

**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: 320 MHz positioning

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802.11bk™-2025
(Amendment to IEEE Std 802.11™-2024
as amended by IEEE Std 802.11bh™-2024,
and IEEE Std 802.11be™-2024)

IEEE Std 802.11bk™-2025
(Amendment to IEEE Std 802.11™-2024,
as amended by IEEE Std 802.11bh™-2024,
and IEEE Std 802.11be™-2024)

**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: 320 MHz positioning

Developed by the

LAN/WAN Standard Committee
of the
IEEE Computer Society

Approved 28 May 2025

IEEE SA Standards Board

Abstract: Modifications to both the IEEE 802.11 medium access control layer (MAC) and physical layers (PHY) are defined in this amendment. It enhances the Fine Timing Measurement protocol to make use of 320 MHz wide channels available with the IEEE 802.11be PHY and MAC.

Keywords: amendment, direction measurement, Fine Timing Measurement, FTM, IEEE 802.11™, IEEE 802.11bk™, positioning, ranging

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 September 2025. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-2544-5 STD28193
Print: ISBN 979-8-8557-2545-2 STDPD28193

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html>.

² Available at: <https://standards.ieee.org/thank-you/contact/>.

regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

³ Available at: <https://standards.ieee.org/about/contact>.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

⁴ Available at: <https://standards.ieee.org/standard/>

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials>.

Participants

At the time this amendment was sent to the IEEE SA Standards Board for approval, the IEEE 802.11 Working Group (WG) had the following officers:

Robert Stacey, *Chair*
Jon Walter Rosdahl, *1st Vice Chair*
Stephen McCann, *2nd Vice Chair*
Volker Jungnickel, *Secretary*

The officers of the Task Group bk and the members of the Working Group are as follows:

Jonathan Segev, *Chair*
Assaf Kasher, *Vice Chair*
Ali Raissinia, *Vice Chair*
Dibakar Das, *Secretary*
Roy Want, *Technical Editor*

Rana Abdelaal	Stéphane Baron	Ching-Chia Cheng
Shaima' Abidrabbu	David Barr	Paul Cheng
Mohamed Abouelseoud	Anuj Batra	Phoebe Cheng
Osama S. Aboumagd	Tuncer Baykas	Xilin Cheng
Tomoko Adachi	Chris Beg	Yajun Cheng
olubukola Adakeja	Firouz Behnamfar	George Cherian
Shubhodeep Adhikari	Jianwei Bei	James Chiang
Peyush Agarwal	Yaron Ben Arie	Rojan Chitrakar
Kosuke Aio	Friedbert Berens	Lin-Kai Chiu
Abdel Karim Ajami	Christian Berger	WenHsien Chiu
Dmitry Akhmetov	Nehru Bhandaru	Baw Chng
Srividhya Alagarsamy	Tong Bian	Hangyu Cho
Amer Al-Baidhani	Harry Bims	Jin Seek Choi
Carlos H. Aldana	Andreas Bluschke	Jinsoo Choi
Vamsi Amalladinne	Lennert Bobet	Tzu-Hsuan Chou
Song-Haur An	David Boldy	Liwen Chu
Amelia Andersdotter	Veerendra Boodannavar	Jinyoung Chun
Carol Ansley	Daniel Borges	Bruce Chung
Gary Anwyl	Albert Bredewoud	Chulho Chung
Diego Arlandis	Frank Burkhardt	Dana Ciochina
Antonio Arregui	Ugo Campiglio	John Coffey
Yusuke Asai	Radhakrishna Canchi	Javier Contreras Albesa
Alfred Asterjadhi	Necati Canpolat	Carlos Cordeiro
Kwok Shum Au	Rui Cao	Diana Cortes
Oscar Au	Laurent Cariou	D. Nelson Costa
Ziv Avital	William Carney	Claudio da Silva
Matthieu Avrillon	Edward Carter	Subir Das
Geert A. Awater	Dave Cavalcanti	Debashis Dash
Mehmet Aygul	Gurkan Cepni	Leonard Dauphinee
Shahnaz Azizi	Dongju Cha	Mike Davis
Agustin Badenes	Chen-Yi Chang	Rolf J. de Vegt
SunHee Baek	Clint F. Chaplin	Antonio DeLaOlivaDelgado
Christy Bahn	Matthew Chappell	Thomas Derham
Eugene Baik	Kirill Chemrov	Patrice Desmoulin
Gabor Bajko	Cheng Chen	Rocco Di Taranto
Hari Ram Balakrishnan	Cheng-Ming Chen	Yanyi Ding
Dmitry Bankov	Evelyn Chen	Mingjie Dong
Priyanka Bansal	Xiaogang Chen	Xiangdong Dong
Zhanjing Bao	You-Wei Chen	Rui Du

Zhenguo Du
Ruchen Duan
Richard Edgar
Alecsander Eitan
Ahmed ElSherif
Marc Emmelmann
Vinko Erceg
Serhat Erkucuk
Juan Fang
Yonggang Fang
Shuling Feng
David Ferruz
Domenico Ficara
Matthew J. Fischer
Paul Fletcher
Yuki Fujimori
Ming Gan
Trivikram Gangur
Mehdi Ganji
Ning Gao
Lalit Garg
Thomas Gee
Alireza Ghaderipoor
Chittabrata Ghosh
Ravi Gidvani
James P. K. Gilb
Sachin Godbole
Tim Godfrey
Bo Gong
Hemamali Gorthi
Fumihide Goto
Niranjan Grandhe
Michael Grigat
Xiangxin Gu
Romain Guignard
Jing Guo
Yuchen Guo
Zheng Guo
Ziyang Guo
Binita Gupta
Raghvendra Gupta
Luis Gutierrez
Taeyoung Ha
Muhammad Kumail Haider
David Halasz
Kenza Hamidouche
Mark Hamilton
Chong Han
Jonghun Han
Xiao Han
Thomas Handte
Zhao Hangbin
Christopher J. Hansen
Jeff Hansen
Daniel N. Harkins
Edward Harrison
Brian D. Hart
Philip Hawkes
Victor Hayes
Chuanfeng He
Ziming He
Ahmadreza Hedayat

Ahmed Helmy
Jerome Henry
Marco Hernandez
Lili Hervieu
Guido R. Hiertz
Ryuichi Hirata
Duncan Ho
Oliver Holland
Ching-Wen Hsiao
Hung-Tao Hsieh
Chien-Fang Hsu
Ostrovsky Hsu
Chunyu Hu
Mengshi Hu
Shengquan Hu
Xiaokun Hu
Chihan Huang
Guogang Huang
Kaikai Huang
Lei Huang
Po-Kai Huang
Qisheng Huang
Kazi Mohammed Saidul Huq
Sung Hyun Hyun Hwang
Hirohiko Inohiza
Salvador Iranzo
Insun Jang
Timothy Jeffries
Elliot YuChih Jen
Eunsung Jeon
Chenhe Ji
Feng Jiang
Hanjin Joh
Toby John
Allan Jones
Vincent Knowles IV Jones
Jorge Juarez
Insik Jung
Volker Jungnickel
Ishaque Ashar Kadampot
Carl W. Kain
Naveen Kakani
Manoj Kamath
Mahmoud Kamel
Sundeep Kancherla
Srinivas Kandala
HaoHua Kang
Kyu-Min Kang
Sugbong Kang
Teag Jin Kang
Shailender Karmuchi
Sudhir Kasargod
Oren Kedem
Richard H. Kennedy
John Kenney
Stuart J. Kerry
Francis Keshmiri
Vyatas R. Kezys
Naseem Khan
Samir Khericha
Evgeny Khorov
Dongwan Kim

Geon Hwan Kim
Hyungjin Kim
Jeongki Kim
Myeong-Jin Kim
Sang Gook Kim
Sanghyun Kim
Yongho Kim
Youhan Kim
Akira Kishida
Shoichi Kitazawa
Arik Klein
Andrey Klimakov
Jarkko Knecht
Geonjung Ko
Prashant Kota
Michail Koundourakis
Bruce P. Kraemer
Alexander Krebs
Chung-Ta Ku
Manish Kumar
Chih-Chun Kuo
Aleksey Kureev
Massinissa Lalam
Zhou Lan
Leonardo Lanante
James Lansford
Hyeong Ho Lee
Il-Gu Lee
Joonsoo Lee
Wookbong Lee
Ilya Levitsky
Joseph Levy
Bo Li
Guoqing Li
Jialing Li
Qinghua Li
Weiyi Li
Yan Li
Yanchun Li
Yapu Li
Ying Li
Yunbo Li
Dong Guk Lim
Hsin-De Lin
Wei Lin
Yousi Lin
Zinan Lin
Erik Lindskog
Chenchen Liu
Dekun Liu
Der-Zheng Liu
Jeff Liu
Jianhan Liu
Peng Liu
Ying Liu
Yong Liu
Vyacheslav Loginov
Miguel Lopez
Mikael Lorgeoux
Hanqing Lou
Hui-Ling Lou
Federico Lovison

Kaiying Lu
Liuming Lu
Kurt Lumbatis
Chaoming Luo
Yuanqiu Luo
Yunping (Lily) Lyu
Li Ma
Yongsen Ma
Yunsi Ma
Haji Muhammad Madni
Girish Madpuwar
Anilkumar Maguluri
Siukai Mak
Jouni K. Malinen
Hiroshi Mano
Abhishek Mantha
Zhi Mao
Roger Marks
Marcos Martinez Vazquez
Sebastian Max
Stephen McCann
Morteza Mehrnoush
Ezer Melzer
Jun Minotani
Shinya Miwa
Apurva Mody
Dignus-Jan Moelker
Pooya Monajemi
Michael Montemurro
Leo Montreuil
Juseong Moon
Hitoshi Morioka
Hiroyuki Motozuka
Robert Mueller
Lakshmi Narayana Mukkapati
Okan Mutgan
Yukimasa Nagai
Kengo Nagata
Gaurang Naik
Hiroki Nakano
Junyoung Nam
Vamadevan Namboodiri
Nima Namvar
Sai Shankar Nandagopalan
Narengerile Narengerile
Sharan Naribole
Karim Nassiri Toussi
Peshal Nayak
Azin Neishaboori
Patrice Nezou
Boon Loong Ng
An Nguyen
Paul Nikolich
Si-Chan Noh
Ryutaro Ohmoto
Hiraku Okada
John Olip
Hassan Omar
Stephen Orr
Masatomo Ouchi
Basak Ozbakis
Pooria Pakrooh

Saju Palayur
Stephen Palm
Sheetal Pandey
Thomas Pare
Jatin Parekh
Eunsung Park
Minyoung Park
Sungjin Park
Glenn Parsons
Abhishek Patil
Gaurav Patwardhan
Lan Peng
Ronny Peng
Eldad Perahia
James E. Petranovich
Albert Petrick
Brian Petry
Charlie Pettersson
Ron Porat
Sachin Pottigari
Clinton Powell
Dinakar Prabhakaran
Henry S. Ptasinski
Srinath Puducheri
Rethnakaran Pulikkoonattu
Emily H. Qi
Yinan Qi
Yue Qi
Yingqiao Quan
Saira Rafique
Kapil Rai
Rakshith Rajashekar
Vishnu Ratnam
Oded Redlich
Josh Redmore
Dror Regev
Mor Reich
Meriam Rezk
Maximilian Riegel
Mark Rison
Joerg Robert
Craig Rodine
Stephen Rodriguez
Jon Walter Rosdahl
Sayak Roy
Kiseon Ryu
Mohamed Salem
Sam Sambasivan
Stephan Sand
Amichai Sanderovich
Avik Santra
Ioannis Sarris
Naotaka Sato
Takuhiro Sato
Sigurd Schelstraete
Benedikt Schweizer
Andy Scott
Sangho Seo
Yongho Seok
Nikola Serafimovski
Kazunobu Serizawa
Ankit Sethi

Julien Sevin
Rubayet Shafin
Vesh Raj Sharma Banjade
Amit Shaw
Stephen J. Shellhammer
Andy Shen
Xiaoman Shen
Ian Sherlock
Shimi Shilo
Atsushi Shirakawa
Tongxin Shu
Isabelle Siaud
Graham Kenneth Smith
Luther Smith
Ju-Hyung Son
Hao Song
Ayush Sood
Robert Sosack
Sudhir Srinivasa
Veena Srivatsa
Robert Stacey
Dorothy Stanley
Adrian P. Stephens
Noel Stott
Paul Strauch
Rainer Strobel
Hang Su
Hongjia Su
Jung Hoon Hoon Suh
Takenori Sumi
Bo Sun
Jiaqi Sun
Li-Hsiang Sun
Yanbin Sun
YanJun Sun
Frank Suraci
Shuntaro Suzuki
Szymon Szott
Mineo Takai
Mohd Talha
Yusuke Tanaka
Zhuqing Tang
Rakesh Taori
Darshak Thakore
Sidharth Thakur
Sri Ramya Thota
Bin Tian
Hiromichi Tomeba
Alejandro Torrijo
Solomon B. Trainin
Tsung-Han Tsai
Genadiy Tsodik
Yuki Tsujimaru
Chunjiang Tu
Kiran Uln
Yoshio Urabe
Inaki Val
Richard D.J. Van Nee
Allert Van Zelst
Prabodh Varshney
Daniel Verenzuela
Lochan Verma

Sindhu Verma
Sameer Vermani
Santiago Vicent Colonques
Pascal Viger
Bo Wang
Chao Chun Wang
Hao Wang
Hejun Wang
Huizhao Wang
Lei Wang
Pu Wang
Qi Wang
Shukun Wang
Steven Qi Wang
Xiaofei Wang
Yi-Hsiu Wang
Zisheng Wang
Lisa Ward
Dong Wei
Hung-Yu Wei
Matthias Wendt
Menzo M. Wentink
Leif Wilhelmsson
Chao-Yi Wu
Guangsheng Wu

Kanke Wu
Tianyu Wu
Wayne Wu
Xuming Wu
John Wullert
Qing Xia
Bo Xiao
Liangxiao Xin
Yan Xin
Fangxin Xu
Weijie Xu
Yanchao Xu
Yue Xu
Hassan Yaghoobi
Ryota Yamada
Aiguo Yan
Min Yan
Peng Yan
Zhongjiang Yan
Subrahmanyam Yanamandra
Jay Yang
Lin Yang
Mao Yang
Rui Yang
Steve T.S. Yang
Xun Yang

Kazuto Yano
James Yee
Peter Yee
Yongjiang Yi
Su Khiong Khiong Yong
Yelin Yoon
Christopher Young
Heejung Yu
Jian Yu
Ruo Chen Zeng
Yan Zeng
Hongyuan Zhang
Jiayi Zhang
Jiayin Zhang
Rong Zhang
Yan Zhang
Yiyan Zhang
Yue Zhao
Lei Zhou
Pei Zhou
Richard (Yujia) Zhou
Lihua Zhu
Peiying Zhu
Juan Carlos Zuniga
Zhisong Zuo

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Tomoko Adachi
Thomas Alexander
Boon Chong Ang
Carol Ansley
Butch Anton
Alfred Asterjadhi
Kwok Shum Au
Stefan Aust
Christian Berger
Harry Bims
Maciej Borowka
Vern Brethour
William Byrd
Paul Cardinal
Clark Carty
Pin Chang
Cheng Chen
Paul Chiuchiolo
Claudio da Silva
Debashis Dash
Mike Davis
Hendricus De Ruijter
Xiandong Dong
Alecsander Eitan
Marc Emmelmann
Joseph Epstein
Luisandrey Fajardofajardo
Michael Fischer
P. Flynn
Avraham Freedman

Ming Gan
Prasanth Gopalakrishnan
Mark Hamilton
Jerome Henry
Marco Hernandez
Lili Hervieu
Ronald Hochnadel
Werner Hoelzl
Oliver Holland
David Hunter
Kazi Mohammed Saidul Huq
Tetsushi Ikegami
Raj Jain
SangKwon Jeong
Pranav Jha
Volker Jungnickel
Aniruddh Kabbinala
Lokesh Kabra
Ishaque Ashar Kadampot
Naveen Kakani
Srinivas Kandala
Piotr Karocki
Assaf Kasher
Stuart J. Kerry
Yongbum Kim
Youhan Kim
Shoichi Kitazawa
Jarkko Knecht
Takashi Kuramochi
Hyeong Ho Lee

James Lepp
Joseph Levy
Jialing Li
Qinghua Li
Weiyi Li
Daozhuang Lin
Ru Lin
Yong Liu
Greg Luri
Michael Lynch
Yongsun Ma
Jouni K. Malinen
Hiroshi Mano
William Rogelio Marchand Nino
Edward Mccall
Stephen McCann
Jonathon McLendon
Nedime Pelin Mohamed Hassan Salem
Michael Montemurro
Hiroyuki Motozuka
Ronald Murias
Rick Murphy
Yukimasa Nagai
Gaurang Naik
Karim Nassiri Toussi
Azin Neishaboori
Paul Nikolich
Stephen Orr
Satoshi Oyama
Pooria Pakrooh

Bansi Patel
Abhishek Patil
Gaurav Patwardhan
Arumugam Paventhan
Clinton Powell
Venkatesha Prasad
Henry Ptasinski
Kapil Rai
Alireza Raissinia
Maximilian Riegel
Benjamin Rolfe
Jon Walter Rosdahl
Stephan Sand
Naotaka Sato
Sigurd Schelstraete
Benedikt Schweizer
Jonathan Segev
Jhony Sembiring
Yongho Seok
Nikola Serafimovski

Rubayet Shafin
Iker Sobron
Robert Sosack
Robert Stacey
Dorothy Stanley
Owen Steinbacher, Jr.
Noel Stott
Walter Struppler
Mark Sturza
Bo Sun
Li-Hsiang Sun
Hongzhi Tao
Rakesh Taori
Bin Tian
Allert Van Zelst
Dmitri Varsanofiev
Prabodh Varshney
John Vergis
Harry Wang
Hejun Wang

Lei Wang
Qi Wang
Xiaohui Wang
Yi-Hsiu Wang
Stephen Webb
Dong Wei
Matthias Wendt
Scott Willy
Andreas Wolf
Qing Xia
Fangxin Xu
Peng Yan
Jay Yang
James Yee
Yu Yuan
Oren Yuen
Sven Zeisberg
Jiayi Zhang
Rong Zhang
Juan Carlos Zuniga

When the IEEE SA Standards Board approved this standard on 28 May 2025, it had the following membership:

Lei Wang, *Chair*
Jon Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au
Ted Burse
Xiaofeng (Alfred) Chen
Doug Edwards
Nehad El-Sherif
J. Travis Griffith
Deborah R. Hagar

Guido R. Hiertz
Ronald W. Hotchkiss
Tyler L. Jaynes
Thomas Koshy
Howard Li
Xiaohui Liu
Kevin W. Lu
Hiroshi Mano

Daleep C. Mohla
Annette D. Reilly
Robby Robson
Daniel Sabin
F. Keith Waters
Sha Wei
Luyang (Eric) Zhang

Introduction

This introduction is not part of IEEE Std 802.11bk-2025, IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 3: 320 MHz Positioning.

This amendment to IEEE Std 802.11-2024 defines modifications to both the IEEE 802.11 medium access control layer (MAC) and physical layers (PHY). It enhances the Fine Timing Measurement protocol to make use of 320 MHz wide channels available with the IEEE 802.11be PHY and MAC.

Contents

3. Definitions, acronyms, and abbreviations	18
3.2. Definitions specific to IEEE 802.11	18
8. PHY service specification	19
8.3 Detailed PHY service specifications.....	19
8.3.5 PHY SAP detailed service specification	19
9. Frame formats.....	20
9.3 Format of individual frame types.....	20
9.3.1 Control frames	20
9.4 Management and Extension frame body components	26
9.4.2 Elements.....	26
11. MLME.....	34
35. Extremely high throughput (EHT) MAC specification	83
35.14 PPDU format, bandwidth, MCS, NSS, and DCM selection rules	83
35.14.2 PPDU format selection.....	83
36. Extremely high throughput (EHT) PHY specification	83
36.2 EHT PHY service interface	83
36.2.2 TXVECTOR and RXVECTOR parameters.....	83
36.2.3 TRIGVECTOR parameters	86
36.2.3a LTFVECTOR parameters	87
36.3 Extremely high throughput (EHT) PHY specification.....	87
36.3.19a EHT Ranging NDP and EHT TB Ranging NDP.....	88
36.3.19b EHT-LTF field using secure EHT-LTF	92
36.3.20 Transmit specification.....	96
36.3.22 EHT transmit procedure.....	96
36.3.23 EHT receive procedure	97
Annex B (normative) Protocol Implementation Conformance Statement (PICS).....	98
B.2.2 General abbreviations for Item and Support columns.....	98
B.4.3 IUT configuration	98
B.4.37 Enhanced positioning (Ranging) features	99
Annex C (normative) ASN.1 encoding of the MAC and PHY MIB	100
C.3 MIB detail	100
Annex AE (informative) SIR-based attack detection	101

Figures

Figure 9-84—STA Info field format in a Ranging NDP Announcement frame if the AID11 is 2043.....	21
Figure 9-102—Trigger Dependent Common Info subfield format for the Ranging Trigger subvariants Poll, Sounding, Secure Sounding, and Report.....	22
Figure 9-103—Trigger Dependent Common Info subfield format of the Passive Sounding Ranging Trigger frame.....	22
Figure 9-104—User Info field format for the Poll and Report Ranging Trigger.....	23
Figure 9-105—User Info field format for Sounding subvariant.....	24
Figure 9-106—User Info field for Secure Sounding subvariant.....	25
Figure 9-723—FTM Parameters field format.....	26
Figure 9-1044—Ranging Parameters field format.....	27
Figure 9-1050a—320 MHz Ranging subelement Data field format.....	30
Figure 9-1051—Secure HE-LTF Parameters element format.....	31
Figure 9-1074bma—Puncture Pattern element format.....	32
Figure 9-1221—FTM frame Action field format.....	33
Figure 9-1237—LMR frame Action field format.....	33
Figure 11-48—TB ranging availability windows, each with one instance of a polling/sounding/reporting triplet.....	40
Figure 11-49—TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP.....	42
Figure 11-50—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs.....	42
Figure 11-50a—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs where only the first TXOP includes an ISTA in ELMSR mode.....	42
Figure 11-50b—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs where each TXOP includes an ISTA in ELMSR mode.....	43
Figure 11-52—TB ranging availability window with two ISTAs.....	44
Figure 11-53—Timing diagram of a measurement sounding phase in TB ranging.....	47
Figure 11-54—TB ranging availability window with multiple TF Ranging Sounding frames Sounding Ranging Trigger frames.....	48
Figure 11-55—Measurement sounding phase with I2R time-division multiplexing.....	48

