the TB ranging measurement exchange with secure LTF, the LTF\_KEY parameter is set as defined in [11.21.6.4.5.2](#H11o21o6o4o5o2) (TB ranging measurement exchange with secure LTF). Otherwise, the LTF\_KEY parameter is not present
* The HE\_LTF\_TYPE parameter is set to 2xHE-LTF
* The GI\_TYPE parameter is set to 1u6s\_GI
* The SPATIAL\_REUSE parameter is set to SRP\_AND\_NON-SRG\_OBSS\_PD\_PROHIBITED
* The BSS\_COLOR parameter is set to the value indicated in the BSS Color subfield of the HE Operation element received from the RSTA

The TXOP\_DURATION parameter is set as defined in 26.11.5 (TXOP\_DURATION)

**11.21.6.4.7 Time of arrival estimationusing phase shift feedback**

Based on Figure [11-37u](#F11o37u) (Timing diagram of a Measurement Sounding phase in TB ranging based on phase shift of I2R NDP or R2I PPDUs), and Equation [(11-6e)](#E11o6e) , to enable the ISTA to derive the RTT, the RSTA needs to compute TOA t2 and feed t2 and t3 back to ISTA using R2I LMR. Instead of utilizing TOA t2 for RTT computation, a phase shift feedback can be prepared by RSTA and fed back to ISTA for deriving RTT.



**Figure 11-37u—Timing diagram of a measurement sounding phase in TB ranging based on phase shift of I2R NDP and R2I NDP PPDUs**

As shown in Figure [[11-37u](#F11o37u)](#F11o37s) (Timing diagram of a Measurement Sounding phase in TB ranging based on phase shift of I2R NDP and R2I NDP PPDUs), in the phase shift feedback method, the ISTA transmits an I2R NDP at TOD t1, and the RSTA determines the phase shift tp2 of the I2R NDP. The RSTA transmits a R2I NDP at TOD t3, and the ISTA determines the phase shift tp4 and TOA t4 of the R2I NDP. tp2 and tp4 are determined from the phase slope of the frequency domain channel estimation of the corresponding NDP. An example of calculation of the phase shift is shown in Annex AD.1.

The RSTA sends the R2I NDP at TOD t3, and after receiving the R2I NDP, the ISTA calculates the phase shift tp4 and TOA t4 of R2I NDP. The value of tp2 and tp4 are calculated utilizing the frequency domain channel estimation of I2R NDP and R2I NDP.

The phase shift is defined as the average linear phase shift between two adjacent tones normalized by the tone spacing. To enable the ISTA calculates the RTT, the RSTA should feed phase shift tp2 and TOD t3 back to the ISTA using R2I LMR, and the ISTA can calculate the RTT as:

RTTISTA = (t4 – t1) – (t3 – t2’’), with t2’’ = tp2 – (tp4 – t4) (11-6e)

When the I2R LMR with phase shift feedback is negotiated between ISTA and RSTA, I2R LMR carries phase shift tp4 and TOD t1, and then the RSTA can calculate the RTT as:

RTTRSTA = (t4’’ – t1) – (t3 – t2), with t4’’ = tp4 – (tp2 – t2)  (11-6f)

**11.21.6.4.8 Measurement exchange in passive TB ranging mode**

**11.21.6.4.8.1 General**

As stated in [11.21.6.1.3](#H11o21o6o1o3) (Passive TB ranging), the passive TB ranging mode is a variant of the TB ranging mode. In all aspects, except where explicitly stated differently, the passive TB ranging mode, its protocols, procedures, components, and definitions follow the rules for TB ranging mode.

In particular the measurement exchanges for passive TB ranging follows the rules and procedures described in [11.21.6.4.3](#H11o21o6o4o3) (TB ranging measurement exchange), with subclauses, unless explicitly stated otherwise.

