IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Specification Framework for TGaz** | | | | |
| **Date:** 2017-10-30 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **email** |
| Chao-Chun Wang | MediaTek Inc | 2840 Junction Ave, San Jose, CA | +1-408-526-1899 | [chao-chun.wang@mediatek.com](mailto:chao-chun.wang@mediatek.com) |

Abstract

This document provides the framework from which sections of the draft TGaz amendment.

The document provides an outline of each the functional blocks that will be a part of the final amendment. The document is intended to reflect the working consensus of the group on the broad outline for the draft specification and is derived from the set of functional requirements. As such it is expected to begin with minimal detail reflecting agreement on specific techniques and highlighting areas on which agreement is still required (<TBD> in the document). It may also begin with an incomplete feature list with additional features added as they are justified. The document will evolve over time until it includes sufficient detail on all the functional blocks and their inter-dependencies so that work can begin on the draft amendment itself.

**Revision history**

|  |  |  |
| --- | --- | --- |
| Revision | Date | Changes |
| 0 | Mar 14, 2016 | Initial Version |
| 1 | March 13, 2017 | R1 |
| 1.1 | May 11th , 2017 | R2 |
| 1.2 | June 25th, 2017 | R5 |
| 1.3 | August 20th, 2017 | R6 |
| 1.4 | October 30th, 2017 | R8 |
| 1.4 | November 3th, 2017 | R9 |

Contents

[1 Definitions 5](#_Toc497138176)

[2 Abbreviations and acronyms 6](#_Toc497138177)

[3 Positioning Protocol for Improved Accuracy and Coverage over 2.4 and 5 GHz bands 6](#_Toc497138178)

[3.1 General 6](#_Toc497138179)

[3.2 Protocol Description 7](#_Toc497138180)

[4 Positioning Protocol while operating in the 60 GHz band 9](#_Toc497138181)

[4.1 General 9](#_Toc497138182)

[5 Scalability aspects of the Positioning Protocol 11](#_Toc497138183)

[6 Security [May 2017] 12](#_Toc497138184)

[7 Using Angle of Departure and Angle of Arrival to estimate position 12](#_Toc497138185)

[8 Positioning Protocol for STA to STA topologies 13](#_Toc497138186)

[9 Frame formats 14](#_Toc497138187)

[10 References 16](#_Toc497138188)

# Definitions

FTM Initiator – the STA initiating the FTM procedure.

FTM Responder – the STA responding to the FTM Procedure establishment request

IFTM – Initial FTM frame.

IFTMR – Initial FTM Request frame.

**Type A Adversary – The attacker** is assumed to have response time to standard-specified OTA events or scenario dependent fields of 1 msec or longer.

**Type B Adversary - The attacker** is assumed to have response time to known OTA events or known pre-defined fields of 1usec or longer (up to 1msec). [2017/0120r2]

**Ranging Protocols –** Time of Flight (ToF) measurement; may be extended for others (needs more discussion)

* REVmc D8.0 Fine Timing Measurement Prototocol (**FTM**)
* VHT NDP Sounding-based .11az protocol (**VHTz**)
* HE NDP Sounding-based .11az protocol (**HEz**)
* Ranging protocol while operating in DMG/EDMG (**EDMGz**)

**Ranging ID** - Association ID-like value assigned to an unassociated STA by an rSTA to facilitate the negotiation phase and subsequently the ranging phase [September, 1473]

HEz mode

rSTA -

# Abbreviations and acronyms

MU – Multi User

SU – Single User

NDP – Null Data Packet

NDPA – NDP Announcement

VHT NDP Sounding-based .11az SU protocol (VHTz)

HEW NDP Sounding-based .11az MU protocol (HEWz)

TOF – Time Of Flight

BRP – Beam Refinement Protocol

# Positioning Protocol for Improved Accuracy and Coverage over 2.4, 5 and 60 GHz bands

## General

1. The .11az protocol shall extend the REVmc iFTMR/iFTM for .11az ToF measurement parameter negotiation
2. The .11az protocol shall support VHT, DMG, EDMG, andHE mode operation, named VHTz, DMGz, EDMGz**.** and HEz mode respectively.
3. The .11az protocol shall define the following phases

* Negation Phase (Capability discovery)
* Measurement Phase (a Time of Flight (ToF) measurement parameter negotiation)
* A set of ToF measurement exchanges

Note: Other protocol phases may be defined as needed and is <TBD> based on more discussion(s)

1. In the HEz mode, the protocol shall define a polling phase for ranging request feedback prior to NDP sounding-based measurement. [May 2017]
2. In the HEz mode, within the MU measurement phase the UL sounding shall use one or more of the following multiplexing techniques:
   1. Spatial Multiplexing using P-Matrix encoding,
   2. OFDMA multiplexing,
   3. TDMA multiplexing (various methods, TBD) [May 2017]