Figure 11-56—TB ranging measurement reporting phase with bidirectional LMR feedback for n ISTAs .	50
Figure 11-58—Non-TB ranging measurement exchange sequence	52
Figure 11-59—Timing diagram of a measurement sounding phase in non-TB ranging	55
Figure 11-60—Non-TB ranging with immediate reporting.....	56
Figure 11-61—Non-TB ranging with delayed reporting.....	56
Figure 11-62—Illustration of min time between measurements and max time between measurements with delayed reporting.....	57
Figure 11-63—Non-TB ranging measurement exchange sequence with bidirectional LMR feedback	57
Figure 11-64—Overview of the TB ranging measurement exchange with secure HE-LTF	59
Figure 11-65—Error recovery of TB ranging measurement exchange using secure HE-LTF	63
Figure 11-66—Overview of the non-TB ranging measurement exchange with secure HE-LTF	64
Figure 11-67—Error recovery non-TB ranging measurement exchange using secure HE-LTF	67
Figure 11-68—ISTA secure HE-LTF octet stream generation.....	69
Figure 11-69—RSTA secure HE-LTF octet stream generation	70
Figure 11-72—Passive TB ranging polling, measurement sounding, and measurement reporting phases ..	77
Figure 11-73—Example timing diagram of a Mmeasurement Ssounding phase in passive TB ranging	79
Figure 11-74—Passive TB ranging Mmeasurement Rreporting phase	80
Figure 36-58a—EHT Ranging NDP format.....	88
Figure 36-58b—An example of an EHT-LTF field in an EHT Ranging NDP with NUM_USERS = 1, NUM_STS = 2, and LTF_REP = 2	89
Figure 36-58c—An example of a secure EHT-LTF field with NUM_USERS=2, NUM_STS = [2,1], and LTF_REP = [2,2].....	90
Figure 36-58d—EHT Ranging NDP format with secure EHT-LTFs.....	90
Figure 36-58e—EHT TB Ranging NDP format.....	91
Figure 36-58f—EHT TB Ranging NDP with secure EHT-LTFs.....	92
Figure 36-58g—Segment parser distributing pseudorandom octets to the sequences for each of the four 80 MHz subblocks in the 320 MHz secure EHT-LTF.....	93
Figure 36-58h—Segment parser example with one 40 MHz subband punctured	94
Figure AE-1—Attacking secure HE-LTF symbols	101
Figure AE-2—Received SIR after attack	102

Tables

Table 9-54—UL Target Receive Power subfield in Trigger frame	21
Table 9-56—Ranging Trigger Subtype subfield encoding	23
Table 9-373—Extended RSN Capabilities field.....	27
Table 9-412—Format And Bandwidth subfield	28
Table 9-413—Max R2I/I2R LTF Total subfields(11az)	29
Table 9-414—Ranging Subelement IDs for Ranging Parameters	29
Table 11-14aa—Subset of puncturing patterns in 320 MHz Ranging when Puncturing Pattern Support field set to 0	37
Table 36-1—TXVECTOR and RXVECTOR parameters	84
Table 36-2a—LTFVECTOR parameters	87
Table 36-62a—Pseudorandom octet index for each nonzero subcarrier index in the n-th quadruplet of 80 MHz segments.....	94

**IEEE Standard for Information Technology—
Telecommunications and Information Exchange between Systems
Local and Metropolitan Area Networks—
Specific Requirements**

**Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications**

Amendment 3: 320 MHz positioning

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using strikethrough (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

3. Definitions, acronyms, and abbreviations

3.2. Definitions specific to IEEE 802.11

Change two definitions in 3.2 as follows:

HE-long training field (LTF) repetitions: [LTF repetitions] Multiple transmissions of high efficiency (HE)-long training field (LTF), next generation vehicle to everything (NGV)-LTF, or extremely high throughput (EHT)-LTF symbols in an HE Ranging null data PPDU, (NDP), NGV Ranging NDP, or HE trigger based (TB) Ranging NDP, EHT Ranging NDP, or EHT TB Ranging NDP, where an ~~HE~~-LTF repetition value of 1 indicates no repetitions, and, for example, a value of 2 ~~or 3~~ would indicate twice ~~or three times~~ as many HE-LTF, NGV-LTF, or EHT-LTF symbols, respectively.

...

Null SAC HE-LTF: ~~Null-sequence Authentication Code (SAC)-Long Training field (LTF):~~ [Null-SAC-LTF] An HE-LTF ~~or EHT-LTF field value as a result of a SAC mismatch between an initiating STA (ISTA) to and a responding STA (RSTA), 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 Validation SAC subfield in the Secure HE 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 a secure HE LTF or null.~~

8. PHY service specification

8.3 Detailed PHY service specifications

Change 8.3.5 as follows:

8.3.5 PHY SAP detailed service specification

8.3.5.15 PHY-RXEND.indication

8.3.5.15.2 Semantics of the service primitive

...

- *IntegrityCheckError*. This value is used to indicate that during the reception of the HE Ranging NDP, ~~or~~ HE TB Ranging NDP, EHT Ranging NDP, or EHT TB Ranging NDP an integrity check was performed and failed.

8.3.5.18 PHY-RXLTFSEQUENCE.request

8.3.5.18.1 Function

This primitive is a request by the MAC sublayer to the local PHY entity to provide the parameters shown in [Table 27-3](#) (LTFVECTOR parameters) for the receipt of an HE Ranging NDP, EHT Ranging NDP, or HE TB Ranging NDP or EHT TB Ranging NDP.

8.3.5.18.2 Semantics of the service primitive

The primitive provides the following parameter:

```
PHY-RXLTFSEQUENCE.request(  
    LTFVECTOR  
)
```

The LTFVECTOR represents a list of parameters needed to receive an HE Ranging NDP, EHT Ranging NDP, or HE TB Ranging NDP, or EHT TB Ranging NDP, including the HE-LTF or EHT-LTF configuration and information on how to generate the secure ~~HE-LTF~~ symbols as described in [27.3.20.6](#) and [36.3.19b.4](#).

8.3.5.18.3 When generated

This primitive is issued by the MAC sublayer to the PHY entity before receiving HE Ranging NDP, ~~and~~ HE TB Ranging NDP, EHT Ranging NDP, and EHT TB Ranging NDP.

8.3.5.18.4 Effect of receipt

The effect of receipt of this primitive ~~is to configure by~~ the PHY entity with the following parameters, as they are not signaled in the PPDU header:

- ~~is to be aware of the number of spatial streams and~~ The number of HE-LTF or EHT-LTF repetitions,
- If secure LTF is used, the information needed to generate the secure LTF symbols based on the parameters in the LTFVECTOR as described in 27.3.20.6 and 36.3.19b.4.
- The number of spatial streams in an HE TB Ranging NDP, and HE Ranging NDP, EHT TB Ranging NDP, and EHT Ranging NDP.

~~that are not signaled in the HE SIG-A of the HE Ranging NDP and HE TB Ranging NDP, as well as to be able to generate the secure LTF symbols based on the parameters in the LTFVECTOR as described in 27.3.20.6 (Construction of secure HE LTF symbols), if secure HE LTF is used.~~

9. Frame formats

9.3 Format of individual frame types

9.3.1 Control frames

9.3.1.19 NDP Announcement frame format

9.3.1.19.4 Ranging NDP Announcement frame format

Change the text in seven paragraphs of 9.3.1.19.4 as follows:

When used as part of the TB ranging measurement exchange, see 11.21.6.4.3, the LTF Offset, R2I NSTS, and R2I Rep subfields are used to indicate the following R2I NDP's HE-LTF configuration, see 27.3.19.1; the I2R NSTS and the I2R Rep subfields are reserved.

When used as part of the non-TB ranging measurement exchange, the I2R NSTS and I2R Rep subfields are used to indicate the following I2R NDP's HE-LTF configuration, see 27.3.19.1 or I2R NDP's EHT-LTF configuration, see 36.3.4.1, while the R2I NSTS and R2I Rep subfields indicate the HE-LTF configuration or EHT-LTF configuration of the R2I NDP, respectively, sent in response by the RSTA, see 11.21.6.4.4.

The LTF Offset subfield is used in the TB ranging measurement exchange protocol with secure LTF (see 11.21.6.4.5.2); it indicates the number of HE-LTF or EHT-LTF to skip when processing the following NDP. The LTF Offset subfield is set to 0 in all other cases.

The R2I NSTS and I2R NSTS subfields indicate the number of spatial streams of the corresponding NDP and ~~is~~ are set to the number of spatial streams minus 1.

The R2I Rep and I2R Rep subfields are set to the number of ~~HE-LTF~~ repetitions of the corresponding HE Ranging NDP minus 1; i.e., the LTF repetitions of the corresponding HE Ranging NDP (see 27.3.19.1), or

EHT Ranging NDP (see 36.3.4.1). If the I2R and R2I Rep subfields have a value equal to 0, then there is no ~~HE~~-LTF repetition in the I2R and R2I NDP₁ respectively.

The Disambiguation subfield is set to 1 as in the STA Info field in an HE NDP Announcement frame regardless of the AID11 subfield.

The format of the STA Info field in a Ranging NDP Announcement frame when the AID is equal to 2043 is shown in Figure 9-84. It is used in the non-TB ranging measurement exchange with secure LTF to carry the sequence authentication code (SAC).

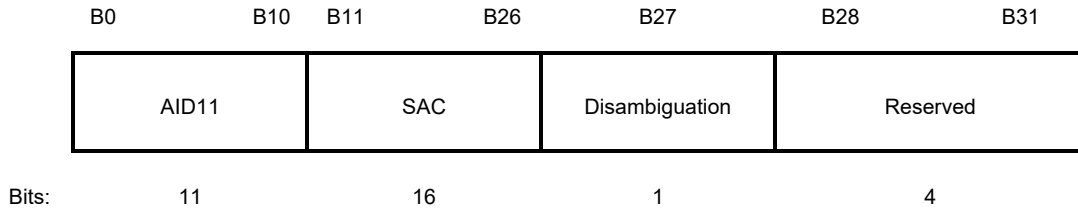


Figure 9-84—STA Info field format in a Ranging NDP Announcement frame if the AID11 is 2043

The SAC subfield contains the 16-bit SAC used in the non-TB ranging measurement exchange with secure LTF; see 11.21.6.4.5.3.

9.3.1.22 Trigger frame format

9.3.1.22.4 HE variant User Info field

Change Table 9-54 in 9.3.1.22.4 as follows:

Table 9-54—UL Target Receive Power subfield in Trigger frame

UL Target Receive Power subfield	Description
0–90	The expected received signal power, in units of dBm, is $Target_{pwr} = -110 + F_{val}$, where F_{val} is the subfield value.
91–126	Reserved
127	<p>The STA transmits the TB PPDU at the STA’s maximum transmit power for the assigned HE-MCS.</p> <p><u>If the eliciting trigger frame is a Sounding Ranging Trigger frame or a Passive Sounding Ranging Trigger frame, then the STA uses the maximum transmit power for HE-MCS 0 for an HE TB Ranging NDP and an HE Ranging NDP or EHT-MCS 0 for an EHT TB Ranging NDP and an EHT Ranging NDP.</u></p> <p><u>If the eliciting trigger frame is a Secure Sounding Ranging Trigger frame, then the STA uses the maximum transmit power for HE-MCS 6 for an HE TB Ranging NDP or EHT-MCS 6 for an EHT TB Ranging NDP.</u></p> <p><u>NOTE—The expected receive signal power is then the STA’s maximum transmit power for the assigned HE or EHT MCS minus the path loss.</u></p> <p><u>If the Trigger frame is a Sounding or Passive Sounding Ranging Trigger frame that does not assign an HE MCS, then the STA’s transmit power is that used for HE MCS 0.</u></p>

UL Target Receive Power subfield	Description
	<p>If the Trigger frame is a Secured Sounding Ranging Trigger frame that does not assign an HE MCS, the assigned HE MCS is assumed to be HE MCS 6 in terms of setting the STA's transmit.</p> <p>NOTE—The expected receive signal power is then the STA's maximum transmit power for the assigned HE MCS minus the path loss.</p>

Change 9.3.2.22.14 as follows:

9.3.1.22.14 Ranging Trigger-variant frame format

The Ranging Trigger Subtype subfield value in the Trigger Dependent Common Info field of the Ranging Trigger frame, ~~see as defined by Table 9-56, indicates~~ signals the Ranging Trigger frame subvariants, ~~which can be one of five Trigger frame types: Poll, Sounding, Secure Sounding, Report and Passive Sounding Ranging Trigger frame.~~

The format of the Trigger Dependent Common Info subfield for the Poll, Sounding, Secure Sounding, and Report Ranging Trigger frame, is shown in Figure 9-102. The Token field in the Trigger Dependent Common Info subfield is used in a Poll Ranging Trigger frame to match it with the partial TSF time in a following Ranging NDP Announcement frame. It is reserved in all other Ranging Trigger frame subvariants.

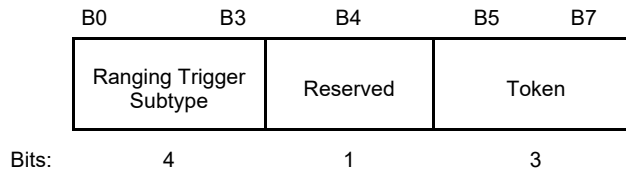


Figure 9-102—Trigger Dependent Common Info subfield format for the Ranging Trigger subvariants Poll, Sounding, Secure Sounding, and Report

The format of the Trigger Dependent Common Info subfield of a Ranging Trigger frame of subvariant Passive Sounding is shown in Figure 9-103. The Sounding Dialog Token Number subfield contains a value in the range of 0 to 63, which identifies a Measurement Sounding phase (I2R NDP and R2I NDP announced by a Sounding Trigger frame and the Ranging NDP Announcement frame, respectively), and the same value is included in the Sounding Dialog Token field of the Ranging NDP Announcement frame transmitted within the same availability window; see 9.3.1.19.

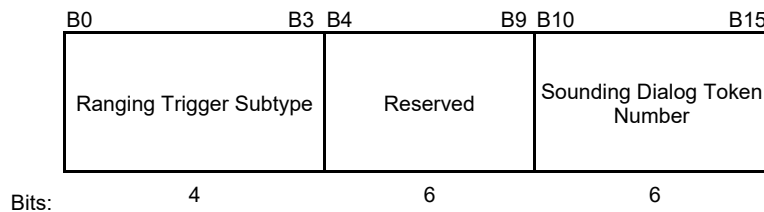


Figure 9-103—Trigger Dependent Common Info subfield format of the Passive Sounding Ranging Trigger frame

The value of the Ranging Trigger Subtype subfield for the Ranging Trigger frame is defined in Table 9-56.

Table 9-56—Ranging Trigger Subtype subfield encoding

Ranging Trigger Subtype subfield value	Ranging Trigger frame subvariant
0	Poll
1	Sounding
2	Secure Sounding
3	Report
4	Passive Sounding
5–15	Reserved

The RA field, and the CS Required and UL BW subfields in the Common Info field of the Ranging Trigger frame are identical to the Basic Trigger frame described in 26.5.2, 35.5.2, and 9.3.1.22, except that the RA field in Ranging Trigger frames with only one User Info field that is not a Special User info field (see 9.3.1.22.3) may be is either an unicast or broadcast individual or a group address.

The More TF subfield of the Common Info field of the Ranging Trigger frame indicates whether a subsequent Poll Ranging Trigger frame is scheduled for transmission within the availability window as defined in 11.21.6.4.3.

When a Ranging Trigger frame is addressed to ISTAs that all have in a TB ranging measurement exchange, see 11.21.6.4.3, with the same RSTA’s BSSID, the TA field of the Ranging Trigger frame is set to the RSTA’s address. The TA field is set to the transmitted BSSID, if the Trigger frame is addressed to a set of ISTAs in which at least two ISTAs are have in a TB ranging measurement exchange with different BSSIDs in the Multiple BSSID set of the RSTA.

9.3.1.23 Subvariants of Ranging Trigger variant

9.3.1.23.1 Poll subvariant

Change 9.3.1.23.1 as follows:

The format of the User Info field in the Poll Ranging Trigger frame is defined in Figure 9-104.

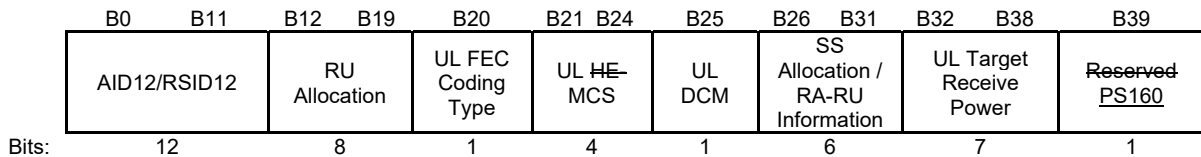


Figure 9-104—User Info field format for the Poll and Report Ranging Trigger

The AID12/RSID12 subfield carries either the ~~12~~twelve LSBs of the AID for an associated ISTA or the ~~12~~twelve LSBs of the RSID for an unassociated ISTA. The ~~RU Allocation, UL FEC Coding Type, UL HE-MCS, UL DCM, SS Allocation/RA-RU Information,~~ and UL Target Receive Power subfields are identical to the corresponding subfield in the Basic Trigger frame; see 9.3.1.22.

If the Poll Ranging Trigger frame is soliciting an HE TB PPDU:

- The RU Allocation, UL DCM, and SS Allocation/RA-RU Information subfields are identical to the corresponding subfields in the HE variant User Info field (9.3.1.22.4).
- The UL MCS subfield is identical to the UL HE MCS subfield in the HE variant User Info field.
- The PS160 subfield is reserved.

If the Poll Ranging Trigger frame is soliciting an EHT TB PPDU:

- The RU Allocation, SS Allocation/RA-RU Information, and PS160 subfields are identical to the corresponding subfields in the EHT variant User Info field (9.3.1.22.5).
- The UL MCS subfield is identical to the UL EHT MCS subfield in the EHT variant User Info field.
- The UL DCM subfield is reserved.

The Trigger Dependent User Info subfield is not present in the Poll Ranging Trigger frame.

9.3.1.23.2 Sounding subvariant

The format of the User Info field in the Sounding Ranging Trigger frame is defined in Figure 9-105.

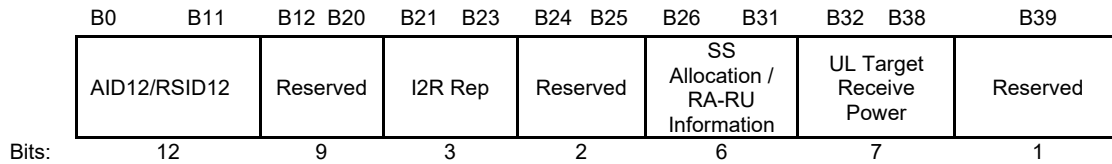


Figure 9-105—User Info field format for Sounding subvariant

The Trigger Dependent User Info subfield is not present in the Sounding Ranging Trigger frame.

The AID12/RSID12 subfield is identical to the corresponding subfield in the Poll Ranging Trigger frame.

The I2R Rep subfield indicates the number of ~~HE~~-LTF repetitions in the corresponding HE TB Ranging NDP or EHT TB Ranging NDP from the STA indicated in the AID12/RSID12 subfield; the I2R Rep subfield is set to the number of ~~HE~~-LTF repetitions minus 1. The value of the I2R Rep subfield is the same in all User Info fields in a single Trigger frame. If the Sounding Ranging Trigger frame is soliciting an HE TB Ranging NDP, the SS Allocation/RA-RU Information and UL Target Receive Power subfields are identical to the corresponding subfields in the HE variant User Info field of a Basic Trigger frame; see 9.3.1.22 9.3.1.22.4. If the Sounding Ranging Trigger frame is soliciting an EHT TB Ranging NDP, the SS Allocation/RA-RU Information and UL Target Receive Power subfields are identical to the corresponding subfields in the EHT variant User Info field of a Basic Trigger frame; see 9.3.1.22.5.

In both the HE variant Common Info field and the EHT variant Common Info field, the UL STBC, LDPC Extra Symbol Segment, Pre-FEC Padding Factor, and PE Disambiguity subfields are reserved.

The GI And HE-LTF Type subfield in the HE variant Common Info field is set to 1 ($2 \times \text{HE-LTF} + 1.6 \mu\text{s GI}$). The GI And HE/EHT-LTF Type field in the EHT variant Common Info field is set to 1 ($2 \times \text{EHT-LTF} + 1.6 \mu\text{s GI}$). The MU-MIMO HE-LTF Mode subfield in the HE variant Common Info field is set to 0 (HE single stream pilot HE-LTF mode).

The Doppler subfield in the HE variant Common Info field is set to 0.

NOTE—The UL Length subfield of a Trigger frame is computed using Equation (27-11) (see 26.5.2.2.4) for soliciting HE PPDU and Equation (36-11) (see 35.5.2.2.4) for soliciting EHT PPDU, which is based on the TXTIME computed in 27.4.3 for HE PPDU and 36.4.3 for EHT PPDU. In case of Sounding Ranging Trigger frame, the resulting UL Length value is equivalent to $13 + 6 \times N_{LTF-REP}N_{HE-LTF}$, where $N_{LTF-REP}$ is the number of HE-LTF repetitions (given by the I2R Rep subfield value plus 1) and N_{HE-LTF} is the number of HE-LTF symbols (given by the Number Of HE-LTF Symbols And Midamble Periodicity subfield), see Figure 9-90a; or is the Number Of HE/EHT-LTF Symbols subfield, see Figure 9-90b.

9.3.1.23.3 Secure sounding subvariant

The format of the User Info field in the Secure Sounding Ranging Trigger is defined in Figure 9-106. There is a single User Info field that is not a Special User Info field in a Secure Sounding Ranging Trigger frame.

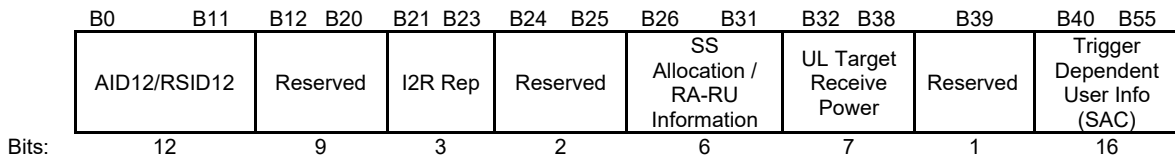


Figure 9-106—User Info field for Secure Sounding subvariant

The AID12/RSID12 subfield is identical to the corresponding subfield in the Poll Ranging Trigger frame.

The I2R Rep subfield is identical to the corresponding subfield in the Sounding Ranging Trigger frame.

The SS Allocation/RA-RU Information and UL Target Receive Power subfields are identical to the corresponding subfields in the Sounding Ranging Trigger frame; see 9.3.1.23.2. ~~Basic Trigger frame~~; see 9.3.1.22.