In passive TB ranging, the RSTA shall transmit the Passive Sounding Ranging Trigger frame instead of the Sounding Ranging Trigger frame. Upon receiving of the Passive Sounding Ranging Trigger frame, if the bandwidth indicated by the frame is less than or equal to 160 MHz, the ISTA shall respond with an HE Ranging NDP instead of an HE TB Ranging NDP; if the bandwidth indicated by the frame is equal to 320 MHz, the ISTA shall respond with an EHT Ranging NDP instead of an EHT TB Ranging NDP; see [11.21.6.4.8.3](#H11o21o6o4o8o3) (Passive TB ranging measurement sounding phase) for further details.

Furthermore, the RSTA shall broadcast two frames, the Primary and Secondary RSTA Broadcast Passive TB Ranging Measurement Report frames containing measurement data and related information; see [11.21.6.4.8.4](#H11o21o6o4o8o4) (Passive TB ranging measurement reporting phase) for further details.

The passive TB ranging exchanges shall only occur in an availability window assigned for Passive TB ranging.

For passive TB ranging, the timestamps reported within each availability window shall be derived from a clock that runs continuously during the availability window.

If there is a discontinuity in the clock for the FTM timestamping between two reported TOD timestamps, then the TOD Not Continuous subfield in the Timestamp Error subfield of the Timestamp Measurement Report subfield in the ISTA Passive TB Ranging Measurement Report element shall be set to 1. Otherwise it shall be set to 0.

**11.21.6.4.8.2 Polling Phase of passive TB ranging**

The Polling phase of passive TB ranging follows the same rules and procedures for the Polling phase of TB ranging described in Subclause [11.21.6.4.3.2](#H11o21o6o4o3o2) (Polling Phase of TB ranging).

**11.21.6.4.8.3 Passive TB ranging measurement sounding phase**

The passive TB ranging measurement sounding follows the same rules and procedures for the measurement sounding for TB ranging described in [11.21.6.4.3.3](#H11o21o6o4o3o3) (TB ranging Measurement Sounding phase), unless explicitly stated otherwise.

The second phase of the passive TB ranging measurement sequence, after the passive TB ranging Polling phase, is called the passive TB ranging measurement sounding phase. The passive TB ranging measurement sounding phase may include one or more Passive Sounding Ranging Trigger frames and HE/EHT Ranging NDP exchanges, a Ranging NDP Announcement frame, and an HE/EHT Ranging NDP transmission; see Figure [11-37v](#F11o37v) (Passive TB ranging polling, Measurement Sounding, and Measurement Reporting phases).



**Figure 11-37v—Passive TB ranging polling, measurement sounding, and measurement reporting phases.**

In passive TB ranging, for each ISTA, the RSTA shall transmit a Passive Sounding Ranging Trigger frame, which includes a single User Info field.

An RSTA shall transmit one or more Passive Sounding Ranging Trigger frames, each of which is addressed to a single ISTA, the first one coming a SIFS time after the TB Polling phase.

An ISTA addressed by the AID/RSID in the Passive Sounding Ranging Trigger frame shall transmit an HE/EHT Ranging NDP a SIFS time after the reception of the Passive TB Ranging Ranging Trigger frame.

An RSTA transmitting a Passive Sounding Ranging Trigger frame shall not use a bandwidth wider than that indicated in the IFTM frame sent to the ISTA, and the RSTA shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the UL BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

NOTE—Generally a PSTA benefits from consistent ranging measurement performance when an RSTA initiates a passive TB ranging sequence with the nominal advertised bandwidth in every TXOP.

An RSTA transmitting a Ranging NDP Announcement frame and an HE/EHT Ranging NDP after receiving an HE/EHT Ranging NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

An ISTA transmitting an HE/EHT Ranging NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH\_BANDWIDTH to be the same value as the UL BW subfield of the Common Info field in the Passive Sounding Ranging Trigger frame.

If the CH\_BANDWIDTH of the Ranging NDP, either the I2R NDP or the R2I NDP, is equal to 320 MHz, the corresponding NDP shall be an EHT Ranging NDP and the R2I LMR in the corresponding measurement exchange sequence shall be transmitted in an EHT MU PPDU. Otherwise, the corresponding NDP shall be an HE Ranging NDP and the R2I LMR shall be transmitted in an HE MU PPDU.