## Protocol Description

1. In the HEz mode, Negotiation phase shall support an enhancement to FTM Request frame in both SU and MU modes for both associated and unassociated STAs
2. In the HEz mode, the SU – SU negotiation procedure in the 11az shall have the following properties:
   1. Frame exchange sequence is the same as REVmc:
      1. FTM Request and Response frame formats needs to be updated, for example the response frame for unassociated STAs carry an ID (Ranging, Pre) and the NGP IE.
3. In the HEz mode, the 11az protocol shall support multiple STAs sending FTM Request in SU mode (SU PPDU) and the AP sends FTM Response in a SU PPDU to address multiple STAs” [July 2017]
4. In the HEz mode, The resource allocation for initial FTM request in MU negotiation for unassociated STAs to be based on OFDMA random access [May 2017]
5. In the HEz mode, the Measurement phase for the ranging protocol for Multiple STAs shall be only based on NDP sounding and have the following frame exchange sequence:



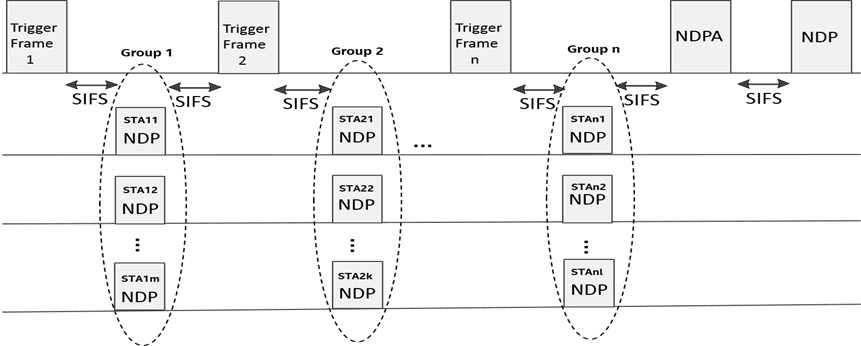
* Note : the detailed design of DL Trigger, DL NDPA, UL NDP, DL NDP are TBD.

1. The measurement phase for the ranging protocol for VHTz shall be based on IEEE 802.11 VHT sounding protocol and have the following frame exchange sequence



Note: the contents of NDP Announce (.11az), NDP (.11az) and Measurement Feedback; and the spacing between the NDP (.11az) and Measurement Feedback are TBD.

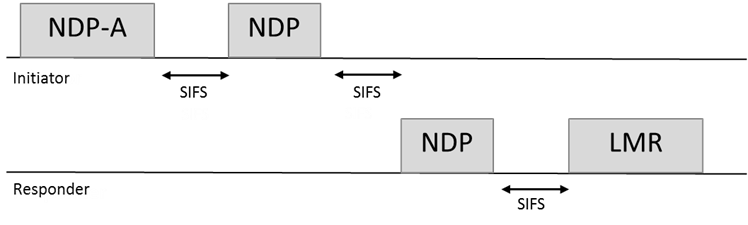
1. In the HEz mode, the measurement phase ranging protocol shall consists of one or more rounds of uplink sounding followed by one round of downlink sounding, where each round of uplink sounding includes one trigger frame soliciting one, or more NDP sounding frame(s) from STA(s) and the downlink sounding consists of one NDPA frame and one NDP sounding frame.
   1. Details of the NDP sounding structure are TBD. [May 2017]



1. For SU operation, the following behavior bounds the protocol development:
   * Only LMR feedback calculation (TOA) and then delivery may require a scheduling mechanism.
   * The SU case does not require a re-occurring availability window mechanism
   * [September, 2017 11-17-1305r2]
2. The SU ranging protocol will support both immediate and delayed reporting.
   * Note: The report formats (e.g. TOA, CSI) to be defined separately
   * [September, 2017 11-17-1305r2]
3. The SU measurement and measurement report sequence shall be:

NDPA (UL) <-SIFS-> NDP (UL) <-SIFS-> NDP (DL) <-SIFS-> LMR (DL)

Where for immediate feedback the LMR is of this round and for delayed the LMR is the feedback from previous round.”

****

1. In VHTz mode the iSTA shall not initiate another measurement sequence earlier than MinToaReady. If the iSTA initiates a following measurement sequence later than MaxToaAvailable, then the results may not be available (flushed)” [Septenmber, 2017 11-17-1305r2]



1. In the HEz mode, availability windows where the rSTA shall perform MU measurements are defined as follows:
   1. These availability windows are scheduled
   2. Within an availability window**,** rSTAs shall perform ranging activities related to polling, measurement, and measurement results and group related scheduling
   3. Each availability window consists by default of a single TXOP and can be extended to multiple TxOPs by announcement if single TxOP is insufficient to accommodate all STAs responding to the polling phase
   4. Availability windows are negotiated/signaled between AP and a STA such that the STA knows when those availability windows occur.
   5. A STA is not expected and does not perform MU ranging measurement and measurement results activities outside these windows. [September, 1455r1]
2. In HEz mode signaling behavior on LMR feedback scheduling is as follows
   1. Measurements and/or measurement results are provided for in the same availability window
   2. Measurement results may be from this window’s measurement or the results of a measurement performed in a prior window
   3. Protocol will support signaling for measurement results availability for current or next availability window within the measurement phase
   4. The Trigger control frame or the NDPA control frame carries a dynamic signaling of measurement results availability in this or next availability window

# Positioning Protocol while operating in the 60 GHz band

## General

1. The 11az protocol shall define at least one mode in which LOS/NLOS estimation (an estimation likelihood that the measurement is performed on a LOS path) is provided as part of the measurement.”
2. The 11az protocol shall define at least one mode in which BRP training may operate on the LOS path (rather than on the strongest path).”