The Trigger Dependent User Info subfield is present in the Secure Sounding Ranging Trigger frame. The Trigger Dependent User Info subfield carries the Sequence Authentication Code (SAC) field. The SAC subfield provides the authentication information for the LTF Sequence Generation information used for the I2R sounding associated with the measurement instance; see 11.21.6.4.5. The length of this subfield is 16 bits.

NOTE—For measurement exchange with secure HE-LTF, the I2R Rep is set to the *RSTA Assigned I2R Rep*; see 11.21.6.3.4.

~~In the Common Info field, the MU MIMO HE LTF Mode, UL STBC, LDPC Extra Symbol Segment, Pre-FEC Padding Factor, and PE Disambiguity subfields are reserved. The GI And HE LTF Type and Doppler subfields in the The HE variant Common Info field and EHT variant Common Info field are set as in the Sounding Ranging Trigger frame; see 9.3.1.23.2.~~

9.3.1.23.4 Report subvariant

The format of the User Info field in the Report Ranging Trigger frame is defined in Figure 9-104 and the subfields of the User Info field are identical to the corresponding subfields in the Poll Ranging Trigger frame soliciting an HE TB PPDU or an EHT TB PPDU.

The Trigger Dependent User Info subfield is not present in the Report Ranging Trigger frame.

9.3.1.23.5 Passive sounding subvariant

The Passive Sounding Ranging Trigger frame follows the definition of the Sounding Ranging Trigger frame except that the RA field is always set to the broadcast address. There is a single User Info field that is not a Special User Info field in a Passive Sounding Ranging Trigger frame.

9.4 Management and Extension frame body components

9.4.2 Elements

9.4.2.1 General

Change Table 9-130 as follows (the entire table is not shown):

Element	Element ID	Element ID Extension	Extensible	Fragmentable
...				
Puncture Pattern Element	254	1	Yes	No
Secure HE-LTF Parameters (see 9.4.2.301)	255	94	Yes	No

9.4.2.166 FTM Parameters element

Change Figure 9-723 as follows:

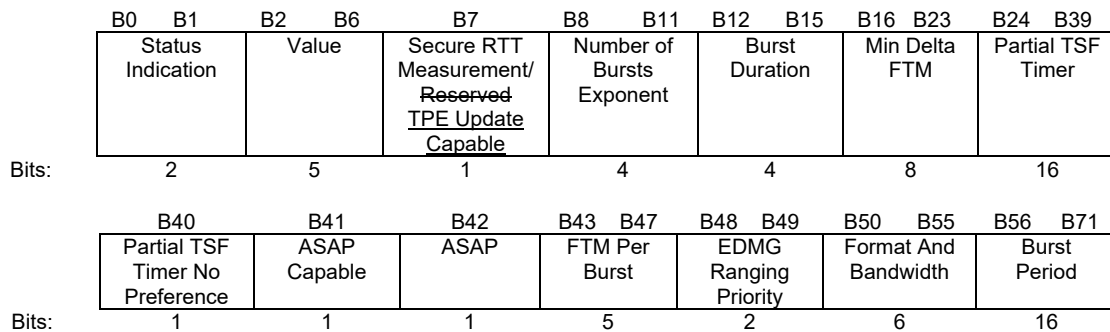


Figure 9-723—FTM Parameters field format

Change 9.4.2.166 FTM Parameters element as follows:

For secure EDMG ranging, the Secure RTT Measurement/TPE Update Capable subfield is set to 1 by an ISTA to request a secure RTT measurement exchange between an ISTA and an RSTA; see 11.21.6.3.32. The Secure RTT Measurement/TPE Update Capable subfield is set to 1 by an RSTA to acknowledge a secure RTT measurement exchange, and to 0 otherwise. ~~In cases other than secure EDMG ranging, the Secure RTT Measurement subfield is reserved.~~ For EDCA based ranging of non-EDMG STAs, the Secure RTT Measurement/TPE Update Capable subfield is set to 1 to indicate that a STA is capable of transmitting or receiving the Transmit Power Envelope element during the FTM session, and to 0 otherwise.

9.4.2.239 Non-Inheritance element

Change Table 9-373 bit 8 as follows:

Table 9-373—Extended RSN Capabilities field

Bit	Information	Notes
...
8	Secure HE -LTF Support	A STA sets the Secure HE -LTF Support field to 1 when dot11SecureLTFImplemented is true. Otherwise, the STA sets the Secure HE -LTF Support field to 0. See 11.21.6.4.5.
...

9.4.2.300 Ranging Parameters element

Change Figure 9-1044 as follows:

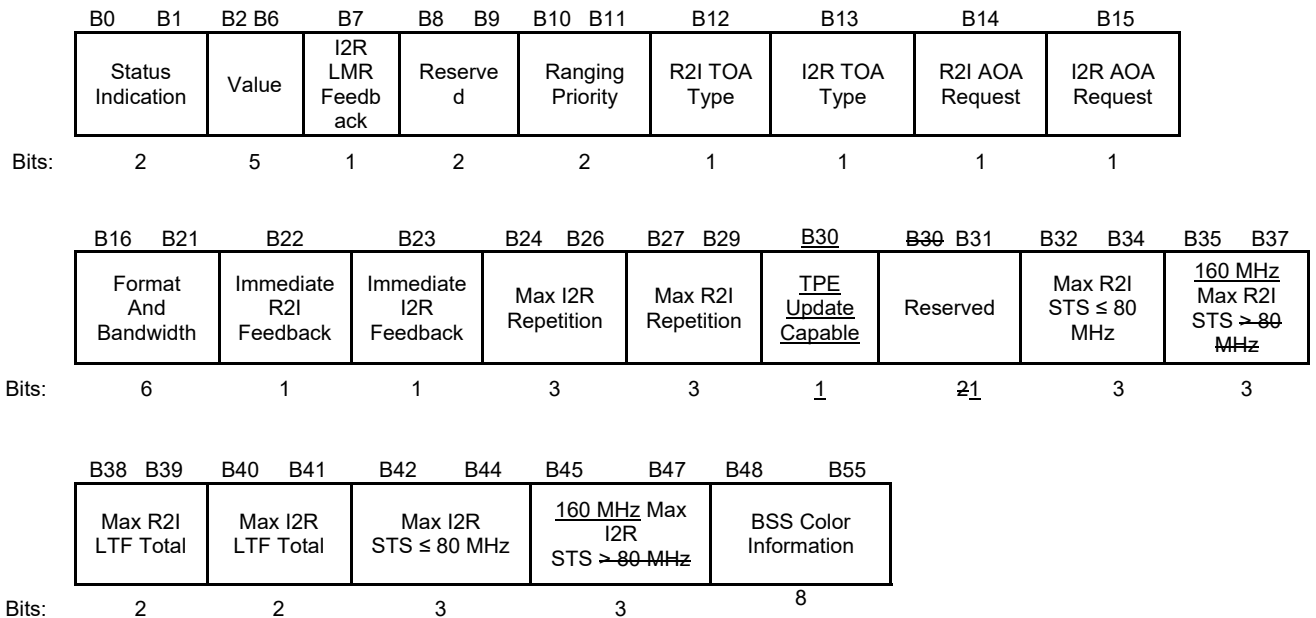


Figure 9-1044—Ranging Parameters field format

... ..

Change the text in 9.4.2.300 following the NOTE as follows:

NOTE—The values of 0 to 7 contained in the Max I2R Repetition and Max R2I Repetition subfields are mapped to the values 1 to 8 for the number of HE-LTF repetitions, respectively.

The TPE Update Capable subfield is set to 1 to indicate that a STA is capable of transmitting or receiving the Transmit Power Envelope element during the FTM session, and to 0 otherwise.

The Ranging Priority subfield of the Ranging Parameters field of the Ranging Parameters element in the IFTMR frame contains the ISTA’s ranging priority request, which indicates the time sensitivity of a ranging operation, and it is set according to Table 9-323.

Change the following table and text in 9.4.2.300:

The Format And Bandwidth subfield indicates the requested or allocated PPDU format and bandwidth used to transmit the I2R/R2I NDP exchange as part of the non-TB ranging, or TB ranging measurement exchange; see 11.21.6.4.3 and 11.21.6.4.4. The encoding of this subfield is given in Table 9-412.

Table 9-412—Format And Bandwidth subfield

Field value	Format	Bandwidth
0	HE	20
1	HE	40
2	HE	80
3	HE	80+80
4	HE (two separate RF LOs)	160
5	HE (single RF LO)	160
6	NGV	10
7	NGV	20
<u>8</u>	<u>EHT</u>	<u>320</u>
9–63	Reserved	Reserved
NOTE—Values 6 and 7 are supported only when dot11NGVOptionImplemented is true.		

The values of 3, 4, and 5 indicate STA support for 160 MHz operation as either 80+80, 160 two-LO, or 160 single-LO, respectively, in addition to supporting 80 MHz, 40 MHz, and 20 MHz bandwidths (e.g., a field value of 5 does not mean the device supports all 160 MHz options but rather 160 MHz single LO).

The field value of 8 specifies the STA support for 320 MHz operation as 320 MHz using EHT format in addition to supporting 160 single RF LO, 80, 40, and 20 MHz bandwidths in HE format.

Change the paragraph in 9.4.2.300 as follows:

The 160 MHz Max R2I STS ~~> 80 MHz~~-subfield indicates for a ~~bandwidths greater than 80~~ 160 MHz bandwidth the maximum number of space-time streams to be used in R2I NDP in the session.

... ..

Change the text in 9.4.2.300 as follows:

The Max R2I LTF Total and Max I2R LTF Total subfields indicate the maximum number of HE-LTFs or EHT-LTFs to be destined to an ISTA in the R2I NDP and an RSTA in an I2R NDP, respectively, the encoding is given in Table 9-413. The maximum number of HE-LTFs or EHT-LTFs limits the allowed combinations of the number of space-time streams and HE-LTF repetitions.

Table 9-413—Max R2I/I2R LTF Total subfields

Field value	Max number of HE-LTFs or EHT-LTFs
0	4
1	8
2	16
3	64

Change the following paragraph in 9.4.2.300 as follows:

The 160 MHz Max I2R STS ~~> 80 MHz~~-subfield indicates for ~~a bandwidths greater than 80 of 160 MHz bandwidth~~ the maximum number of space-time streams to be used in I2R NDP in the session.

Insert one new subelement ID for the 320 MHz Ranging subelement in the table as follows:

Table 9-414—Ranging Subelement IDs for Ranging Parameters

Subelement ID	Name	Extensible
0	Non-TB Specific subelement	Yes
1	TB-specific subelement	Yes
2	Secure HE-LTF subelement	Yes
<u>3</u>	<u>320 MHz Ranging subelement</u>	<u>Yes</u>
34 –220	Reserved	
221	Vendor Specific	
222–255	Reserved	

... ..

Change the following paragraphs in 9.4.2.300 as shown:

The Secure HE-LTF subelement is included in the IFTMR frame to indicate that the initiator supports use of secure HE-LTF and the associated parameters; it is included in the IFTM if the initiator and the responder successfully negotiate an FTM session where secure HE-LTF is used.

The format of the Secure HE-LTF subelement is as shown in Figure 9-1050.

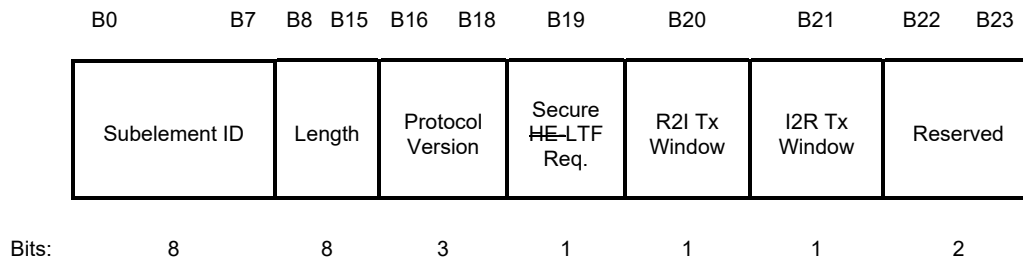


Figure 9-1050—Secure HE-LTF subelement format

The Subelement ID and Length fields are defined in Figure 9-1050.

The Protocol Version field in the IFTMR frame is set to the value 0 by the ISTA, with values 1 to 7 reserved for future use; see Table 9-415. In the IFTM frame, the Version field is set to the value 0 by the RSTA, with values 1 to 7 reserved for future use. The interpretation of the version field in the IFTMR frame and IFTM frame, and the possible resulting actions, are described in 11.21.6.3.4.

The Secure HE-LTF Required field is set to 1 by the ISTA to indicate it requires secure HE-LTF to be enabled and is set to 1 by the RSTA to enable a secure HE-LTF measurement exchange between an ISTA and an RSTA. Otherwise, the Secure HE-LTF Required field is set to 0.

The R2I Tx Window field in the IFTMR frame is set to 1 to indicate the ISTA requests use of the optional frequency domain Tx Window in the R2I NDPs, and 0 to indicate the default frequency domain Tx window. In the IFTM frame, the R2I Tx Window field is set to 1 to indicate the RSTA will use the optional frequency domain Tx window in the R2I NDPs, and 0 to indicate the default frequency domain Tx window; see Table 9-415.

The I2R Tx Window field in the IFTMR frame is set to 1 to indicate that the ISTA supports use of the optional frequency domain Tx window in the I2R NDPs, and 0 to indicate the default frequency domain Tx window. In the IFTM frame, the I2R Tx Window field is set to 1 by the RSTA to request that the ISTA use the optional frequency domain Tx window in the I2R NDPs, and 0 to indicate the default frequency domain Tx window; see Table 9-415.

Table 9-415 Secure HE-LTF protocol section identifier

Protocol Version	Secure HE-LTF PHY sections
0	27.3.19 <u>36.3.19a</u>
1–7	Reserved

Insert the following definition for the new subelement at the end of this subclause:

The format of the 320 MHz Ranging subelement follows the definition in Figure 9-1078. The Subelement field is set according to Table 9-414. The Length field is defined in 9.4.3.

The Data field format is as shown in Figure 9-1050a.

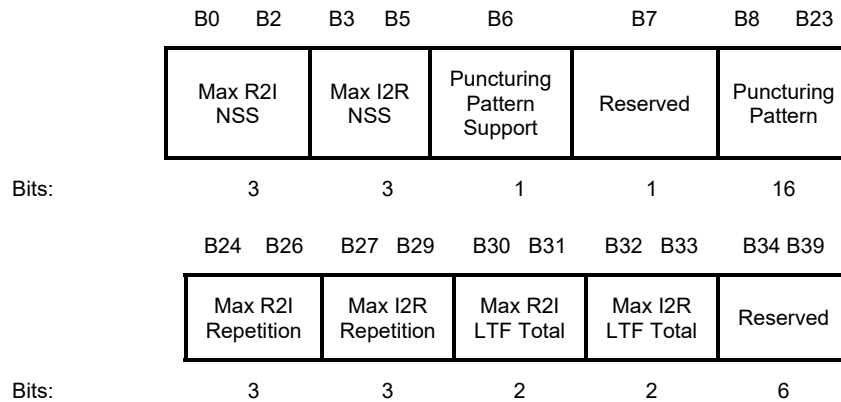


Figure 9-1050a—320 MHz Ranging subelement Data field format

The Max R2I NSS field indicates the maximum number of spatial streams to be used in an R2I NDP for 320 MHz PPDU bandwidth transmissions in the session.

The Max I2R NSS field indicates the maximum number of spatial streams to be used in an I2R NDP for 320 MHz PPDU bandwidth transmissions in the session.

The Puncturing Pattern Support field is set to 1 to indicate support of all puncturing patterns as listed in Table 36-30; it is set to 0 to indicate support of only the subset of puncturing patterns defined in Table 11-14aa.

The Puncturing Pattern field is used by the RSTA to convey the disabled subchannel bitmap to the ISTA in the IFTM frame. It is reserved when included in the IFTMR frame by the ISTA.

The Max R2I Repetition field indicates the maximum number of LTF repetitions that the RSTA uses in the preamble of an R2I NDP for 320 MHz PPDU bandwidth transmission; the subfield is set to the number of LTF repetitions minus 1.

The Max I2R Repetition field indicates the maximum number of LTF repetitions that the ISTA uses in the preamble of an I2R NDP for 320 MHz PPDU bandwidth transmission; the subfield is set to the number of LTF repetitions minus 1.

The Max R2I LTF Total and Max I2R LTF Total fields indicate the maximum number of EHT-LTFs to be destined to an ISTA in the R2I NDP and an RSTA in an I2R NDP, respectively, for 320 MHz PPDU bandwidth transmission. The encoding is given in Table 9-413.

Change “HE-LTF” to “LTF” in the following subclauses and Figure 9-1049 as shown:

9.4.2.301 Secure ~~HE~~-LTF Parameters element

The Secure ~~HE~~-LTF Parameters element is optionally included in the IFTM frame, as described in 9.6.7.33, and the LMR frame, as described in 9.6.7.49, for a secure ~~HE~~-LTF measurement exchange mode of the non-TB ranging and TB ranging measurement exchange (see 11.21.6.4.5). The use of the Secure ~~HE~~-LTF Parameters element is described in 11.21.6.

The format of the Secure ~~HE~~-LTF Parameters element is shown in Figure 9-1051.

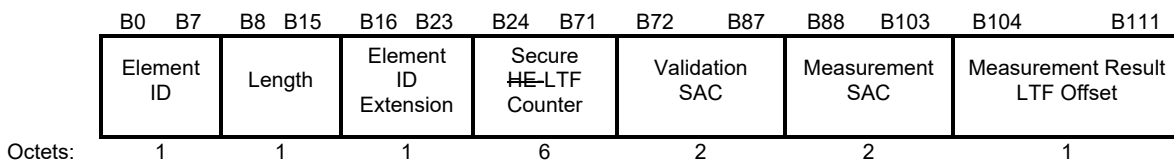


Figure 9-1051—Secure ~~HE~~-LTF Parameters element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Secure ~~HE~~-LTF Counter field is used to determine the randomized LTF sequence of an I2R NDP and R2I NDP in one of the following secure ~~HE~~-LTF measurement exchange sequences:

- An I2R NDP and an R2I NDP immediately following a Ranging NDP Announcement frame, in a non-TB ranging measurement exchange (11.21.6.4.4).
- A sequence of an I2R NDP, a Ranging NDP Announcement frame, an R2I NDP, in a TB ranging measurement exchange (11.21.6.4.3).

The Secure ~~HE~~-LTF Counter field is used in the IFTM frame and the R2I LMR frame when part of a secure ~~HE~~-LTF measurement exchange; it is reserved otherwise.

The Validation SAC field is a nonzero value associated with the secure ~~HE~~-LTF counter carried in the same Secure HE-LTF Parameters element and validates the randomized LTF sequence; see 11.21.6.3.4. This field is used in the initial protected FTM frame, the R2I protected LMR frame, and is reserved otherwise.

The Measurement SAC field is used to verify that range measurement results contained in the LMR frame are calculated using the same LTF sequence between ISTA and RSTA. The Measurement SAC field is the same value as the SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP in the non-TB ranging measurement exchange or the SAC subfield in the Trigger Dependent User Info of the Secure Sounding Ranging Trigger frame in the TB ranging measurement exchange; see 11.21.6.4.5. This field is reserved in the IFTM frame.

Insert new subclause 9.4.2.331 as follows:

9.4.2.331 Puncture Pattern element

The format of the Puncture Pattern element is shown in Figure 9-1074bma.

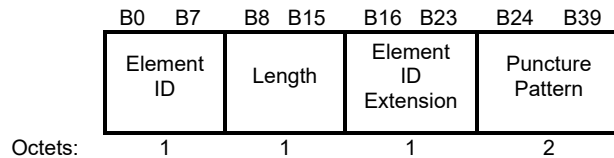


Figure 9-1074bma—Puncture Pattern element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Puncture Pattern field in the Puncture Pattern element has the same format and value as the Disabled Subchannel Bitmap field sent in the EHT Operation element (see 9.4.2.321) as part of the Beacon transmissions.

9.6.7.33 FTM frame format

Change Figure 9-1221 as follows:

<u>Category</u>	<u>Public Action</u>	<u>Dialog Token</u>	<u>Follow Up Dialog Token</u>	<u>TOD</u>	<u>TOA</u>				
Octets:	1	1	1	1	6	6			
	TOD Error	TOA Error	LCI Report (optional)	Location Civic Report (optional)	FTM Parameters (optional)		FTM Synchronization Information (optional)		
Octets:	2	2	variable	variable	variable	variable			
	Ranging Parameters (optional)	Secure HE-LTF Parameters (optional)	Channel Measurement Feedback Type (optional)	Channel Measurement Feedback (optional)	Direction Measurement Results (optional)	Multiple Best AWP ID (optional)	Multiple AOD Feedback (optional)	LOS Likelihood (optional)	<u>Transmit Power Envelope (optional)</u>
Octets:	variable	14	2	variable	9	variable	variable	4	<u>variable</u>

Figure 9-1221—FTM frame Action field format

Insert the following new paragraph at the end of the 9.6.7.33:

The Transmit Power Envelope field is optionally present. If present, it contains one or more Transmit Power Envelope elements as defined in 9.4.2.160.

9.6.7.49 LMR frame format

Change Figure 9-1237 in 9.6.7.49 as follows:

	<u>Category</u>	<u>Public Action</u>	<u>Dialog Token</u>	<u>TOD</u>	<u>TOA</u>	<u>TOD Error</u>	<u>TOA Error</u>
Octets:	1	1	1	6	6	1	1
	CFO Parameter	R2I NDP Tx PWR	I2R NDP Target RSSI	Secure HE-LTF Parameters (optional)	AOA Feedback (optional)	<u>Transmit Power Envelope (optional)</u>	<u>Puncture Pattern (optional)</u>
Octets:	2	1	1	14	9	<u>variable</u>	<u>5</u>

Figure 9-1237—LMR frame Action field format

Insert the following paragraphs in 9.6.7.49 as follows:

The AOA Feedback field is optionally present. If present, it contains a Direction Measurement Results element as defined in 9.4.2.302.

The Transmit Power Envelope field is optionally present. If present, it contains one or more Transmit Power Envelope elements, as defined in 9.4.2.160.

The Puncture Pattern field is optionally present. If present, it contains a Puncture Pattern element as defined in 9.4.2.331.

11. MLME

Change the following subclauses to Clause 11 as follows:

11.21.6.2 FTM capabilities

A STA in which `dot11SecureLTFImplemented` is true shall set the Secure ~~HE~~-LTF Support field of the RSNXE to 1. Otherwise, it shall set the Secure ~~HE~~-LTF Support field to 0.