As in TB ranging, an ISTA participating in a passive TB ranging exchange shall measure the TOD of its own HE/EHT Ranging NDP and either the TOAs, or both the TOAs and the phase shift feedback TOAs (PSTOAs), when it receives the RSTA’s HE/EHT Ranging NDP. In addition, optionally the ISTA may also measure and report either the TOAs, or both the TOAs and the PSTOAs, when it receives the HE/EHT Ranging NDPs transmitted by the other ISTAs participating in the passive TB ranging exchange. By reporting the timestamps for when it received the other ISTAs NDP transmissions, the quality of the location estimate for a PSTA listening in to the passive TB ranging exchanges can be improved.

The number of NSTS used in the passive TB ranging exchanges shall be less than or equal to 4.

When phase shift feedback is negotiated between an ISTA and an RSTA in passive TB ranging, the protocol for the measurement sounding phase differs from passive TB ranging with TOA feedback on the following points:

* The RSTA shall measure phase shift feedback TOA (PSTOA), in addition to measuring the TOA, on the I2R NPD it receives from the ISTA.
* The ISTA shall measure:  
  + the phase shift TOA (PSTOA), in addition to measuring the TOA, for the R2I NDP it receives from the RSTA,
  + and may also measure phase shift TOA(s) (PSTOAs), in addition to measuring the TOA(s), for the I2R NDP(s) it receives from other ISTA(s).

See Figure [11-37w](#F11o37w) (Example Timing diagram of a Measurement Sounding phase in passive TB ranging) for an example of timestamps measured by the RSTA, ISTA and a PSTA in a passive TB ranging measurement exchange. The timestamp values t1, t2, t3 and t4 are analogous to the corresponding labeled timestamps in [11.21.6.4.3.3](#H11o21o6o4o3o3) (Measurement Sounding phase of TB ranging). The timestamps t5 and t6 are the times at which the I2R NDP and R2I NDPs arrive at the PSTA, respectively.



**Figure 11-37w—Example timing diagram of a measurement sounding phase in passive TB ranging**

The PSTA may use the ISTA’s and RSTA’s timestamps, together with its own measured TOAs of the ranging NDPs, t5 and t6, to calculate its differential time of flight to the RSTA and the ISTA.

The differential time-of-flight (DToF) from PSTA to RSTA and ISTA (DToF\_PRI) is defined by Equation [(11-6g)](#E11o6g).

DToF\_PRI = ToF\_PR – ToF\_PI, (11-6g)

Where, ToF\_PR is the time of flight between the PSTA and the RSTA, and ToF\_PI is the time of flight between the PSTA and the ISTA. The differential time of flight DToF\_PRI can be computed as per Equation [(11-6h)](#E11o6h):

DToF\_PRI = t6 – t5 – 0.5 × t3’ + 0.5 × t2’ – 0.5 × t4’ + 0.5 × t1’, (11-6h)

where,

t1’ and t4’ are the time at which the I2R NDP was transmitted from the ISTA and the time at which the R2I NDP was received by the ISTA, respectively, converted by the PSTA from the ISTA’s time basis to the PSTA’s time basis.

t2’ and t3’ are the time at which the I2R NDP was received by the RSTA and the time at which the R2I NDP was transmitted by the RSTA, respectively, converted by the PSTA from the RSTA’s time basis to the PSTA’s time basis.

At the PSTA, the mechanism by which t1’ and t4’ is derived from t1, t4, the ISTA’s reported CFO, and the PSTA’s CFO measured with respect to the RSTA, is implementation dependent.

At the PSTA, the mechanism by which t2’ and t3’ is derived from t2, t3, and the PSTA’s CFO measured with respect to the RSTA, is implementation dependent.

By multiplying the differential time of flight, DToF\_PRI, with the speed of light, the differential distance from PSTA to RSTA and ISTA can be computed.