# Scalability aspects of the Positioning Protocol

This section describes the protocol features that enable operation in a dense environment.

# Security [May 2017]

1. The security setup to be negotiated in a separate optional step prior to the 802.11az protocol parameter negotiation
   1. Note that in lieu of security negotiation, keys derived using an out-of-band mechanism may be used to secure the exchange between the initiator and the responder [May 2017]
2. The REVmc, HEz, and VHTz FTM modes, the fields over which range measurements are performed shall be protected against a VHT/HE Type B adversary attack [May 2017]
3. The DMGz and EDMGz FTM modes, the fields over which range measurements are performed shall be protected against a DMG/EDMG Type B adversary attack (TGaz R37)
4. In the PHY Security mode (VHTz, HEz, DMGz, EDMGz), the field used for channel/ToA measurement shall not include any form of repetition in time domain or structure that is predictable [September 2017, 1373r1]

# Using Angle of Departure and Angle of Arrival to estimate position

# Positioning Protocol for STA to STA topologies

# Frame formats

1. The Initial FTM Request shall include
   1. at least one of

-FTM Parameters element

*-NGP* Parameters element (optional subelements for ranging protocol- specific parameters)

* 1. optionally LCI and/or Location Civic Measurement Request element

-Trigger Field

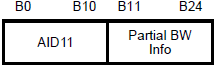
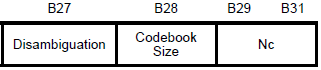
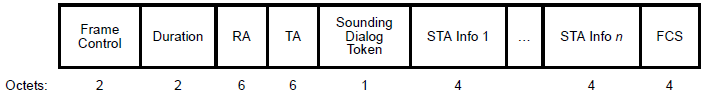
-Trigger field set to 1 (for 802.11-2016 FTM backward compatibility)

1. In 11az NDP ranging measurement phase, the NDPA has the following properties

B0 B1 bits value of the Sounding Dialog Token field shall be set to 0b10 to indicate 11az sequence

AID field will be used to indicate the receiver participating in the sounding exchange

Feedback Type field will be in 4-byte per STA info field (refer to the figure below)



Reserved

Reserved

Feedback

Type

B26

1. The ID for ranging operation for an unassociated STA used for measurement phase will be in the FTM Rsp frame
2. The protocol shall define a single Trigger Type field value for the 11az amendment and a Trigger Sub-type subfield in Trigger Dependent Common Info field [May 2017]
3. The NGP Parameters element includes:*At least one of VHTz-specific Subelement, HEz-specific subelement or EDMGz-specific subelement*

*Note: if the rSTA has not advertised support for the corresponding protocol it will ignore it if at least one supported protocol specific subelement is specified; otherwise the iFTM will have a status* Field in the FTM or NGP Parameters element is *not SUCCESSFUL*

1. The NGP Parameters element with the status Field in the FTM or NGP Parameters element is set to SUCCESSFUL, includes one of VHTz-specific Subelement, HEz-specific subelement or EDMGz-specific subelement
2. The Status and Value fields in the iFTM shall be set as defined in IEEE802.11-2016

[September 2017, 1473]

1. The VHTz-Specific subelement when included in the iFTMR shall include

<nothing defined yet>

[September 2017, 1473]

1. The VHTz-specific subelement when included in the iFTM with the status Field in the FTM or NGP Parameters element is set to SUCCESSFUL shall include
   1. Response: Immediate or Delayed
   2. if Response == Delayed
      1. MinToaReady and MaxToaAvailable
      2. the results (ToA/ToD) are delivered within the successive sounding sequence

[September 2017, 1473]

1. The HEz-Specific subelement when included in the iFTMR shall include
   1. Periodic Availability Window schedule

[September 2017, 1473]

1. The HEz-specific subelement when included in the iFTM with the Status Field in the FTM or NGP Parameters element is set to SUCCESSFUL shall include:
   1. Response: Immediate or Delayed
   2. If Response == Immediate
      1. results are provided in the same or next Availability Window based on a dynamic indication during the measurement phase
   3. If Response == Delayed
      1. results are of the measurements performed in the previous Availability Window
   4. Included only when Status Field in the FTM or NGP Parameters element is set to SUCCESSFUL
      1. Ranging ID assigned to the initiator

[September 2017, 1473]

# References

Missing refrences to submissions the SFD description comes from.

[] <https://mentor.ieee.org/802.11/dcn/17/11-17-1373-01-00az-phy-security-frd-and-srd-text.pptx>

[]<https://mentor.ieee.org/802.11/dcn/17/11-17-1455-01-00az-mu-measurement-and-feedback-scheduling.pptx>

[] https://mentor.ieee.org/802.11/dcn/17/11-17-1473-02-00az-11az-negotiation-protocol-update.pptx