11.21.6.3 FTM procedure negotiation

11.21.6.3.1 General

Insert the following paragraphs at the end of 11.21.6.3.1 as follows:

NOTE 3—Prior to the transmission of any ranging frame(s) including IFTM frame (negotiation), FTM frame (measurement), and/or FTM session termination frame sent by an AP to an associated ISTA in the EMLSR mode, the AP transmits an initial control frame exchange (see 35.3.17).

NOTE 4—The transmission of an initial control frame is not required for an unassociated ISTA since only the associated ISTA can negotiate to be in the EMLSR mode.

The RSTA and ISTA shall transmit all frames that are part of the ranging measurement exchange(s) on the specific link that was identified by the Link ID bitmap field of the MLO Link Info element included in the IFTMR and IFTM negotiation frame exchange.

NOTE 5—Exactly one bit in the Link ID Bitmap subfield of the MLO Link Info element is set to 1 (see 35.3.14.3).

11.21.6.3.2 Negotiation for EDCA based ranging measurement exchange

Change 11.21.6.3.2 by adding text between the fifth and sixth paragraphs as follows:

... ..

For EDCA based ranging where the value of the corresponding Format And Bandwidth field value that indicates DMG or EDMG format, see Table 9-325, the ISTA shall indicate, in the Ranging Priority subfield of the FTM Parameters field of the FTM Parameters element in the IFTMR frame, its ranging priority as described in Table 9-323. Otherwise, the Ranging Priority subfield of the FTM Parameters field of the FTM Parameters element is reserved.

An unassociated ISTA that is capable of receiving a Transmit Power Envelope element as part of its FTM procedure shall set its TPE Update Capable subfield in the IFTMR frame to 1. An RSTA that is capable of transmitting a Transmit Power Envelope element as part of the FTM procedure shall respond with an IFTM frame with the TPE Update Capable field set to 1, if the IFTMR frame included a TPE Update Capable subfield set to 1.

An associated ISTA shall set the TPE Update Capable subfield to 0.

An RSTA that sets the TPE Update Capable subfield to 1 shall include at least one Transmit Power Envelope element in the IFTM frame and the first FTM frame of each burst instance of this FTM session. When one or more Transmit Power Envelope elements are included in the FTM frames, the Transmit Power Envelope

elements shall be the same as the ones carried in the Beacon and other management frames transmitted by the RSTA.

When the request was successful:

— The RSTA shall indicate, in the Format And Bandwidth field, a format and bandwidth that it supports. The RSTA should indicate the same format and bandwidth in the Format And Bandwidth field as that requested by the ISTA, if the RSTA supports this. The RSTA shall not assign a value that indicates:

... ..

11.21.6.3.3 Negotiation for TB and non-TB ranging measurement exchange

Change the eighth paragraph of 11.21.6.3.3 as follows:

When a Ranging Parameters element is included in the IFTMR frame, the ISTA shall indicate the following parameters in the Ranging Parameters field:

—

— Maximum number of space-time streams it is capable of receiving in the R2I NDP for 160 MHz bandwidths ~~greater than 80 MHz~~, in the 160 MHz Max R2I STS ~~> 80 MHz~~ subfield.

— Maximum number of space-time streams it is capable of transmitting in the I2R NDP for bandwidths less than or equal to 80 MHz, in the Max I2R STS ≤ 80 MHz subfield.

— Maximum number of space-time streams it is capable of transmitting in the I2R NDP for 160 MHz bandwidths ~~greater than 80 MHz~~, in the 160 MHz Max I2R STS ~~> 80 MHz~~ subfield.

—

Change 11.21.6.3.3 by adding the following text to the end of the eighth paragraph as follows:

— Immediate or delayed feedback capability in the I2R LMR by setting the Immediate I2R Feedback subfield to 1 or 0, respectively.

To request a 320 MHz FTM session, an ISTA shall include a 320 MHz Ranging subelement in the Ranging Parameters element in the IFTMR frame and set the Format And Bandwidth subfield to a value of 5 or less. In the subelement:

— The Max R2I NSS field is set to the maximum number of spatial streams the ISTA is capable of receiving in the R2I NDP for a 320 MHz bandwidth minus 1.

— The Max I2R NSS field is set to the maximum number of spatial streams the ISTA is capable of transmitting in the I2R NDP for a 320 MHz bandwidth minus 1.

— The Puncturing Pattern Support field is set to 1 to indicate support of all puncturing patterns, or it is set to 0 to indicate support of only the subset of puncturing patterns defined in Table 11-14aa.

— The Max R2I Repetition field is set to the maximum number of LTF repetitions it is capable of receiving in the preamble of the R2I NDP for 320 MHz bandwidth minus 1.

— The Max I2R Repetition field is set to the maximum number of LTF repetitions it is capable of transmitting in the preamble of the I2R NDP for 320 MHz bandwidth minus 1.

- The Max R2I LTF Total field is set to indicate the maximum number of LTFs in total it is capable of receiving for 320 MHz bandwidth, including all repetitions, in the R2I NDP.
- The Max I2R LTF Total field is set to indicate the maximum number of LTFs in total it is capable of transmitting for 320 MHz bandwidth, including all repetitions, in the I2R NDP.

... ..

Change 11.21.6.3.3 in paragraph 21 as follows:

When the negotiation is successful for TB ranging and non-TB ranging, the corresponding IFTM frame from the RSTA shall include a Ranging Parameters element with the parameters that define the negotiated range measurement session. The RSTA shall indicate the following parameters in the Ranging Parameters field:

- In the Format And Bandwidth subfield, ~~it assigns~~ the maximum allowed bandwidth used during measurement exchanges (referred to as *RSTA Assigned Max Bandwidth*) is assigned. This value shall not be greater than the value in the corresponding IFTMR frame. If the IFTMR frame included a 320 MHz Ranging subelement, the bandwidth may be assigned as 320 MHz regardless of the Format And Bandwidth subfield value in the IFTMR frame.
-
- In the 160 MHz Max R2I STS \geq 80 MHz subfield, either the maximum number of space-time streams it is capable of transmitting in the R2I NDP for 160 MHz bandwidths ~~greater than 80 MHz~~, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as 160 MHz RSTA Assigned R2I STS \geq 80 MHz).
- In the 160 MHz Max I2R STS \geq 80 MHz subfield, either the maximum number of space-time streams it is capable of receiving in the I2R NDP for 160 MHz bandwidths ~~greater than 80 MHz~~, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as 160 MHz RSTA Assigned I2R STS \geq 80 MHz).
-

If the Format And Bandwidth subfield is set to 8, the RSTA shall include a 320 MHz Ranging subelement in the Ranging Parameters element in the IFTM frame. In the 320 MHz Ranging subelement:

- The Max R2I NSS field is set to either the maximum number of spatial streams it is capable of transmitting in the R2I NDP for 320 MHz bandwidth minus 1, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as *320 MHz RSTA assigned R2I NSS*).
- The Max I2R NSS field is set to either the maximum number of spatial streams it is capable of receiving in the I2R NDP for 320 MHz bandwidth minus 1, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as *320 MHz RSTA assigned I2R NSS*).
- The Puncturing Pattern Support field is set to 1 to indicate support of all puncturing patterns, or it is set to 0 to indicate support of only the subset of puncturing patterns defined in Table 11-14aa.
- If the RSTA has included the Disabled Subchannel Bitmap field in the EHT Operation element, the Puncturing Pattern field is set to the same value; otherwise, the Puncturing Pattern field is set to all zeros, representing no puncturing.

- In the Max R2I Repetition field, it assigns the maximum number of LTF repetitions in the preamble of the R2I NDP for this session (referred to as 320 MHz RSTA assigned R2I Rep). This value shall not be greater than the value in the corresponding IFTMR frame.
- In the Max I2R Repetition field, it assigns the maximum number of LTF repetitions in the preamble of the I2R NDP for this session (referred to as 320 MHz RSTA assigned I2R Rep). This value shall not be greater than the value in the corresponding IFTMR frame.
- In the Max R2I LTF Total field, either the maximum number of LTFs in total it is capable of transmitting to this ISTA, including LTF repetitions, in the R2I NDP, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as 320 MHz RSTA assigned R2I LTF Total).
- In the Max I2R LTF Total field, either the maximum number of LTFs in total it is capable of receiving, including LTF repetitions, in the I2R NDP, or the value in the corresponding IFTMR frame, whichever is smaller (referred to as 320 MHz RSTA assigned I2R LTF Total).

If the RSTA is an EHT AP that has included the Disabled Subchannel Bitmap field in the EHT Operation element, and the ISTA has set the Puncturing Pattern Support field in the 320 MHz Ranging subelement of the IFTMR frame to 0, the RSTA shall not assign a 320 MHz bandwidth unless the Disabled Subchannel Bitmap field in the EHT Operation element corresponds to one of the entries of Table 11-14aa.

Table 11-14aa—Subset of puncturing patterns in 320 MHz Ranging when Puncturing Pattern Support field set to 0

<u>Disabled Subchannel Bitmap field value</u>	<u>Corresponding entry for the 320 MHz bandwidth in Table 36-30</u>	
	<u>Field value</u>	<u>Puncturing pattern (RU or MRU index)</u>
[1111 0000 0000 0000]	9	[x x 1 1 1 1 1 1] (3x996-tone MRU 1)
[0000 0000 0000 1111]	12	[1 1 1 1 1 1 x x] (3x996-tone MRU 4)

If an RSTA has an ongoing 320 MHz FTM session and is including the Disabled Subchannel Bitmap field in the EHT Operation element (9.4.2.321) as part of the Beacon frame transmissions, the RSTA shall also include the Puncture Pattern field in any LMR frame sent to an unassociated ISTA.

Upon the reception of a new puncture pattern, an unassociated ISTA shall either:

- Receive Beacon frames from the RSTA to learn the switching time and activate the new puncture pattern before performing ranging measurement exchange(s) with the new puncture pattern.
- Terminate the FTM session if it is not able to support the new puncture pattern.

Once the new puncture pattern takes effect, the RSTA and ISTA shall use the new puncture pattern to perform ranging measurement exchanges.

...

Change 11.21.6.3.3 in paragraph 28 as follows:

Upon reception of an IFTMR frame with the Format And Bandwidth subfield set to a value of 3, 4, or 5 representing the ISTA’s support for one of the 160 MHz ~~BW~~ bandwidth options, the RSTA shall respond with the same requested value in the Format And Bandwidth subfield in the IFTM frame, if it supports the requested 160 MHz ~~BW~~ bandwidth option; otherwise, respond with a value less than 3. Upon reception of an IFTMR frame with the Ranging Parameters element including a 320 MHz Ranging subelement the RSTA

shall respond with the value of 8 in the Format And Bandwidth subfield in the Ranging Parameters element and include a 320 MHz Ranging subelement in the IFTM frame, if it supports the requested 320 MHz bandwidth with the corresponding puncturing pattern included in the Disabled Subchannel Bitmap field in the EHT Operation element.

... ..

Insert the following new paragraphs at the end of 11.21.6.3.3:

An unassociated ISTA that is capable of receiving a Transmit Power Envelope element as part of its FTM procedure shall set its TPE Update Capable subfield in the IFTMR frame to 1. An RSTA that is capable of transmitting a Transmit Power Envelope element as part of the FTM procedure shall respond with an IFTM frame with the TPE Update Capable field set to 1, if the IFTMR frame included a TPE Update Capable subfield set to 1.

An associated ISTA shall set the TPE Update Capable subfield to 0.

An RSTA that sets the TPE Update Capable subfield to 1 shall include at least one Transmit Power Envelope element in the IFTM frame, and all LMR frames of the FTM session. When one or more Transmit Power Envelope elements are included in the IFTM or LMR frames, the Transmit Power Envelope elements shall be the same as the ones carried in the Beacon and other management frames transmitted by the RSTA.

Change 11.21.6.3.4 as follows:

11.21.6.3.4 Negotiation for secure ~~HE~~-LTF in the TB and non-TB ranging measurement exchange

An ISTA and an RSTA may activate a secure ~~HE~~-LTF measurement exchange for non-TB ranging or TB ranging that uses randomized LTF sequences in the I2R NDPs and R2I NDPs, refer to 11.21.6.4.5.

An RSTA in which dot11SecureLTFImplemented is true shall set the Secure ~~HE~~-LTF Support field in the RSNXE to 1. An ISTA in which dot11SecureLTFImplemented is true shall include the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in an IFTMR frame.

When an RSTA has set the Secure ~~HE~~-LTF Support field to 1 in the RSNXE, then to request a secure ~~HE~~-LTF measurement exchange mode with the RSTA, an ISTA with dot11SecureLTFImplemented equal to true shall include the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in the IFTMR frame and set the Secure ~~HE~~-LTF Required field in the Secure ~~HE~~-LTF subelement to 1.

When an ISTA has included the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in its IFTMR frame and set the Secure ~~HE~~-LTF Required field to 1, then the RSTA that has set the Status Indication field to 1 (i.e., Successful) shall include the Secure ~~HE~~-LTF subelement in the Ranging Parameter element in its IFTM frame and set the Secure ~~HE~~-LTF Required field to 1 to assign a secure ~~HE~~-LTF measurement exchange mode with the ISTA.

When an ISTA has included the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in an IFTMR frame, then to assign a secure ~~HE~~-LTF measurement exchange mode with the ISTA, an RSTA with dot11SecureLTFImplemented equal to true shall include a Secure ~~HE~~-LTF subelement in the Ranging Parameters element in an IFTM and set its Secure ~~HE~~-LTF Required field to 1.

When an ISTA has included the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in its IFTMR frame and set the Secure ~~HE~~-LTF Required field to 1, the ISTA shall set the Max R2I Repetition and Max I2R Repetition subfields to a value greater than 0.

When an RSTA assigns a secure ~~HE~~-LTF measurement exchange by including a Secure ~~HE~~-LTF subelement in the Ranging Parameters element in its IFTM frame and setting the Secure ~~HE~~-LTF Required subfield to 1, the RSTA shall set the *RSTA Assigned R2I Rep* to the Max R2I Repetition subfield value in the IFTMR frame ~~which that~~ shall be greater than 0, and the RSTA shall set *RSTA Assigned I2R Rep* to a value greater than 0 and less than or equal to the Max I2R Repetition subfield value in the IFTMR frame, where the *RSTA Assigned R2I Rep* and *RSTA Assigned I2R Rep* specify the number of ~~HE~~-LTF repetitions in the preamble of the R2I and I2R NDP for this session, respectively. Similarly, if the RSTA has included a 320 MHz Ranging subelement together with the Ranging Parameters element in the IFTM frame, the RSTA shall set the 320 MHz *RSTA Assigned R2I Rep* and 320 MHz *RSTA Assigned I2R Rep* to values greater than 0.

When an ISTA has included the Secure ~~HE~~-LTF subelement in the Ranging Parameters element in the IFTMR frame, it shall indicate to the RSTA a request to use the optional frequency domain Tx window in the R2I NDPs by setting the R2I Tx Window field to 1, otherwise shall set it to 0; and indicate its support of the optional frequency domain Tx window in the I2R NDPs by setting the I2R Tx Window field to 1, otherwise shall set it to 0.

When an RSTA has assigned a secure ~~HE~~-LTF measurement exchange mode, by including a Secure ~~HE~~-LTF subelement in the Ranging Parameters element in the IFTM frame, and setting its Secure ~~HE~~-LTF Required field to 1, the RSTA shall also include a Secure ~~HE~~-LTF Parameters element in the IFTM frame that contains the values of the Validation SAC and Secure ~~HE~~-LTF Counter subfields.

The secure LTF negotiation supports negotiation of the secure ~~HE~~-LTF protocol version⁷ (see Table 9-415), which allows an RSTA and ISTA to negotiate the highest mutually supported secure ~~HE~~-LTF protocol version. The secure ~~HE~~-LTF protocol version is indicated in the Protocol Version field within the Secure ~~HE~~-LTF subelement. If an RSTA includes a Secure ~~HE~~-LTF element in the IFTM frame, it shall set the Protocol Version subfield to either the same or a lower value than the ISTA's Secure Protocol Version sent in the IFTMR frame with the Status Indication subfield equal to 1 (i.e., Success), or a higher value than the ISTA's Secure Protocol Version with the Status Indication subfield equal to 2 (i.e., "Request incapable. Do not send same request again."²). Upon receiving an IFTM frame with Status Indication subfield set to 1 (i.e., successful) that includes a Secure ~~HE~~-LTF subelement, the ISTA shall either proceed with the RSTA's Protocol Version assignment, or if it does not meet its required security level, shall terminate by transmitting an FTMR frame with trigger field set to 0.

11.21.6.4 Measurement exchange

Change 11.21.6.4.3 as follows:

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).

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 **P**olling, **M**measurement **S**sounding and **M**measurement **R**eporting phases, as well as signaling of modification of availability window parameters; (see 11.21.6.5.1); and TB ranging session termination; (see 11.21.6.6.2). 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 and 11.21.6.4.3.3). Each availability window of the TB ranging measurement exchange consists of one or more triplets of sequential phases: **P**olling phase, **M**measurement **S**sounding phase and **M**measurement **R**eporting phase. Figure 11-48 shows an example of two availability windows, each composed of a single triplet of **P**olling, **M**measurement **S**sounding and **M**measurement **R**eporting phases. An RSTA and ISTA participating in TB ranging shall perform any **P**olling, **M**measurement **S**sounding, and **M**measurement **R**eporting phases only within the availability windows.

Replace Figure 11-48 with the following figure:

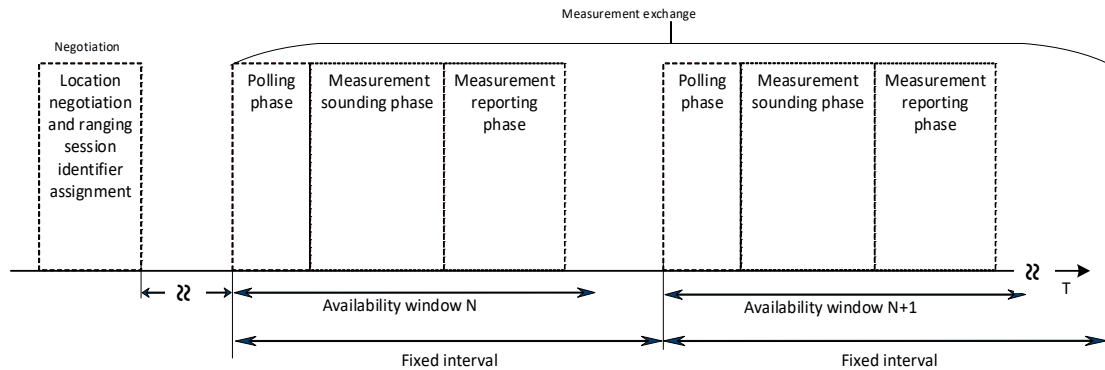


Figure 11-48—TB ranging availability windows, each with one instance of a polling/sounding/reporting triplet

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 11-49 and Figure 11-50). 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 and 11.21.6.4.3.4. 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).

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 1—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_x 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.

NOTE 2—For an HE MU PPDU or an EHT MU PPDU addressed to an unassociated ISTA, the STA_ID parameter in the TXVECTOR of the PPDU is set to the RSID (to be used in the preamble).

For a Ranging Trigger frame or an NDP Announcement frame transmitted in an HE PPDU or an EHT PPDU, the BSS_COLOR parameter of the PPDU shall be set to the value indicated in the BSS Color Information field of the Ranging Parameters element transmitted by the RSTA.

For any R2I LMR frame or I2R LMR frame (if negotiated) transmitted between an RSTA and an unassociated ISTA, the BSS_COLOR parameter of the PPDU shall be set to 0 or the value indicated in the BSS Color Information field of the Ranging Parameters element transmitted by the RSTA.

An RSTA shall follow the rules defined in 26.5.2 or 35.5.2 when transmitting any Ranging Trigger frames. ~~of variant Location for TB ranging with the following rules:~~

Additionally, when transmitting the following frames:

- 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, or EHT PPDU.
- An RSTA shall not transmit a Ranging Trigger frame nor a Ranging NDP Announcement frame in a VHT MU PPDU ~~or~~, HE MU PPDU, or EHT MU PPDU that is not an EHT SU transmission.

An RSTA shall not transmit a Sounding Ranging Trigger frame soliciting an HE TB Ranging NDP or an EHT 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 FTMR 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 ~~FF~~ Ranging Trigger frame 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_x 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 26.5.2 or 35.5.2 when transmitting any HE TB PPDUs or EHT TB PPDUs, respectively, for TB ranging with the exceptions defined in 11.21.6.4.3.2, 11.21.6.4.3.3_x, and 11.21.6.4.3.4.

Replace Figure 11-49 with the following figure:

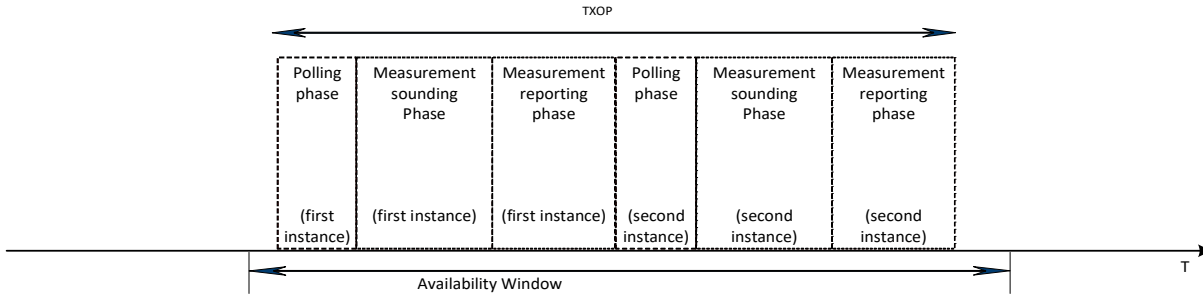


Figure 11-49—TB ranging availability window with two instances of polling/sounding/reporting triplets within a single TXOP

Replace Figure 11-50 with the following figure:

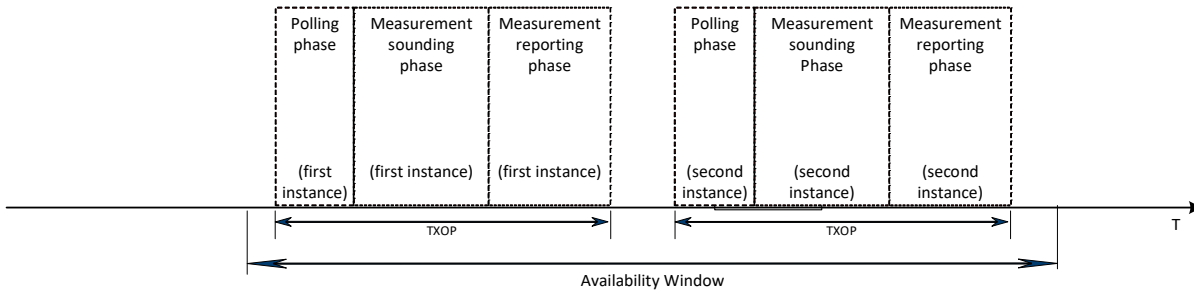


Figure 11-50—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs

Insert the paragraphs and figures at the end of 11.21.6.4.3.1 as follows:

To perform a TB ranging measurement exchange with an associated ISTA in the EMLSR mode, the RSTA shall transmit an initial control frame exchange (see 35.3.17) at the beginning of the TB ranging measurement exchange prior to the transmission of each triplet, which includes polling, measurement sounding and measurement reporting phases; see Figure 11-50a and Figure 11-50b.