See [11.21.6.4.8.5](#H11o21o6o4o8o5) (Passive TB ranging differential time-of-flight calculations using phase shift TOA timestamps) for how the PSTA’s differential distance to the RSTA and the ISTA can be computed using PSTOAs measured by the RSTA and the ISTA.

**11.21.6.4.8.4 Passive TB ranging measurement reporting phase**

The passive TB ranging measurement reporting follows the same rules and procedures for the measurement reporting for TB ranging described in [11.21.6.4.3.4](#H11o21o6o4o3o4) (TB ranging Measurement Sounding phase), unless explicitly stated otherwise.



**Figure 11-37x—Passive TB ranging measurement reporting phase**

The last phase of the passive TB ranging measurement sequence is the passive TB ranging measurement reporting phase and occurs a SIFS time after the passive TB ranging measurement sounding phase; see Figure [11-37x](#F11o37x) (Passive TB ranging measurement reporting phase) for a depiction of the passive TB ranging measurement reporting phase.

In the passive TB ranging measurement reporting phase, an RSTA shall send a Passive TB Ranging Measurement Report frame and the Report Ranging Trigger frame to one or more ISTAs that sent an HE/EHT Ranging NDP in the preceding passive TB ranging measurement sounding phase. An ISTA addressed by the Report Ranging Trigger frame shall transmit an ISTA Passive TB Ranging Measurement Report frame a SIFS time after the Report Ranging Trigger frame transmission to report its I2R LMR.

In order to facilitate broadcasting of the ISTA’s timestamps by the RSTA the ISTA Passive TB Ranging Measurement Report frame shall be transmitted as a public Action frame.

The ISTA Passive TB Ranging Measurement Report element, see [[[[9.4.2.304](#H09o4o2o304)](#H09o4o2o304)](#H09o4o2o304)](#H09o4o2o302) (ISTA Passive TB Ranging Measurement Report element), in ISTA Passive TB Ranging Measurement Report frames shall contain:

* a Sounding Dialog Token Number identifying the measurement sounding phase in which the reported ISTA’s timestamps were measured;
* the CFO of the ISTA with respect to the RSTA;
* the TOD timestamp for the I2R NDP that the ISTA transmitted – labeled with the AID12/RSID12 of the ISTA;
* the TOA, timestamp for the R2I NDP that the ISTA received from the RSTA;
* optionally, the TOA timestamps for the I2R NDPs received from other ISTAs participating in the passive TB ranging (i.e. polling, sounding and reporting triplet) identified by the Sounding Dialog Token Number – labeled with their respective AID12/RSID12s.

If phase shift TOA reporting has been negotiated, the ISTA Passive TB Ranging Measurement Report element shall also include:

* the PS-TOA timestamp of the R2I NDP that the ISTA received from the RSTA; and
* optionally, the PS-TOAs for the I2R NDPs received from other ISTAs participating in the passive TB ranging (i.e. polling, sounding, and reporting triplet) identified by the Sounding Dialog Token Number– labeled with their respective AID12/RSID12s.

The ISTA Passive TB Ranging Measurement Report frame shall include an entry for the ISTA's I2R NDP TOD.

The ISTA shall set the More subfield in the More & N Timestamp Measurements Report field in the ISTA Passive TB Ranging Measurement Report element contained in the ISTA Passive TB Ranging Measurement Report frame to 1 if it has more timestamps ready to report but does not have space in its allocated resources by the RSTA for ISTA Passive TB Ranging Measurement Report frame. Else the ISTA shall set the More subfield to 0.

The RSTA shall send the Primary and Secondary RSTA Broadcast Passive TB Ranging Measurement Report frames, the Primary a SIFS time after receiving the ISTA Passive TB Ranging Measurement Report frames from the ISTA and the Secondary a SIFS following the Primary; see Figure [11-37x](#F11o37x) (Passive TB ranging measurement reporting phase).