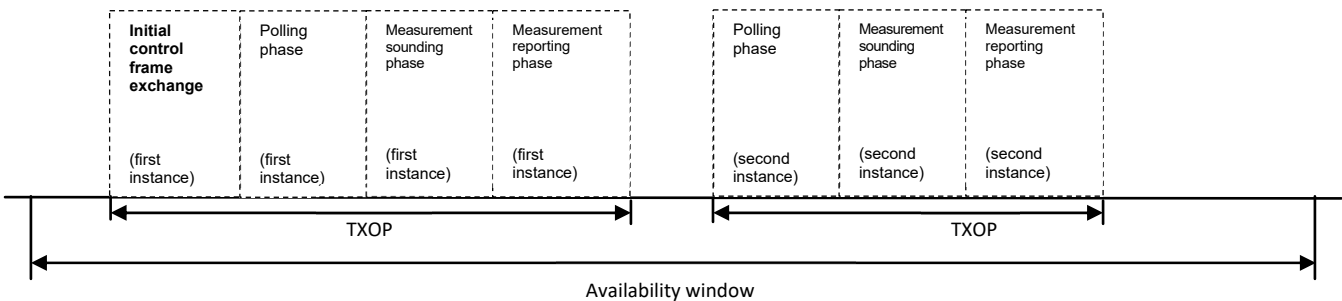


Figure 11-50a—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs where only the first TXOP includes an ISTA in EMLSR mode

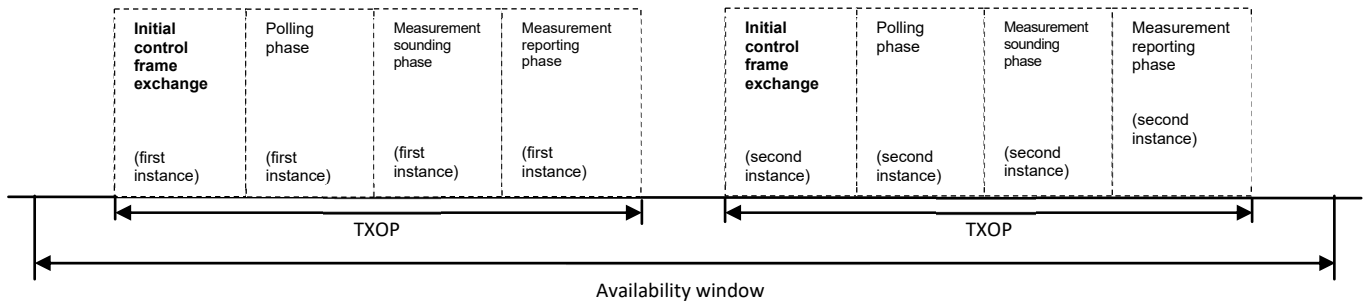


Figure 11-50b—TB ranging availability window with two instances of polling/sounding/reporting triplets in separate TXOPs where each TXOP includes an ISTA in EMLSR mode

To perform a TB ranging measurement exchange with any combination of two or more ISTAs, where at least one ISTA is in the EMLSR mode, the AP shall transmit an initial control frame exchange (see 35.3.17) at the beginning of the TB ranging measurement exchange prior to the transmission of each triplet, and the measurement sounding phase shall not include more than a single Sounding Ranging Trigger frame to avoid the ISTA(s) in the EMLSR mode switching back to the listening operation before the triplets ends.

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, and no more than one ~~in~~ which it receives a response from at least one ISTA; The Ranging variant Trigger frame of poll is called the ~~TF Ranging Poll frame~~ Poll Ranging Trigger frame. The RSTA shall allocate each RU in the ~~TF Ranging Poll frame~~ Poll Ranging Trigger frame to only one ISTA. Any ISTA addressed by a User Info field in a ~~TF Ranging Poll frame~~ Poll Ranging Trigger 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~~ TB PPDU in its designated RU allocation as identified in the ~~TF Ranging Poll frame~~ Poll Ranging Trigger frame, otherwise shall not send a CTS-to-self to avoid resource allocation in this measurement sequence; see Figure 11-50.

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~~ Poll Ranging Trigger 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~~ Poll Ranging Trigger frame, and in ~~TFs Ranging Trigger frames~~ subsequent Ppolling, Mmeasurement Ssounding and Mmeasurement Rreporting 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 Ranging Trigger frame~~ frame, 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 11-49; or a new TXOP, see example in Figure 11-50 depending on the maximum allowed TXOP duration and the predicted length of the extra instances of polling/sounding/reporting triplets.

Replace Figure 11-52 with the following figure:

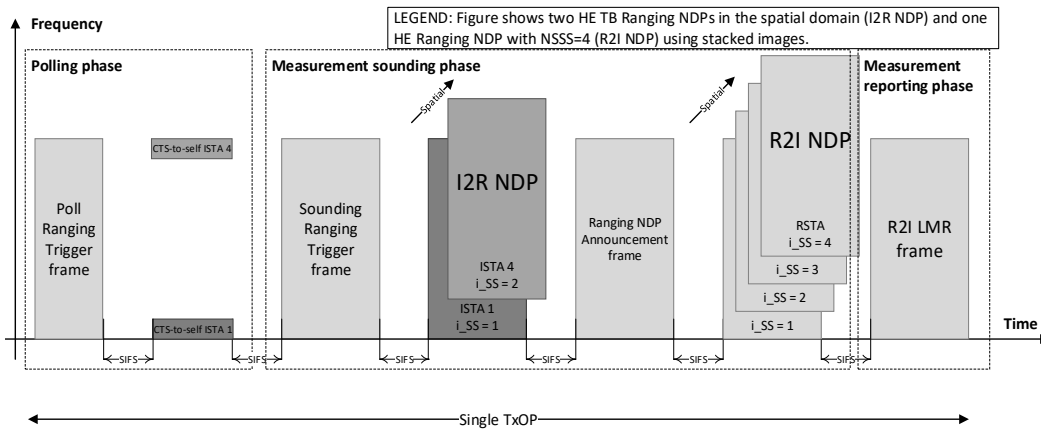


Figure 11-52—TB ranging availability window with two ISTAs

11.21.6.4.3.3 Measurement Sounding phase of TB ranging

Change 11.21.6.4.3.3 as follows (renumbering subsequent NOTES as necessary):

The measurement sounding phase commences a SIFS time after the Polling phase and is the second phase of each polling/sounding/reporting triplet; see Figure 11-52. The measurement sounding phase consists of one or more Sounding Ranging Trigger frames; (see 9.3.1.22.10) allocating uplink resources to one or more ISTAs; (see Figure 11-48 and Figure 11-50). The Ranging variant Trigger frame of sounding subvariant is called the TF Ranging Sounding frame Sounding Ranging Trigger frame. Each TF Ranging Sounding frame Sounding Ranging Trigger 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 27.3.19.2) or an EHT TB Ranging NDP (see 36.3.4.2). A 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 and the R2I NDP is an HE Ranging NDP; as described in 27.3.19.1, or an EHT Ranging NDP as described in 36.3.4.1. Figure 11-52 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. The STA Info field(s) in the NDP Announcement frame shall be directed to the same ISTA(s) that were allocated uplink resources in the measurement sounding phase, which makes use of the R2I NDP.~~

NOTE 1—A 320 MHz bandwidth of the Ranging NDP Announcement frame is indicated based on rules in 17.3.5.2 if the frame is transmitted in a non-HT duplicate PPDU, or based on rules in Table 36-28 if the frame is transmitted in an EHT MU PPDU.

The RSTA shall select a sounding 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.

If the sounding bandwidth is 320 MHz the Sounding Ranging Trigger frame(s) in the measurement sounding phase shall solicit an EHT TB Ranging NDP. Otherwise, the Sounding Ranging Trigger frame(s) shall solicit HE TB Ranging NDPs.

The RSTA shall set the TXVECTOR parameter CH_BANDWIDTH of the ~~Trigger frame~~ Sounding Ranging Trigger frame to ~~that same the sounding bandwidth~~, and shall use the same value for the UL BW subfield of the Common Info field of said ~~Trigger frame~~. If the sounding bandwidth is 320 MHz, the RSTA shall include a Special User Info field and set the UL Bandwidth Extension field accordingly. When transmitting the Ranging NDP Announcement frame and R2I NDP, the RSTA shall set the TXVECTOR parameter CH_BANDWIDTH to that same bandwidth value.

In the ~~TF Ranging Sounding~~ Sounding Ranging Trigger frame, the RSTA shall set the SS Allocation subfield and the I2R Rep subfield of the User Info fields corresponding to each of the ~~triggered~~ ISTAs ~~triggered by the Trigger frame~~ in the following ways:

- The Number ~~o~~f Spatial Streams in each SS Allocation subfield shall not exceed the assigned value ~~RSTA Assigned I2R STS \leq 80 MHz for the corresponding sounding bandwidth ISTA; i.e., if the UL BW subfield in the Common Info field indicated a sounding bandwidth is less than or equal to 80 MHz, the RSTA assigned I2R STS \leq 80 MHz, if the sounding bandwidth is 160 MHz, and not exceed the 160 MHz RSTA Assigned I2R STS $>$ 80 MHz for the corresponding ISTA otherwise, and if the sounding bandwidth is 320 MHz, the 320 MHz RSTA assigned I2R NSS.~~
- All the I2R Rep subfields in the User Info fields of the ~~TF Ranging Sounding~~ Sounding Ranging Trigger frame shall be set to the same value. This value indicates the number of LTF repetitions in the I2R NDP preamble and shall not exceed the assigned value of any of the ~~RSTA Assigned I2R Rep corresponding to the triggered ISTA triggered by this Trigger frame; i.e., the RSTA assigned I2R rep if the sounding bandwidth is less than 320 MHz or the 320 MHz RSTA assigned I2R rep otherwise.~~
- 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 or the Number Of HE/EHT-LTF Symbols subfield in the Common Info field, shall not exceed the assigned value ~~RSTA Assigned I2R LTF Total for any of the triggered ISTA triggered by this Trigger frame; i.e., the RSTA assigned I2R LTF Total if the sounding bandwidth is less than 320 MHz or the 320 MHz RSTA assigned I2R LTF Total otherwise.~~

The RSTA shall set the UL Spatial Reuse subfield to PSR_AND_NON_SRG_OBSS_PD_PROHIBITED in the EHT variant Common Info field of the Sounding Ranging Trigger frame, and the RSTA should set it to the same value in the HE variant Common Info field.

NOTE 2—Setting the UL Spatial Reuse subfield in the HE variant Common Info field to PSR_AND_NON_SRG_OBSS_PD_PROHIBITED matches the setting in the preamble of the HE TB Ranging NDP.

After transmission of the ~~TF Ranging Sounding~~ Sounding Ranging Trigger frame, 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.
- 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~~ 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 as follows: ~~in the following way~~

- The R2I NSTS subfield value shall not exceed the assigned value ~~RSTA assigned R2I STS \leq 80 MHz for the corresponding~~ for each ISTA; i.e., the RSTA assigned R2I STS \leq 80 MHz ~~if the TXVECTOR~~

~~parameter CH_BANDWIDTH for this Ranging NDP Announcement frame if the sounding bandwidth is less than or equal to 80 MHz, the and not exceed 160 MHz RSTA assigned R2I STS > 80 MHz for the corresponding ISTA otherwise if the sounding bandwidth is equal to 160 MHz, and the 320 MHz RSTA assigned R2I NSS otherwise.~~

- The number of LTF repetitions in the R2I Rep subfield shall ~~be set to a value not to exceed the assigned value~~ *RSTA Assigned R2I Rep*, for the corresponding each ISTA; i.e., *the RSTA assigned R2I rep* if the sounding bandwidth is less than 320 MHz and the 320 MHz RSTA assigned R2I rep otherwise.
- 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 assigned value for each corresponding ISTA; i.e., *the RSTA Assigned R2I LTF Total* if the sounding bandwidth is less than 320 MHz and the 320 MHz RSTA assigned R2I LTF Total otherwise 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.
- 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 a SIFS after the Ranging NDP Announcement frame; if the sounding bandwidth is equal to 320 MHz, the R2I NDP shall be formatted as an EHT Ranging NDP, as described in 36.3.4.1; otherwise, the R2I NDP shall be formatted as an HE Ranging NDP, as described in 27.3.19.1.

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 11-49 and Figure 11-50). 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.

When a TXOP includes both a TB ranging measurement exchange soliciting EHT frames of 320 MHz bandwidth and a TB ranging measurement exchange soliciting HE frames of less than 320 MHz bandwidth, then the RSTA shall send all Ranging Trigger frames in non-HT duplicate PPDU.

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 11-53. 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).

Replace Figure 11-53 with the following figure:

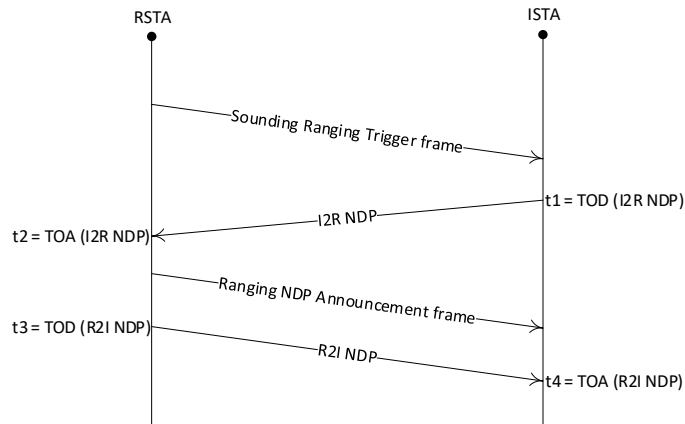


Figure 11-53—Timing diagram of a measurement sounding phase in TB ranging

The Round-Trip Time (RTT_ISTA) observed by ISTA is defined as:

$$\text{RTT}_{\text{ISTA}} = [(t4 - t1) - (t3' - t2')]$$

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 frame; (see 11.21.6.4.3.4) is implementation dependent.

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

$$\text{RTT}_{\text{RSTA}} = [(t4' - t1') - (t3 - t2)]$$

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 frame is implementation dependent; see 11.21.6.4.3.4.

NOTE 34—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 frame.

NOTE 42—Refer to 27.3.15.3 for carrier frequency offset (CFO) correction requirement for HE TB PPDU transmission.

In an LMR frame, 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~~ Sounding Ranging Trigger frame, see Figure 11-54, 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 11-55.

Replace Figure 11-54 with the following figure:

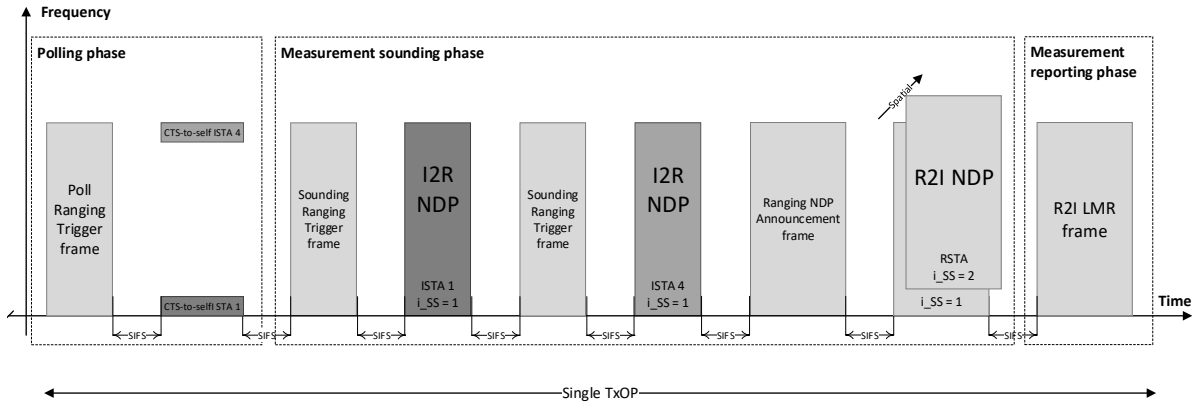


Figure 11-54—TB ranging availability window with multiple TF Ranging Sounding frames
Sounding Ranging Trigger frames

Replace Figure 11-55 with the following figure:

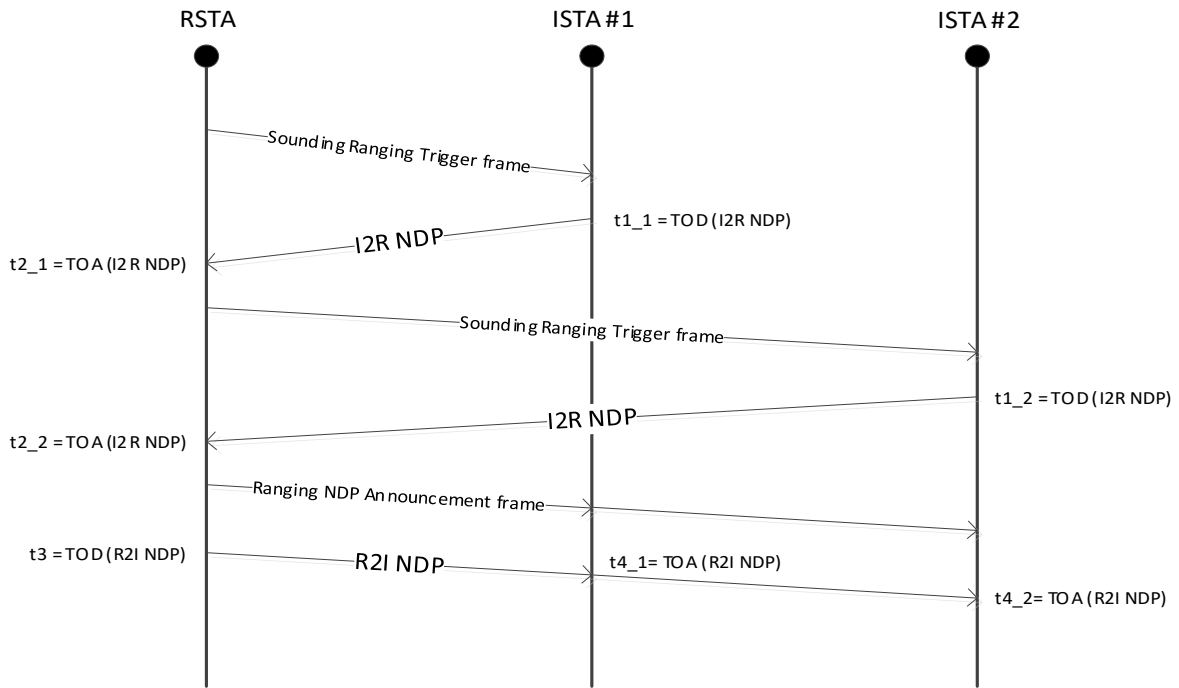


Figure 11-55—Measurement sounding phase with I2R time-division multiplexing

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

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~~Poll Ranging Trigger frame, 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~~Poll Ranging Trigger frame. 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 frame~~Poll Ranging Trigger frame whose partial TSF time is carried in the Ranging NDP Announcement frame.

NOTE 53—An ISTA that tries to synchronize to the RSTA's TSF time ~~will need~~s 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~~Ranging Trigger frame was larger than the received Partial TSF and the absolute difference is more than 2^{15} , then the ISTA should increase the RSTA's tracked TSF[63:22] value by 1.
- If the ISTA's TSF[21:6] at the reception of the ~~TF Ranging Poll~~Ranging Trigger frame is less than the Partial TSF and the absolute difference is more than 2^{15} , the ISTA should decrease the RSTA's tracked TSF[63:22] value by 1.

11.21.6.4.3.4 Measurement Reporting phase of TB ranging measurement

Change 11.21.6.4.3.4 as follows (renumbering subsequent NOTES as necessary):

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 11-50. The measurement results shall be carried in LMR frames; see 9.6.7.49. LMR frames shall carry measurement results from the RSTA to the ISTA, and if negotiated also from the ISTA to the RSTA; see Figure 11-56. If the Range Reporting is performed in the context of a ~~Secure FTM S~~session, see ~~11.21.6.3 (FTM procedure negotiation)~~, the corresponding LMR and FTM; see ~~11.21.6.5.1 (Availability Window parameter modification)~~; frames shall be transmitted using Protected Fine Timing Action frames, ~~and~~ see 9.6.34.

NOTE 1—For the definition of secure FTM session, see 11.21.6.3.1.

The feedback type of the I2R and R2I LMR frames 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~~Poll Ranging Trigger 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).

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 ~~S~~sounding phase from which the reported TOA and TOD values were measured; see 11.21.6.4.3.3.

NOTE 21—LMR feedback is carried in Action No-Ack frames and is therefore neither acknowledged nor retransmitted; see 9.6.7.49.

The RSTA shall transmit an R2I LMR frame 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, 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 sounding bandwidth selected in the measurement sounding phase is equal to 320 MHz and the Sounding Ranging Trigger frame(s) solicit EHT TB Ranging NDP(s), the corresponding R2I LMR frame(s) shall be transmitted in an EHT MU PPDU. Otherwise, the R2I LMR frame shall be transmitted in an HE MU PPDU or an HE SU PPDU. If there is more than one R2I LMR, all the R2I LMR frames shall be carried in one HE MU PPDU or one EHT MU PPDU, where each RU contains a single user.~~

NOTE 3—If there is only one R2I LMR, the PPDU carrying the R2I LMR is using one of the following formats: HE SU, HE MU, or EHT MU (using EHT SU transmission).

If the 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. ~~The Ranging variant Trigger frame of report subvariant is called the TF Ranging LMR.~~

If the sounding bandwidth selected in the measurement sounding phase is equal to 320 MHz and the Sounding Ranging Trigger frame(s) solicit EHT TB Ranging NDP(s), the corresponding Report Ranging Trigger frame shall solicit an EHT TB PPDU. Otherwise, the Report Ranging Trigger frame shall solicit an HE TB PPDU.

A TB ranging measurement reporting phase, including the optional I2R LMR frame, is illustrated in Figure 11-56. If the I2R LMR was negotiated by one or more ISTAs, then ~~a SIFS time~~ after transmitting out the R2I LMR frame, the RSTA transmits a Report Ranging Trigger frame to solicit the I2R LMR frame(s). This ~~TF~~Report Ranging Trigger frame shall allocate uplink resources to ISTAs that negotiated an I2R LMR and were allocated resources in the preceding measurement sounding phase. The RSTA shall allocate each RU in the Report Ranging Trigger frame to only one ISTA. In response to the Report Ranging Trigger frame, 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~~ Poll Ranging Trigger 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 frame to 1.

Replace Figure 11-56 with the following figure:

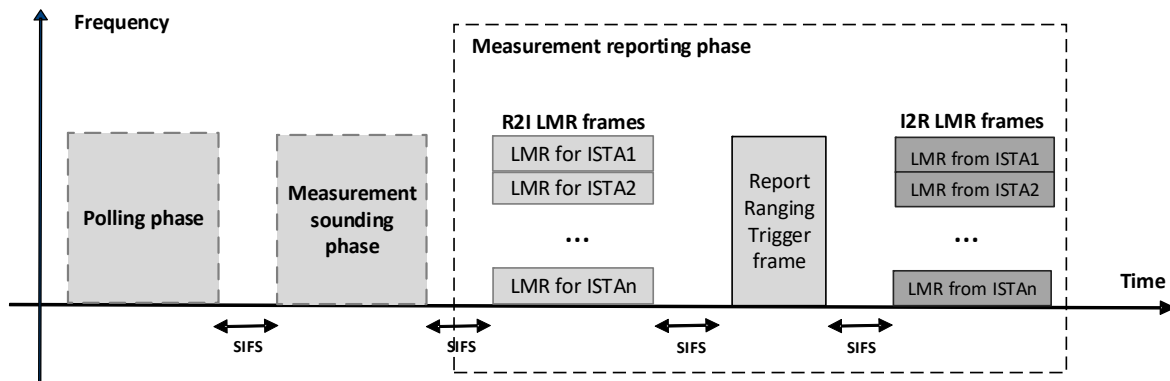


Figure 11-56—TB ranging measurement reporting phase with bidirectional LMR feedback for *n* ISTAs

In TB ranging, the PHY shall issue the PHY-RXEND.indication primitive with error condition IntegrityCheckError, if the PHY detects an 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 an 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 frame carrying the TOA measured from the R2I NDP to 1.

NOTE 42—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 frame; see 9.6.7.49. The ISTA shall estimate the CFO parameter based on the PPDU carrying the ~~TF Ranging Sounding frame~~ Sounding Ranging Trigger 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 frame. 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 frame.

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

In the 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 the 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

Change 11.21.6.4.4 as follows:

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.

An ISTA shall not transmit a Ranging NDP Announcement frame in a VHT MU PPDU, HE MU PPDU, or EHT MU PPDU that is not an EHT SU transmission.

NOTE—For an EHT MU PPDU addressed to an unassociated STA, the STA_ID parameter in the TXVECTOR of the PPDU is set to 2045 (to be used in the preamble).

For an NDP Announcement frame transmitted in an HE PPDU or an EHT PPDU, the BSS COLOR parameter of the PPDU shall be set to the value indicated in the BSS Color Information field of the Ranging Parameters element transmitted by the RSTA.

For any R2I LMR frame or I2R LMR frame (if negotiated) transmitted between an RSTA and an unassociated ISTA, the BSS_COLOR parameter of the PPDU shall be set to 0 or the value indicated in the BSS Color Information field of the Ranging Parameters element transmitted by the RSTA.

...

Replace Figure 11-55 with the following figure:

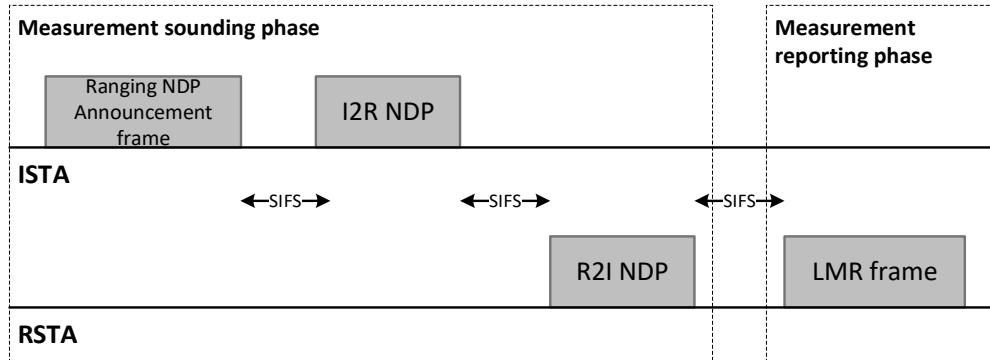


Figure 11-58—Non-TB ranging measurement exchange sequence

11.21.6.4.4.2 Measurement sounding phase of non-TB ranging

Change 11.21.6.4.4.2 as follows:

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 11-58. I2R NDP and R2I NDP, ~~refer to are both either HE Ranging NDPs respectively or EHT Ranging NDPs~~ when dot11NGVOptionImplemented is equal to false and are both NGV Ranging NDPs when dot11NGVOptionImplemented is equal to true. ~~and HE ranging NDPs otherwise.~~ The measurement-reporting phase consists of an LMR frame, which is a Location Measurement Report as defined in 9.6.7.49.

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.

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 11-60. 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, and 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~~ an individually addressed frame 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 ~~NDP~~ 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. If the I2R NDP is transmitted with a 320 MHz bandwidth, the format shall be an EHT Ranging NDP; if the bandwidth is less than 320 MHz and dot11NGVOptionImplemented is equal to false, it shall be an HE Ranging NDP. If dot11NGVOptionImplemented is equal to true, it shall be an NGV Ranging NDP.

The RSTA shall transmit the R2I NDP with the same bandwidth and format as the ~~Ranging I2R NDP Announcement frame~~, while the LMR frame may be transmitted at a different bandwidth, according to the rules of multiple frame transmission in an EDCA TXOP, see 10.23.2.8. The allowed bandwidths for the Ranging NDP Announcements frame, I2R NDP, and R2I NDP shall be less than or equal to 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.~~
- ~~— 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; 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 bandwidth is less than or equal to 80 MHz, the~~ 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 ~~the~~ respective assigned values; i.e., the *RSTA assigned I2R STS* ≤ 80 MHz and *RSTA assigned R2I STS* ≤ 80 MHz, if the bandwidth is less than or equal to 80 MHz, if respectively. If the bandwidth is equal to 160 MHz, if the bandwidth is greater than 80 MHz, the ISTA shall set these same subfields to values not to exceed the 160 MHz *RSTA assigned I2R STS* > 80 MHz and 160 MHz *RSTA assigned R2I STS* > 80 MHz, and if the bandwidth is 320 MHz, the 320 MHz *RSTA assigned I2R NSS* and 320 MHz *RSTA assigned R2I NSS* 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 respective assigned values; i.e., the *RSTA assigned I2R rep* and *RSTA assigned R2I rep* respectively if the bandwidth is less than 320 MHz, and the 320 MHz *RSTA assigned I2R rep* and 320 MHz *RSTA assigned R2I rep* otherwise. 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 corresponding assigned values; i.e., if the bandwidth is less than 320 MHz, the *RSTA assigned I2R LTF Total* and *RSTA assigned R2I LTF Total* and the 320 MHz *RSTA assigned I2R LTF Total* and 320 MHz *RSTA assigned R2I LTF Total* otherwise respectively.

After transmission of the Ranging NDP Announcement frame, 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 0.
- 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 an LTFVECTOR containing the following parameters:

- The SECURE_LTF_FLAG parameter set to 0.
- 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 11-59. 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).

Replace Figure 11-59 with the following figure:

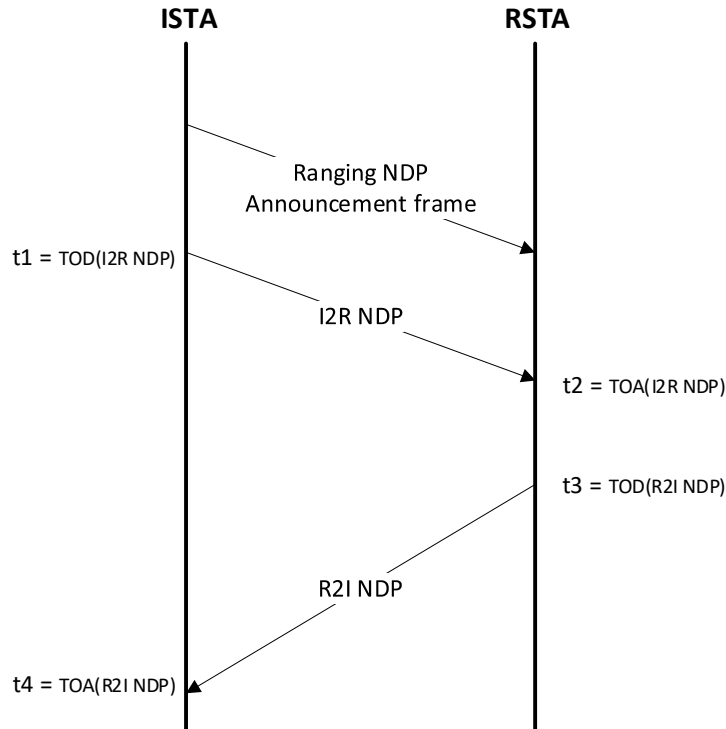


Figure 11-59—Timing diagram of a measurement sounding phase in non-TB ranging

The Round Trip Time (RTT_{ISTA}) based on first path reporting is defined as:

$$RTT_{ISTA} = [(t4 - t1) - (t3' - t2')]$$

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 frame is implementation dependent.

The Round Trip Time (RTT_{RSTA}) based on first path reporting is defined as:

$$RTT_{RSTA} = [(t4' - t1') - (t3 - t2)]$$

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 frame is implementation dependent.

In an LMR frame, 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 Measurement reporting phase of 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 11-60.

Replace Figure 11-60, Figure 11-61, and Figure 11-62 with the following figures and change paragraph text as shown:

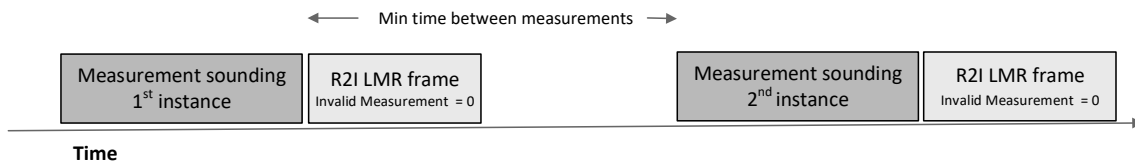


Figure 11-60—Non-TB ranging with immediate reporting

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 frame and the optional I2R LMR frame 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 11-61.

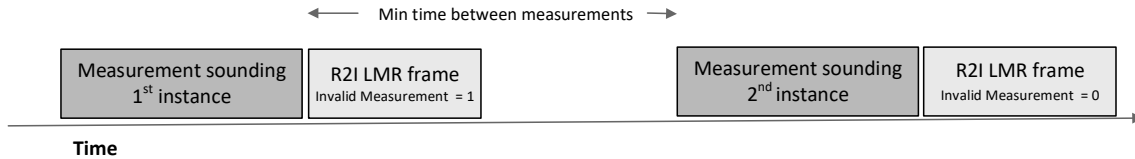


Figure 11-61—Non-TB ranging with delayed reporting

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 11-62. 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.

The Dialog 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 frame 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.

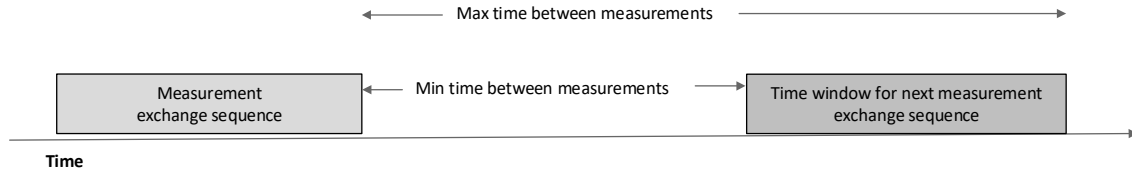


Figure 11-62—Illustration of min time between measurements and max time between measurements with delayed reporting

If I2R LMR feedback is negotiated, the non-TB ranging measurement exchange (11.21.6.4.4) sequence shall follow the sequence shown in Figure 11-63. After a 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 frame could be either immediate or delayed.

NOTE 1—LMR feedback is carried in an Action No-Ack frame and is therefore neither acknowledged nor retransmitted; see 9.6.7.49.

Replace Figure 11-63 with the following figure:

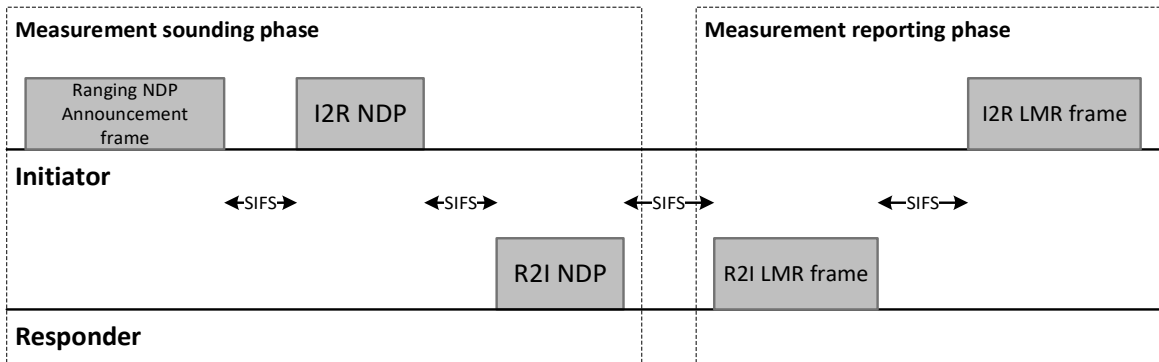


Figure 11-63—Non-TB ranging measurement exchange sequence with bidirectional LMR feedback

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.

If the RSTA included a 320 MHz Ranging subelement in the IFTM frame and set the Format and Bandwidth field to 8 in the Ranging Parameters element, the R2I LMR and I2R LMR frames shall be carried as follows:

- In an HE SU PPDU, if the I2R and R2I NDPs were HE Ranging NDPs.
- In an EHT MU PPDU using EHT SU transmission, if the I2R and R2I NDPs were EHT Ranging NDPs.

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 Ranging NDP~~ HE Ranging NDP or 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 2—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 the 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 t_4 and t_1 are adjusted by the RSTA, and t_2 and t_3 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 frame should discard the TOA carried in the LMR.

In the 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 the 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 9.4.2.303) in the I2R LMR frame. The AOA field contains the Direction Measurement Results element described in 9.4.2.303.

Change identified text from 11.21.6.4.5 through 11.21.6.4.5.2 as follows:

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

11.21.6.4.5.1 General

Both the TB and the non-TB ranging measurement exchanges allow for the use of secure ~~HE~~-LTF for PHY security if the ISTA and RSTA have established a secure HE-LTF measurement setup as defined in 11.21.6.3.4. The frame exchange sequences stay nominally the same as described in 11.21.6.4.3 and 11.21.6.4.4, except that the ~~HE Ranging I2R NDP~~, and ~~HE TB Ranging R2I NDP~~ shall use secure ~~HE~~-LTF as described in 27.3.19.1, ~~and~~ 27.3.19.2, 36.3.4.1, and 36.3.4.2, respectively. To use the secure ~~HE~~-LTF, the ISTA and RSTA need to share and communicate pseudorandom bit sequences that are used to generate and demodulate the secure ~~HE~~-LTF; the details and management thereof are described in 11.21.6.4.5.2 to 11.21.6.4.5.6.

11.21.6.4.5.2 TB ranging measurement exchange with secure ~~HE~~-LTF

An example of the negotiation and two TB Ranging Measurement Exchanges with secure ~~HE~~-LTF is shown in Figure 11-64, where the LTF_VALID_SAC and SEC_LTF_CTR refer to the values of the Validation SAC and Secure ~~HE~~-LTF Counter subfields. The first value of the Validation SAC and its associated Secure ~~HE~~-LTF Counter subfields shall be included in a protected IFTM frame, and thereafter any subsequent value of the Validation SAC and its corresponding Secure ~~HE~~-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 as 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 ~~HE~~-LTF where there are multiple ISTAs involved in the measurement sequence, the RSTA shall transmit a Secure Sounding Ranging Trigger frame that includes a single User Info field to trigger a single ISTA at a time.

NOTE 1—In the TB ranging measurement exchange with secure LTF, the AP always transmits a single Ranging Sounding Trigger frame per ISTA, and hence if the triplet includes an associated ISTA in the EMLSR mode, it cannot include any other additional ISTAs in the same triplet.

Replace Figure 11-64 with the following:

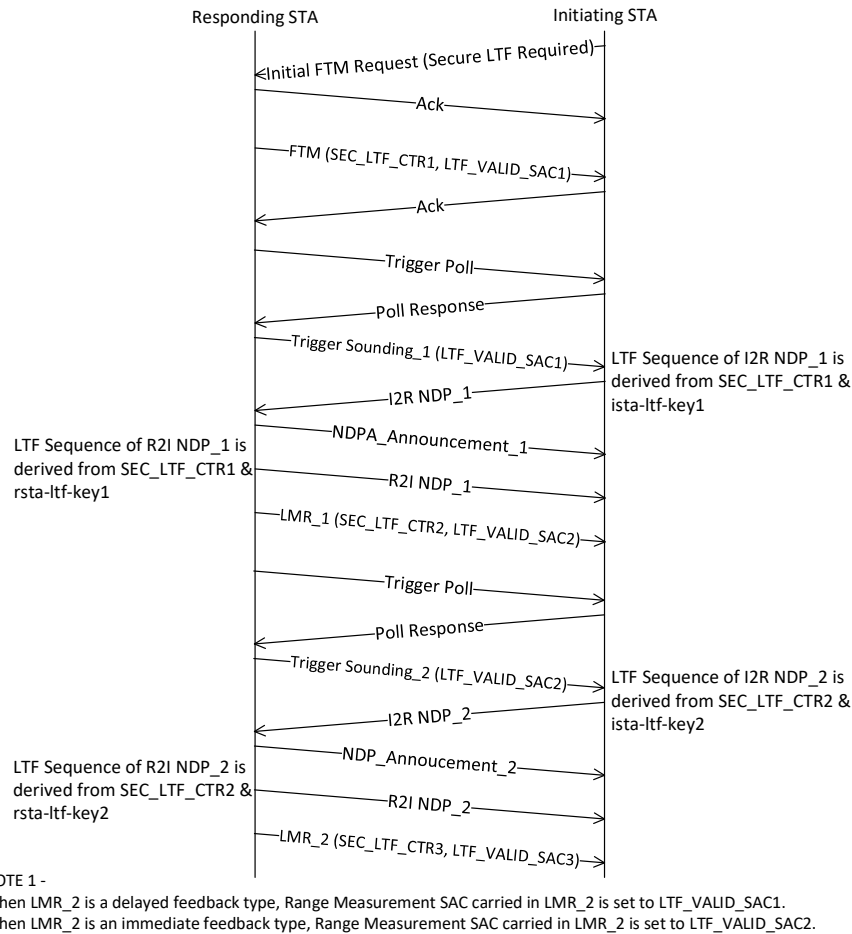


Figure 11-64—Overview of the TB ranging measurement exchange with secure HE-LTF

When an RSTA has established a secure HE-LTF measurement exchange with an ISTA as specified in 11.21.6.3.4, 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 HE-LTF Parameters element in the last transmitted protected IFTM frame, 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 assigned value of the *RSTA Assigned I2R Rep* corresponding bandwidth to the ISTA; i.e., where the value of the RSTA assigned I2R rep, if the bandwidth is less than 320 MHz and the 320 MHz RSTA assigned I2R rep otherwise 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 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, 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*, respectively, for generating the secure ~~HE~~-LTF based on ~~the value of~~ the Secure LTF Counter subfield in the Secure ~~HE~~-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.
- 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 TB Ranging NDP or EHT TB Ranging NDP from the ISTA, the RSTA shall:

- a) Send a Ranging NDP Announcement frame.
- b) Send an HE Ranging NDP or 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~~-LTF based on ~~the value of~~ the Secure ~~HE~~-LTF Counter subfield in the Secure ~~HE~~-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.
- c) Send a protected LMR frame that includes the Secure ~~HE~~-LTF Parameters element to the ISTA.

Otherwise, the RSTA shall follow the rules in 10.23.2.2 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 Equation (11-7) and Equation (11-8).

$$\text{Offset}_i \leq \sum_{k \in \text{MaxOffset}_i} \text{N_LTF}_k \times \text{Rep}_k \quad (11-7)$$

$$\text{Offset}_i \geq \text{Offset}_j + \text{N_LTF}_j \times \text{Rep}_j, \forall j \in \text{MinOffset}_i \quad (11-8)$$

If $\text{Offset}_i = 0$ then $\text{N_STS}_i \geq \text{N_STS}_j, \forall j$

where

Offset_n represents the LTF Offset subfield value of the n^{th} STA Info field in the Ranging NDP Announcement frame.

N_STS_n represents the R2I NSTS subfield value plus 1 of the n^{th} STA Info field in the Ranging NDP Announcement frame.

N_LTF_n represents the number of ~~HE~~-LTF symbols based on N_STS_n , see Table 21-13, for the n^{th} STA Info field in the Ranging NDP Announcement frame.

Rep_n represents the R2I Rep subfield value plus 1 of the n^{th} 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 i^{th} STA Info field in the Ranging NDP Announcement frame.

MaxOffset represents the set of indexes of all STA Info fields excluding i^{th} 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 assigned value of the corresponding bandwidth; i.e., the RSTA assigned R2I rep, if the bandwidth is less than 320 MHz, and the 320 MHz RSTA assigned R2I rep otherwise, 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 ~~HE~~-LTF Parameters element in the last protected IFTM frame, or last protected LMR frame, received from the RSTA, the ISTA shall send an HE TB Ranging NDP or EHT TB Ranging NDP with the TXVECTOR parameters LTF_KEY and LTF_IV that are set to *ista-ltf-key* and *ltf-iv*, respectively, for generating the secure ~~HE~~-LTF based on ~~the value of the~~ Secure LTF Counter subfield in the Secure ~~HE~~-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.