The Primary RSTA Broadcast Passive TB Ranging Measurement Report frame shall contain the following:

* Passive TB Ranging LCI Table Counter
* Passive TB Ranging LCI Table Countdown Info
* RSTA Passive TB Ranging Measurement Report
* Passive TB Ranging LCI Table (optionally present)

Each time an RSTA transmits a Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, it shall set the Passive TB Ranging LCI Table Counter value such as to refer to the latest version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

If a Passive TB Ranging LCI Table element is included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, and this element has different content as compared to the last transmitted Passive TB Ranging LCI Table element, then Passive TB Ranging LCI Table Counter shall be incremented by 1 (modulo 256) from the value associated with the previous Passive TB Ranging LCI Table element content. (The first time the RSTA transmits a Passive TB Ranging LCI Table element the value shall be set to 0). This new value of the Passive TB Ranging LCI Table Counter is now associated with this new version of the Passive TB Ranging LCI Table element.

If a Passive TB Ranging LCI Table element is included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, and this element has the same content as the last transmitted Passive TB Ranging LCI Table element, then Passive TB Ranging LCI Table Counter value shall be the value associated with this last version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

If a Passive TB Ranging LCI Table element is not included in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, then the Passive TB Ranging LCI Table Counter value shall be the value associated with the last version of the Passive TB Ranging LCI Table element transmitted by the RSTA.

When the Passive TB Ranging LCI Table is present in the Primary Broadcast Passive TB Ranging Measurement Report frame, the RSTA LCI Report field of the Passive TB Ranging LCI Table Report element shall contain the Antenna Placement and Calibration subelement if the RSTA has dot11PassiveTBRangingAODImplemented equal to true, and shall not contain the Antenna Placement and Calibration subelement if the RSTA has dot11PassiveTBRangingAODImplemented equal to false.

When the Passive TB Ranging LCI Table is present in the Primary Broadcast Passive TB Ranging Measurement Report frame, the corresponding entree of the ISTA LCI Reports Entries field of the Passive TB Ranging LCI Table Report element shall contain the Antenna Placement and Calibration subelement if the ISTA has dot11PassiveTBRangingAoDImplemented equal to true, and shall not contain the Antenna Placement and Calibration subelement if the ISTA has dot11PassiveTBRangingAODImplemented equal to false.

The Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame shall contain the following:

* ISTA Passive TB Ranging Measurement Reports

See Subclause [9.6.7.52](#H09o6o7o52) (Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame format).

When phase shift feedback is negotiated between an ISTA and an RSTA in Passive TB ranging, the protocol for the measurement reporting phase differs from Passive TB ranging with TOA feedback on the following points:

* The RSTA shall report its measured PSTOA in the R2I LMR frame.
* The ISTA shall report its measured PSTOA(s), in addition to its measured TOA(s), in the ISTA Passive TB Ranging Measurement Report frame.
  + The PSTOAs are indicated as phase shift TOA timestamps by setting the Measurement Report field of the ISTA Passive TB Ranging Measurement Report element, see [9.4.2.304](#H09o4o2o304) (ISTA Passive TB Ranging Measurement Report element), to the value 10 (PSTOA).
* In the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame, the RSTA shall send a broadcast frame containing its measured PSTOA, in addition to its measured TOA, for the I2R NDPs it has received from the ISTA.
* In the Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame the RSTA shall rebroadcast the timestamps the ISTA has reported to the RSTA. As the ISTA has negotiated phase shift feedback, these would contain PSTOAs in addition to TOAs.

When phase shift feedback is negotiated in Passive TB ranging, the reporting by both the RSTA and the ISTA of phase shift TOAs, the TOD, and CFO shall be immediate feedback. The reported TOAs may be immediate or delayed feedback. When the TOA feedback is delayed, the dialog token shall refer to the previous measurement instance for the RSTA-ISTA pair.

The TODs and PSTOAs measured by the RSTA shall be broadcast in the Primary RSTA Broadcast Passive TB Ranging Measurement Report frame in the reporting phase following the measurement exchange in which they were measured.

The CFO, TOD, and PSTOAs reported by the ISTA shall be rebroadcasted in the Secondary RSTA Broadcast Passive TB Ranging Measurement Report frame in the reporting phase following the measurement exchange in which they were measured.

***Insert the following new clause:***

**11.21.6.4.9 Passive TB ranging differential time-of-flight calculations using phase shift TOA timestamps**

In Figure [11-37y](#F11o37y) (Example of passive TB ranging measurement exchanges with PSTOA measurements), passive TB ranging measurement exchanges and their reception by a passive station, a PSTA, are depicted for the case when the RSTA and the ISTA are measuring and reporting phase shift TOAs, PSTOAs; see Annex [AD.1](#AnnexADo1) for how the phase shift TOAs are calculated.

The RSTA measures the PSTOA tp2 and the ISTA measures the PSTOA tp4, in addition to measuring their TODs, t3 and t1 respectively. The ISTA also measures its CFO with respect to the RSTA. The ISTA reports its CFO and timestamps to the RSTA and the RSTA broadcasts these as well as its own timestamps to the PSTA.

The ISTA also measures and reports the TOA timestamps for the ranging NDPs it receives and the RSTA also measures and broadcasts the TOAs of the ranging NDPs it receives, as well as the ISTAs reported TOAs, though these timestamps are not used in the calculations described here.

****

**Figure 11-37y—Example of passive TB ranging measurement exchanges with PSTOA measurements.**

The differential time of flight from the PSTA to the RSTA and the ISTA (DToF\_PRI) is defined by Equation [(11-6i)](#E11o6i):

DToF\_PRI = ToF\_PR – ToF\_PI, (11-6i)

Where, ToF\_PR is the time of flight between the PSTA and the RSTA, and the ToF\_PI is the time of flight between the PSTA and the ISTA.

The differential time of flight (DToF\_PRI) can then be computed as as per Equation [(11-6j)](#E11o6j):

DToF\_PRI = t6 – t5 – 0.5 × t3’ + 0.5 × tp2’ – 0.5 × tp4’ + 0.5 × t1’.  (11-6j)

The timestamp t1’ is the time at which the I2R NDP was transmitted from the ISTA and the timestamp tp4’ is the PSTOA measurement for the time at which the R2I NDP was received by the ISTA, converted from the ISTA’s time basis to the PSTA’s time basis.

The timestamp tp2’ is the PSTOA measurement for the time at which the I2R NDP was received by the RSTA and t3’ is the time at which the R2I NDP was transmitted from the RSTA, converted from the RSTA’s time basis to the PSTA’s time basis.

At the PSTA, the mechanism by which t1’ and tp4’ is derived from t1, tp4, the ISTA’s reported CFO, and the PSTA’s CFO measured with respect to the RSTA is implementation dependent.

At the PSTA, the mechanism by which t2’ and tp3’ is derived from t2, tp3, and the PSTA’s CFO measured with respect to the RSTA is implementation dependent.

**3.2 Definitions specific to IEEE 802.11**

***TGbk editor: Please update subclause 3.2 as follows (track changes enabled):***

**Null-SAC-LTF** : A LTF present in an initiating STA (ISTA) to a responding STA (RSTA) null data PPDU (NDP), or RSTA to ISTA NDP in the Ranging frame exchange, resulting from a mismatch of sequence authentication code (SAC) subfield in the STA Info field of a Ranging NDP Announcement frame, or the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame, with either the value of the Validation SAC subfield in the Secure LTF Parameters element in the last transmitted FTM frame, or the last transmitted Location Measurement Report frame to the ISTA, or is equal to 0 . The TXVECTOR LTF\_KEY and LTF\_IV parameter corresponding to this LTF are set to generate any secure LTF or null.

**Straw Poll: Do you support to incorporate the proposed draft text in this document 11-23/0390r2 to the TGbk Draft 1.0?**

**Result: Yes/No/Abstain**