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 ~~HE~~-LTF Parameters element in the last protected IFTM frame or last protected LMR frame received from the RSTA, the ISTA shall send an HE TB Ranging NDP or EHT TB Ranging NDP with the TXVECTOR parameters LTF_KEY and LTF_IV ~~that are~~ set to the *ista-ltf-key* and *ltf-iv*, respectively, for generating ~~any~~ a secure ~~HE~~-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*, respectively, for generating the secure ~~HE~~-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.
- 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 ~~HE~~-LTF Parameters element in the protected LMR frame:

- The Measurement SAC subfield in the Secure ~~HE~~-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 ~~HE~~-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 do not~~ do not 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 I2R NDP and transmitting an R2I NDP results in a Null-SAC-LTF, the RSTA shall not use the TOA and TOD value of the I2R NDP and R2I NDP respectively and shall set the Invalid Measurement Indication subfield to 1 in the TOA error field in the protected LMR frame carrying the TOA value of the I2R NDP. ~~When a frame exchange that consists of receiving an HE TB Ranging NDP and transmitting an HE Ranging NDP results in a Null-SAC HE LTF, the RSTA shall not use the TOA and TOD value of the HE TB Ranging NDP and HE Ranging 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 TB Ranging NDP.~~

When an ISTA receives a Secure Sounding Ranging Trigger frame from an RSTA in which the SAC subfield in the Trigger Dependent User Info field is not equal to the Validation SAC subfield in the Secure ~~HE~~-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 TB Ranging~~ NDP.
- Not use the TOA value of the R2I NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR frame carrying the TOA value of the R2I NDP if the I2R LMR transmission from the ISTA was negotiated. ~~Shall not use the TOA value of the R2I HE Ranging, 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 Ranging NDP if the I2R LMR transmission from the ISTA was negotiated.~~

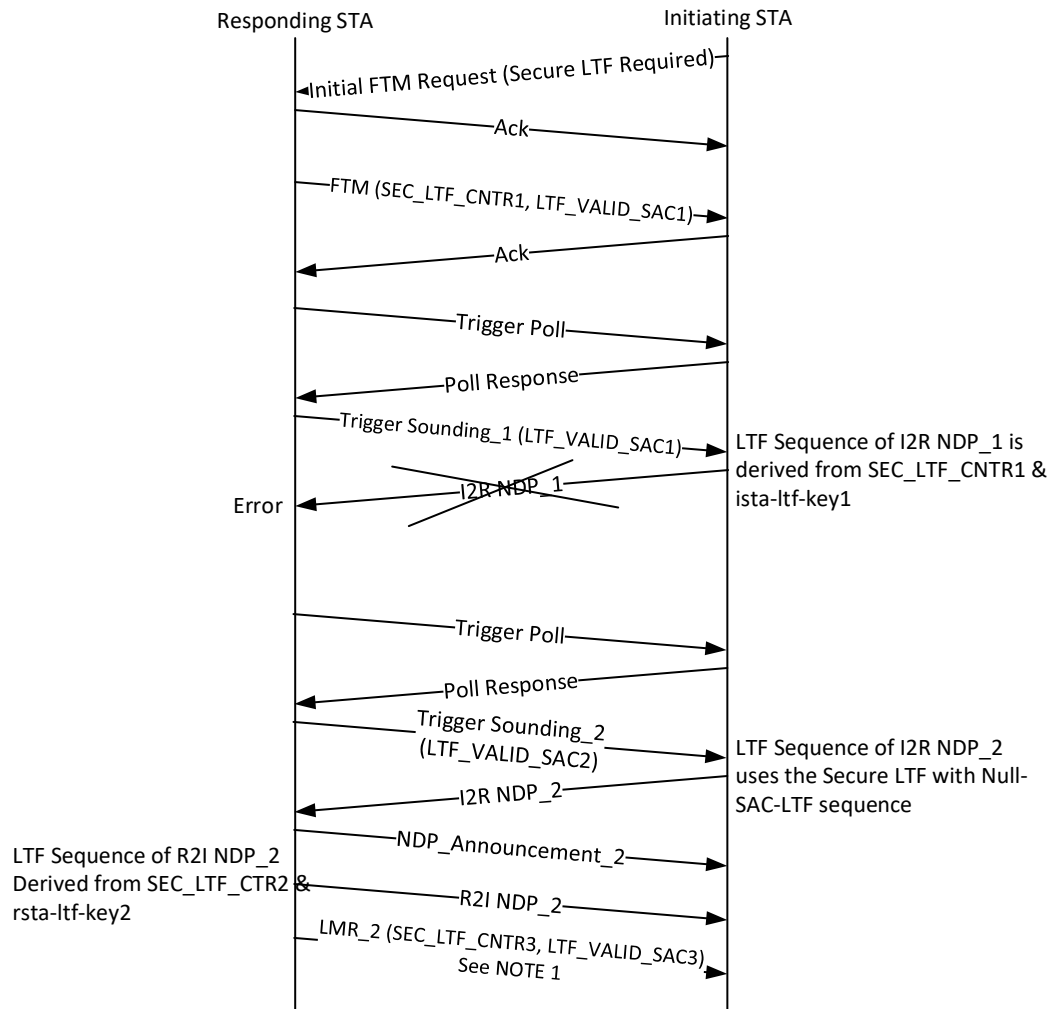
~~The STA shall discard the SAC value used in the frame exchange and shall not use the same SAC value in the current measurement exchange.~~

The STA shall use a new SAC value and its corresponding ista-ltf-key and rsta-ltf-key in every ranging measurement exchange, even if the current ranging measurement exchange is unsuccessful.

NOTE—In TB ranging measurement exchange with secure ~~HE~~-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 11-65.

Change Figure 11-65 by deleting the two occurrences of “HE” and capitalizing “null-” to “Null-” shown as follows:



NOTE 1 -
 Range measurement result carried in LMR_2 is invalid and Range Measurement SAC field carried in LMR_2 is reserved, regardless of whether LMR_2 is a delayed feedback type or an immediate feedback type.

Figure 11-65—Error recovery of TB ranging measurement exchange using secure HE-LTF

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 respective assigned values of the corresponding bandwidth; i.e., the of RSTA assigned I2R rep and the RSTA assigned R2I rep respectively, if the bandwidth is less than 320 MHz, and the 320 MHz RSTA assigned I2R rep and 320 MHz RSTA assigned R2I rep otherwise. ~~corresponding to the RSTA. Both values of the RSTA assigned R2I Rep, and RSTA Assigned I2R Rep, shall be greater 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-~~HE~~-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~~-LTF based on the Secure ~~HE~~-LTF Counter subfield in the Secure ~~HE~~-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.

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-~~HE~~-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*, respectively, for generating a secure ~~HE~~-LTF based on the values of the Secure ~~HE~~-LTF Counter subfield in the Secure ~~HE~~-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.
- 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.
- 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 Validation SAC subfield in the Secure ~~HE~~-LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall confirm reception of an I2R NDP a SIFS after the Ranging NDP Announcement frame, then:

- Send an R2I NDP to the ISTA with the TXVECTOR parameters *rsta-ltf-key* and *ltf-iv* for generating a secure LTF. ~~Send an HE Ranging NDP to the ISTA with the TXVECTOR parameters *rsta ltf key* and *ltf iv* for generating any secure HE LTF to the ISTA, only if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the Ranging NDP Announcement frame.~~
- Send a protected LMR frame with a Secure ~~HE~~-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 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 SAC subfield in the STA Info field with AID11 equal to 2043 is equal to the Validation SAC subfield in the Secure ~~HE~~-LTF Parameters element in the last transmitted protected IFTM frame or last transmitted protected LMR frame to the ISTA, the RSTA shall confirm reception of an I2R NDP a SIFS after the Ranging NDP Announcement frame, then:

- Send an ~~HE Ranging R2I~~ NDP with the TXVECTOR parameters *rsta-ltf-key* and *ltf-iv* for generating a secure ~~HE~~-LTF based on the values of the Secure ~~HE~~-LTF Counter in the Secure ~~HE~~-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 Ranging NDP from the ISTA a SIFS after the Ranging NDP Announcement frame~~; see 11.21.6.4.5.4.
- Send a protected LMR frame that includes the Secure ~~HE~~-LTF Parameters element to the ISTA; ~~only if the RSTA receives an HE Ranging I2R 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 *ista-ltf-key* and *ltf-iv*, respectively, for receiving a secure ~~HE~~-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.
- 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.
- 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 ~~HE~~-LTF Parameters element in the protected LMR frame and set the Measurement SAC subfield in the Secure ~~HE~~-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-~~HE~~-LTF in an ~~HE Ranging NDP~~ HE Ranging NDP or EHT Ranging NDP, the STA shall not use the TOD value of the HE Ranging NDP or EHT Ranging NDP for the secure range measurement exchange.

When a STA receives a Null-SAC-~~HE~~-LTF in an ~~HE Ranging NDP~~ HE Ranging NDP or EHT Ranging NDP, the STA shall not use the TOA value of the ~~HE Ranging NDP~~ HE Ranging NDP or EHT Ranging NDP, and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the protected LMR frame carrying the TOA value of the ~~HE Ranging NDP~~ HE Ranging NDP or 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 11-67.

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.

Change Figure 11-67 baseline, deleting the two occurrences of “HE” as follows:

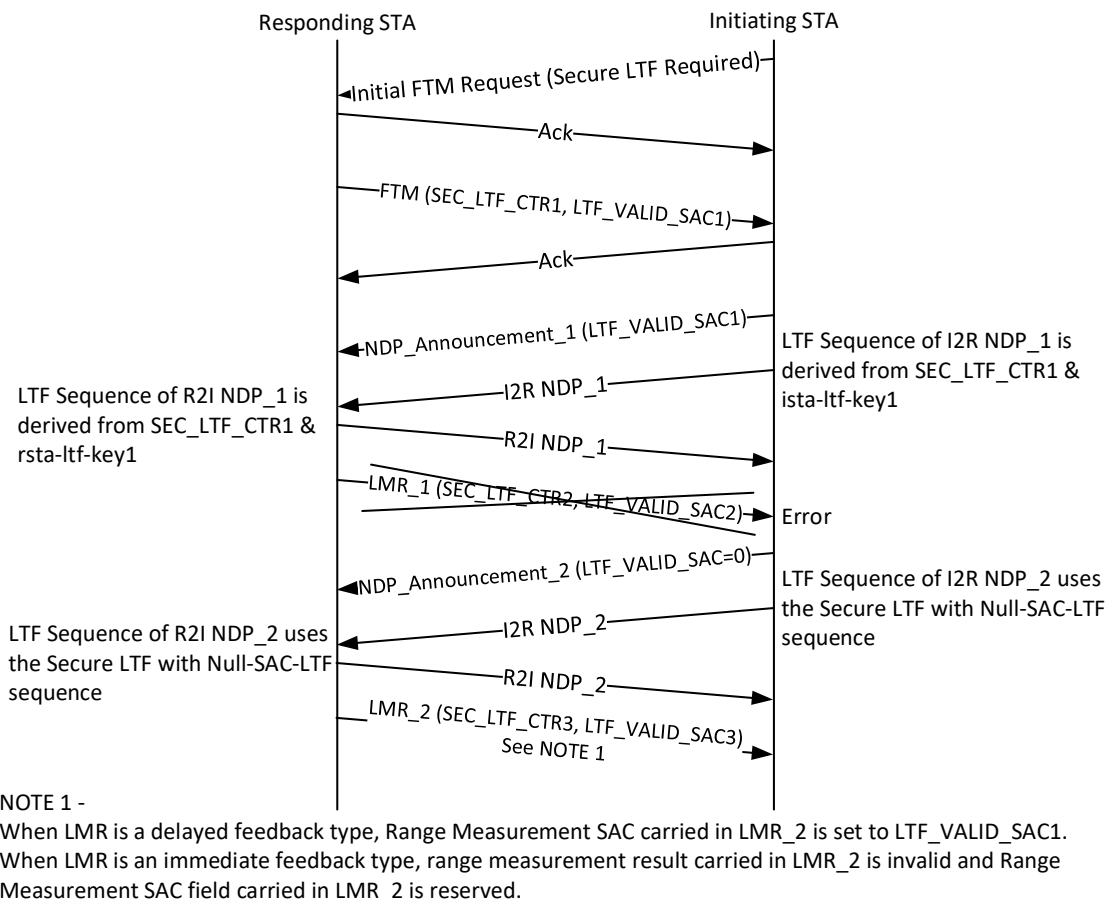


Figure 11-67—Error recovery non-TB ranging measurement exchange using secure HE-LTF

11.21.6.4.5.4 Overview of secure HE-LTF octet stream generation

This subclause 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 HE-LTFs. The mechanism is illustrated in Figure 11-68 and Figure 11-69.

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:

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

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 is equal to ExtractBits(SAC-and-LTF-Keys, 0, 16)

ista-ltf-key is equal to ExtractBits(SAC-and-LTF-Keys, 16, 128)
rsta-ltf-key is equal to ExtractBits(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 PPDU transmitted by the ISTA. The *rsta-ltf-key* shall be used to generate the pseudorandom octet stream to protect all of the LTFs in PPDU 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 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 ~~HE~~-LTF bit generator shall be constructed as follows:

- First 6 octets shall be the transmitter MAC address (A2).
- Next 6 octets shall encode 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 ~~HE~~-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 ~~HE~~-LTF bit generator generates the required number of AES blocks using the AES algorithm (see FIPS 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 to obtain the octet stream used for secure ~~HE~~-LTF generation.

NOTE 1—A 6-octet parameter representing the value the Secure LTF Counter subfield is sufficient because ~~a protected individually addressed Management~~ an individually addressed protected Management frame that uses a 6-octet PN is used to convey the LTF sequence information that carries the counter.

NOTE 2—The pseudorandom bit generator is based on AES-128 Counter mode approved by NIST (see NIST SP 800-90A R1 [B66]).

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 ~~HE~~-LTF measurement requires a variable number of octets from the pseudorandom octet stream depending on the TXVECTOR or RXVECTOR parameters for the LTFs as described in 27.3.20.2. 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 ~~HE~~-LTF octet stream generation on an ISTA

Figure 11-68 illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an ISTA.

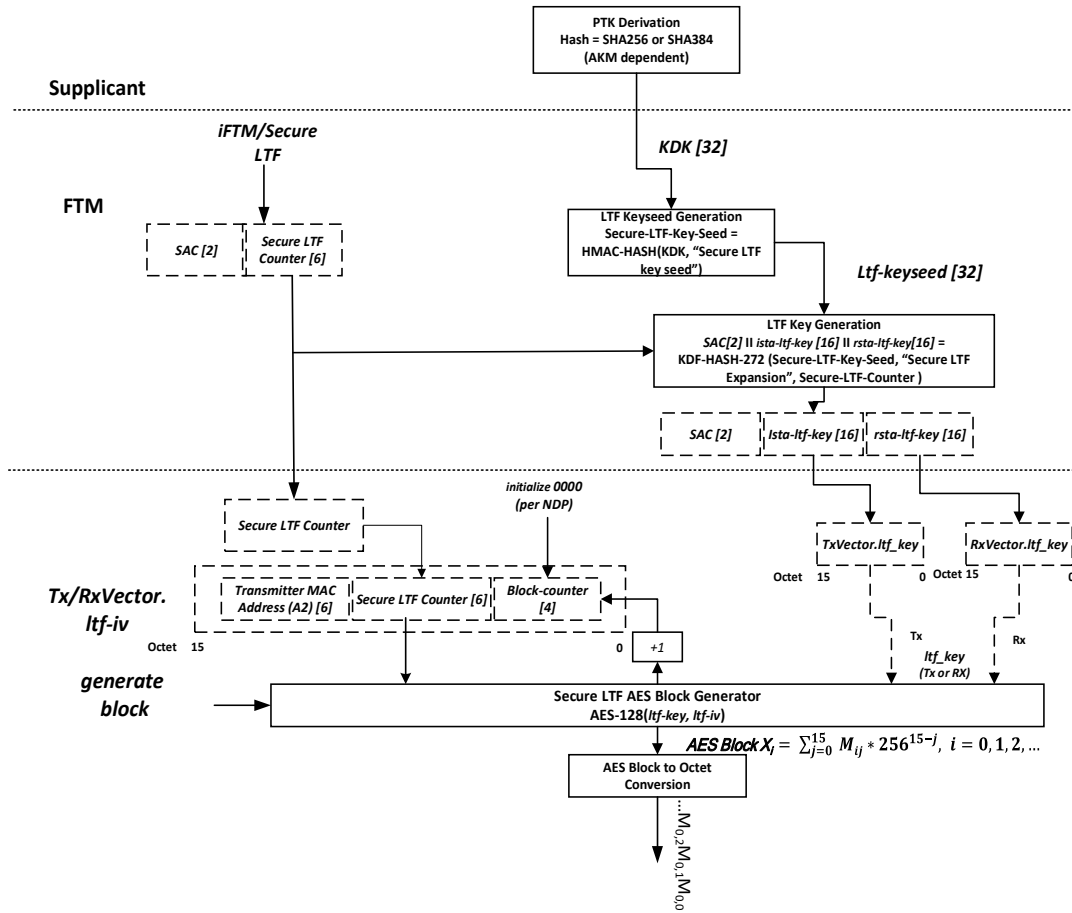


Figure 11-68—ISTA secure HE-LTF octet stream generation

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 Secure LTF Counter subfield and the block counter.

11.21.6.4.5.6 Secure HE-LTF input octet stream generation on an RSTA

Figure 11-69 illustrates the scheme for generating the SAC, LTF protection keys, and counter values used to generate a pseudorandom octet stream on an RSTA.

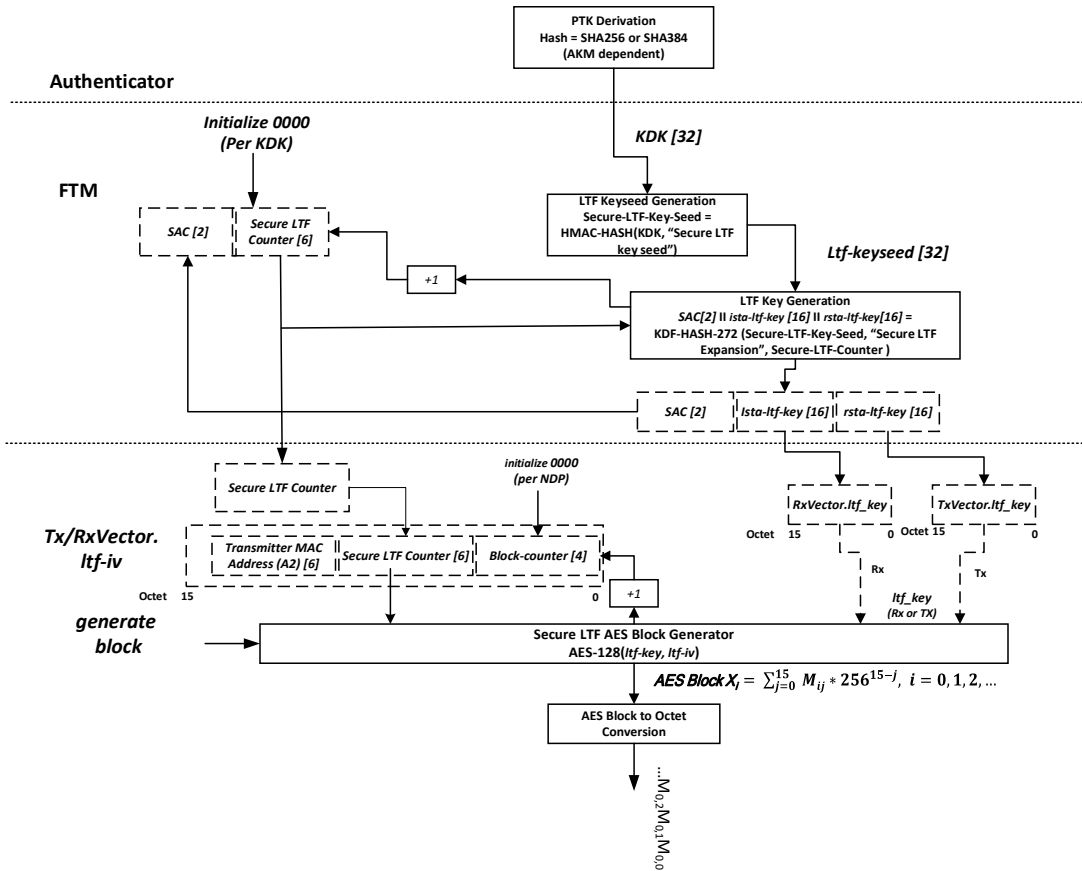


Figure 11-69—RSTA secure HE-LTF octet stream generation

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 HE-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.

Change the first three paragraphs of 11.21.6.4.6 as follows:

11.21.6.4.6 Transmission of a Rranging 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:
 - If the CH_BANDWIDTH is equal to 320 MHz is set to EHT_MU.
 - Otherwise, is set to HE_SU.
- 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) and non-TB ranging measurement exchange (11.21.6.4.4), is set to 0.
 - Is set to 1, in the TB ranging measurement exchange with secure ~~HE~~-LTF (11.21.6.4.5.2) and the non-TB ranging measurement exchange with secure ~~HE~~-LTF (11.21.6.4.5.3), is set to 1.
- 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 NDPs; it is set to 0 otherwise.
- In the TB ranging measurement exchange with secure ~~HE~~-LTF (11.21.6.4.5.2), the NUM_USERS parameter is set to the number of ISTAs to which the HE Ranging NDP or EHT Ranging NDP is transmitted.
- In the Non-TB ranging measurement exchange (11.21.6.4.4), 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.
- If the FORMAT parameter is equal to HE_SU, The DOPPLER parameter is set to 0.
- The NUM_STS parameter is set as follows:
 - In the TB ranging measurement exchange (11.21.6.4.3), 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 ~~HE~~-LTF (11.21.6.4.5.2):
 - When the HE Ranging NDP or EHT Ranging NDP is transmitted to more than one ISTA, the NUM_STS[*p*] parameter 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 Ranging NDP or EHT Ranging NDP is transmitted to one ISTA, the NUM_STS parameter 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.
 - In the Non-TB ranging measurement exchange (11.21.6.4.4) and the non-TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.3), set to the same value as the R2I NSTS subfield in the STA Info field with AID11 subfield equal to 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), 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 HE-LTF (11.21.6.4.5.2):
 - When the HE Ranging NDP or EHT Ranging NDP is transmitted to more than one ISTA, the LTF_REP[p] parameter 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 Ranging NDP or EHT Ranging NDP is transmitted to one ISTA, the LTF_REP parameter 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.
 - In the non-TB ranging measurement exchange (11.21.6.4.4) and the non-TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.3), 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), and TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.2), set to the sounding bandwidth, 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) and non-TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.3), set to the same value as the ~~RXVECTOR~~TXVECTOR parameter CH_BANDWIDTH in the preceding ~~Ranging~~R2I NDP Announcement frame.
 - If the FORMAT parameter is equal to EHT_MU, the INACTIVE_SUBCHANNELS parameter is set to the Puncturing Pattern field in the 320 MHz Ranging subelement of the IFTM frame.
 - ~~In 11.21.6.4.5, In the TB and non-TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5),~~ the LTF_KEY parameter is set as defined in 11.21.6.4.5.2 and 11.21.6.4.5.3. Otherwise, the LTF_KEY parameter is not present.

- In the TB ranging measurement exchange with secure HE-LTF, the LTF_OFFSET parameter is set as defined in 11.21.6.4.5.2. Otherwise, the LTF_OFFSET parameter is not present.
- If the FORMAT parameter is equal to HE_SU, the HE_LTF_TYPE parameter is set to 2xHE-LTF.
- If the FORMAT parameter is equal 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 PRS_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 $D_{Ranging_NDPA}$, which is the value of the Duration/ID field in the MAC header of the preceding Ranging NDP Announcement frame. The TXOP_DURATION parameter is set as follows:
 - If the FORMAT parameter is equal to HE_SU, the TXOP_DURATION parameter is set to either 127 or the value defined in Equation (26-3), replacing D_{HE_NDPA} by the following value:
 - In the TB ranging measurement exchange (11.21.6.4.3), and TB ranging measurement exchange with secure LTF (11.21.6.4.5.2), $D_{Ranging_NDP_Announcement}$, which is the Duration/ID field in the MAC header of the preceding Ranging NDP Announcement frame.
 - In the non-TB ranging measurement exchange (11.21.6.4.4) and non-TB ranging measurement exchange with secure LTF (11.21.6.4.5.3), $D_{Ranging_NDP}$, which is the TXOP field within the HE-SIG-A2 of the preceding I2R NDP.
 - If the FORMAT parameter is equal to EHT_MU, the TXOP_DURATION parameter is set to either 127 or the value defined in Equation (35-3), replacing D_{EHT_NDPA} by the following value:
 - In the TB ranging measurement exchange (11.21.6.4.3), and TB ranging measurement exchange with secure LTF (11.21.6.4.5.2), $D_{Ranging_NDP_Announcement}$, which is the Duration/ID field in the MAC header of the preceding Ranging NDP Announcement frame.
 - In the non-TB ranging measurement exchange (11.21.6.4.4) and non-TB ranging measurement exchange with secure LTF (11.21.6.4.5.3), $D_{Ranging_NDP}$, which is the TXOP field within the U-SIG of the preceding I2R NDP.

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:
 - If the CH_BANDWIDTH is equal to 320 MHz, is set to EHT_MU.
 - Otherwise, is set to HE_SU.
- 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), is set to 0.
 - ~~Is set to 1.~~ In the non-TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.3), is set to 1.
- 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 NDPs; it is set to 0 otherwise.
- If the FORMAT parameter is equal to HE_SU, 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 NDP Announcement frame, except if the value in the I2R NDP Tx Power subfield was set to a reserved value.
- The CH_BANDWIDTH is set to the same value as the TXVECTOR parameter CH_BANDWIDTH or CH_BANDWIDTH_IN_NON_HT in the preceding Ranging NDP Announcement frame.
- If the FORMAT parameter is equal to EHT_MU, the INACTIVE_SUBCHANNELS parameter is set to the Puncturing Pattern field in the 320 MHz Ranging subelement of the IFTM frame.
- In the non-TB ranging measurement exchange with secure ~~HE~~-LTF, the LTF_KEY parameter is set as defined in 11.21.6.4.5.2. Otherwise, the LTF_KEY parameter is not present.
- If the FORMAT parameter is equal to HE_SU, the HE_LTF_TYPE parameter is set to 2xHE-LTF.
- If the FORMAT parameter is equal 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 PRS_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 follows:

- If the FORMAT parameter is equal to HE_SU, the TXOP_DURATION parameter is set to either 127 or the value defined in Equation (26-3), replacing D_{HE_NDPA} by $D_{\text{Ranging NDP Announcement}}$, which is the Duration/ID field in the MAC header of the preceding Ranging NDP Announcement frame.
- If the FORMAT parameter is equal to EHT_MU, the TXOP_DURATION parameter is set to either 127 or the value defined in Equation (35-2), replacing D_{EHT_NDPA} by $D_{\text{Ranging NDP Announcement}}$, which is the Duration/ID field in the MAC header of the preceding Ranging NDP Announcement frame.

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:
 - If the CH_BANDWIDTH is equal to 320 MHz, is set to EHT_TB.
 - Otherwise, is set to HE_TB.
- The 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), is set to 0.
 - ~~Is set to 1;~~ In the TB ranging measurement exchange with secure HE-LTF (11.21.6.4.5.2), is set to 1.
- 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 NDPs; it is set to 0 otherwise.
- If the FORMAT parameter is equal to HE_TB, 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~~ RXVECTOR parameter CH_BANDWIDTH or CH_BANDWIDTH IN NON_HT in the preceding Ranging Sounding Trigger frame.
- If the FORMAT parameter is equal to EHT_TB the INACTIVE_SUBCHANNELS parameter is set to the Puncturing Pattern field in the 320 MHz Ranging subelement of the IFTM frame.
- In the TB ranging measurement exchange with secure HE-LTF, the LTF_KEY parameter is set as defined in 11.21.6.4.5.2. Otherwise, the LTF_KEY parameter is not present.

- If the FORMAT parameter is equal to HE_TB, the HE_LTF_TYPE parameter is set to 2xHE-LTF.
- If the FORMAT parameter is equal to EHT_TB, 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 received from the RSTA.
- The TXOP_DURATION parameter is set as follows:
 - If the FORMAT parameter is equal to HE_TB, the TXOP_DURATION parameter is set as defined in 26.11.5.
 - If the FORMAT parameter is equal to EHT_TB, the TXOP_DURATION parameter is set as defined in 35.11.1.5.

~~The TXOP_DURATION parameter is set as defined in 26.11.5 (TXOP_DURATION).~~

11.21.6.4.8 Measurement exchange in passive TB ranging mode

11.21.6.4.8.1 General

Change 11.21.6.4.8.1 as follows:

As stated in 11.21.6.1.3, 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 follow the rules and procedures described in 11.21.6.4.3, 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, the ISTA shall respond with an HE Ranging NDP instead of an HE TB Ranging NDP (or respectively an EHT Ranging NDP instead of an EHT TB Ranging NDP); see 11.21.6.4.8.3 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 for further details.

The passive TB ranging exchanges shall only occur in an availability window assigned for Passive TB ranging. Within the RSTA assigned availability window for passive ranging, the RSTA and ISTA shall only perform passive TB ranging activities.

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.

The Ranging Trigger frame, the NDP Announcement frame, the Primary RSTA Broadcast Passive TB Ranging Measurement report frame, and the Secondary RSTA Broadcast Passive TB Ranging Measurement report frame shall be transmitted in a non-HT duplicate PPDU.

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 11.21.6.4.3.2.

11.21.6.4.8.3 Measurement sound phase of Ppassive TB ranging-measurement sounding phase

Change 11.21.6.4.8.3 as follows:

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, 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 Ranging L2R~~ NDP exchanges, a Ranging NDP Announcement frame, and an ~~HE Ranging R2I~~ NDP transmission; see Figure 11-72.

Replace Figure 11-72 with the following:

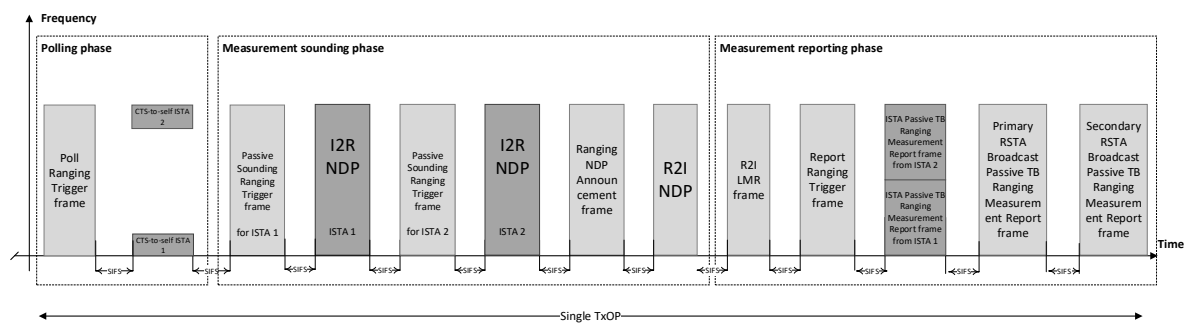


Figure 11-72—Passive TB ranging polling, measurement sounding, and measurement reporting phases

In passive TB ranging, for each ISTA, the RSTA shall transmit a Passive Sounding Ranging Trigger frame, which includes a single User Info field that is not a Special 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 Ranging I2R~~ 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 sounding bandwidth wider than that indicated in the IFTM frame sent to the ISTA, and the RSTA shall set the associated TXVECTOR parameter CH_BANDWIDTH or CH_BANDWIDTH_IN_NON_HT to be the sounding bandwidth, 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 Ranging R2I~~ NDP after receiving an ~~HE Ranging I2R~~ NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH_BANDWIDTH or CH_BANDWIDTH_IN_NON_HT to the sounding bandwidth 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 Ranging I2R~~ NDP as a response to a Passive Sounding Ranging Trigger frame shall set the TXVECTOR parameter CH_BANDWIDTH to be in the same way value as when sending an HE TB Ranging NDP or EHT TB Ranging NDP in response to the Trigger frame, respectively, i.e., based on the Common Info field and User Info field in the Passive Sounding Ranging Trigger frame.

As in TB ranging, an ISTA participating in a passive TB ranging exchange shall measure the TOD of its own ~~HE Ranging I2R~~ NDP and either the TOAs, or both the TOAs and the phase shift feedback TOAs (PSTOAs), when it receives the RSTA's ~~HE Ranging R2I~~ 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 Ranging I2R~~ NDPs transmitted by the other ISTAs participating in the passive TB ranging exchange. By reporting the timestamps for when it received the other ISTA's NDP transmissions, the quality of the location estimate for a PSTA listening in to the passive TB ranging exchanges can be improved.

The value of NSTS/NSS 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 NDP 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 11-73 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. The timestamps t5 and t6 are the times at which the I2R NDP and R2I NDPs arrive at the PSTA, respectively.

Replace Figure 11-73 with the following figure:

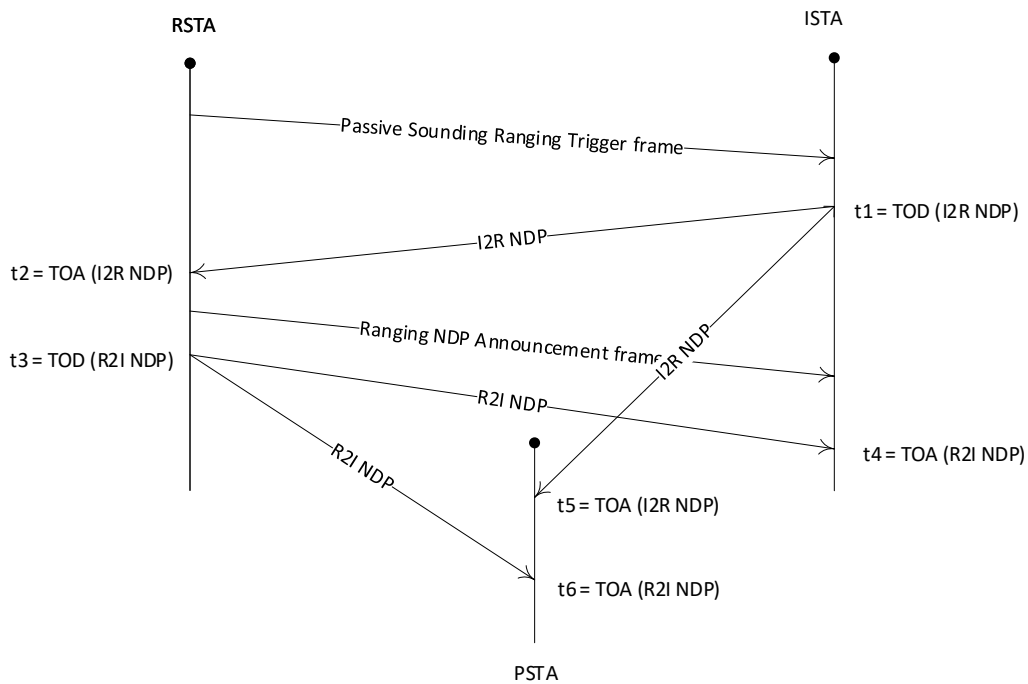


Figure 11-73—Example timing diagram of a Measurement Sounding phase in passive TB ranging

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 (11-11).

$$DToF_PRI = ToF_PR - ToF_PI \tag{11-11}$$

where

- ToF_PR is the time of flight between the PSTA and the RSTA
- 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 defined in~~ Equation (11-12).

$$DToF_PRI = t6 - t5 - 0.5 \times t3' + 0.5 \times t2' - 0.5 \times t4' + 0.5 \times t1' \tag{11-12}$$

where

- t1' and t4' are the times 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 times 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 11.21.6.4.9 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 Measurement reporting phase of Ppassive 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, unless explicitly stated otherwise.

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 11-74 for a depiction of the passive TB ranging measurement reporting phase.

Replace Figure 11-74 with the following figure:

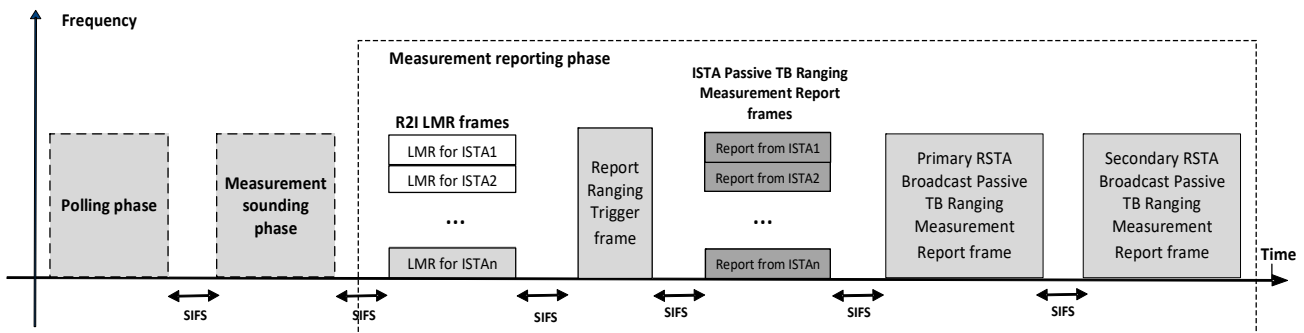


Figure 11-74—Passive TB ranging measurement reporting phase

In the passive TB ranging measurement reporting phase, an RSTA shall send a ~~Passive TB Ranging Measurement Report~~ R2I LMR frames and the Report Ranging Trigger frame to one or more ISTAs that sent an ~~HE Ranging I2R 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 measurement results~~.

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 9.4.2.306, 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.
- Optionally, the PS-TOAs 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.

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 the 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 11-74.

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 the 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 entry 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 at least one ~~the following~~ ISTA Passive TB Ranging Measurement Reports: see 9.6.7.52.

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 9.4.2.306, 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.

35. Extremely high throughput (EHT) MAC specification

35.14 PPDU format, bandwidth, MCS, NSS, and DCM selection rules

35.14.2 PPDU format selection

Insert the following paragraph list item for NDPA at the end of the subclause:

- A Ranging NDP Announcement frame with 320 MHz bandwidth shall be transmitted in a non-HT duplicate PPDU or EHT MU PPDU that is an EHT SU transmission.

36. Extremely high throughput (EHT) PHY specification

36.2 EHT PHY service interface

36.2.2 TXVECTOR and RXVECTOR parameters

*Change the existing rows in Table 36-1 for parameters “APEP_LENGTH” and “PSDU_LENGTH”.
Insert new rows at the end of Table 36-1 (but before the notes) as follows:*

Table 36-1—TXVECTOR and RXVECTOR parameters

Parameter	Condition	Value	TXVECTOR	RXVECTOR
APEP_LENGTH	FORMAT is EHT_MU or EHT_TB	Integer. If 0 and FORMAT is EHT_MU, indicates an EHT sounding NDP or <u>EHT Ranging NDP</u> . If 0 and FORMAT is EHT_TB, indicates an <u>EHT TB Ranging NDP</u> . Otherwise, indicates the number of octets in the range 1 to aPSDUMaxLength in the A-MPDU pre-EOF padding (see Table 36-70) that is carried in the PSDU.	MU	N
	FORMAT is PHY_VER_UNKNOWN	Not present.		
	Otherwise	See corresponding entry in Table 21-1 or Table 27-1.		
PSDU_LENGTH	FORMAT is EHT_MU or EHT_TB	Indicates the number of octets in the PSDU in the range 0 to aPSDUMaxLength octets (see Table 36-70). A value of 0 indicates an EHT sounding NDP, <u>an EHT Ranging NDP or an EHT TB Ranging NDP</u> .	N	Y
	FORMAT is PHY_VER_UNKNOWN	Not present.		
	Otherwise	See corresponding entry in Table 21-1 or Table 27-1.		
(...existing fields...)				
NUM_USERS	<u>FORMAT is EHT_MU and RANGING_FLAG is present</u>	<u>If SECURE_LTF_FLAG is 0, set to 1.</u> <u>If SECURE_LTF_FLAG is 1, set to the number of users of an EHT Ranging NDP with secure EHT-LTF.</u> <u>If NUM_USERS is larger than 1, NUM_STS, LTF_REP and LTF_KEY are arrays with number of entries equal to NUM_USERS</u>	<u>Y</u>	<u>N</u>
	<u>FORMAT is EHT_MU or HE_TB, and RANGING_FLAG is not present</u>	<u>Not present.</u>		

IEEE Std 802.11bk-2025
 IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—
 Local and Metropolitan Area Networks—Specific Requirements
 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
 Amendment 3: 320 MHz Positioning

Parameter	Condition	Value	TXVECTOR	RXVECTOR
	<u>Otherwise</u>	<u>See corresponding entry in Table 21-1 or Table 27-1.</u>		
(...existing fields...)				
TIME_OF_DEPARTURE_REQUESTED	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is present</u>	<p><u>The value true indicates that the MAC entity requests that the PHY entity measure and report time of departure parameters corresponding to the time when the first frame energy is sent by the transmitting port.</u></p> <p><u>The value false indicates that the MAC entity requests that the PHY entity neither measures nor reports time of departure parameters.</u></p>	<u>O</u>	<u>N</u>
	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is not present</u>	<u>Not present.</u>		
	<u>Otherwise</u>	<u>See corresponding entry in Table 21-1 or Table 27-1.</u>		
LTF_KEY	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is present, and SECURE_LTF_FLAG is 1</u>	<u>Contains the <i>rsta-ltf-key</i> or <i>ista-ltf-key</i> (see 11.21.6.4.5.4) when the secure EHT-LTFs are used (see 11.21.6.4.5).</u>	<u>Y</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>		
LTF_IV	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is present and SECURE_LTF_FLAG is 1</u>	<u>Contains the <i>ltf-iv</i> (see 11.21.6.4.5.4) used to generate the secure EHT-LTFs.</u>	<u>Y</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>		

Parameter	Condition	Value	TXVECTOR	RXVECTOR
LTF_REP	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is present</u>	<u>Indicates the number of EHT-LTF repetitions.</u>	<u>Y</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>		
RANGING_FLAG	<u>FORMAT is EHT_MU</u>	<u>If present, indicates the PPDU is an EHT Ranging NDP.</u> <u>Not present otherwise.</u>	<u>O</u>	<u>N</u>
	<u>FORMAT is EHT_TB</u>	<u>If present, indicates the PPDU is an EHT TB Ranging NDP.</u> <u>Not present otherwise.</u>	<u>O</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>	<u>N</u>	<u>N</u>
SECURE_LTF_FLAG	<u>FORMAT is EHT_MU or EHT_TB, and the RANGING_FLAG is present.</u>	<u>Set to 1 when the EHT Ranging NDP or EHT TB Ranging NDP uses secure EHT-LTF.</u> <u>Set to 0 otherwise.</u>	<u>Y</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>		
TX_WINDOW_FLAG	<u>FORMAT is EHT_MU or EHT_TB, and RANGING_FLAG is present and SECURE_LTF_FLAG is 1</u>	<u>Set to 1 when the secure EHT-LTF of an EHT Ranging NDP or EHT TB Ranging NDP uses the optional frequency domain Tx window.</u> <u>Set to 0 otherwise.</u>	<u>Y</u>	<u>N</u>
	<u>Otherwise</u>	<u>Not present.</u>		

36.2.3 TRIGVECTOR parameters

Insert the following subclause at the end of the 36.2.3:

36.2.3a LTFVECTOR parameters

The LTFVECTOR is carried in a PHY-RXLTFSEQUENCE.request that configures the PHY to be able to demodulate an EHT Ranging NDP or an EHT TB Ranging NDP. The parameters in Table 36-2a are defined as part of the LTFVECTOR parameter list in the PHY-RXLTFSEQUENCE.request primitive.

Table 36-2a—LTFVECTOR parameters

Parameter	Value
LTF_NSTS	Indicates the number of space-time streams in the following EHT Ranging NDP or the following EHT TB Ranging NDP.
LTF_REP	Indicates the number of EHT-LTF repetitions in the following EHT Ranging NDP or the following EHT TB Ranging NDP.
SECURE_LTF_FLAG	Set to 1 when the EHT Ranging NDP or EHT TB Ranging NDP uses secure EHT-LTF. Set to 0 otherwise.
LTF_KEY	Included when SECURE_LTF_FLAG is set to 1. Contains the <i>rsta-ltf-key</i> or <i>ista-ltf-key</i> (see 11.21.6.4.5.4) when receiving the secure EHT-LTFs.
LTF_IV	Included when SECURE_LTF_FLAG is set to 1. Contains the <i>ltf-iv</i> (see 11.21.6.4.5.4) for secure EHT-LTFs or null otherwise.
LTF_OFFSET	Included when SECURE_LTF_FLAG is set to 1. Indicates the number of EHT-LTFs to skip before beginning to process the EHT-LTF symbols.
TX_WINDOW_FLAG	Included when SECURE_LTF_FLAG is set to 1. Set to 1 when the secure EHT-LTF of an EHT Ranging NDP or EHT TB Ranging NDP uses the optional frequency domain Tx window. Set to 0 otherwise.

36.3 Extremely high throughput (EHT) PHY specification

Change the caption of Table 36-37 to be “Common field for the EHT sounding NDP and for the EHT Ranging NDP”.

Insert the following subclause 36.3.19a and its subclauses at the end of 36.3.19:

36.3.19a EHT Ranging NDP and EHT TB Ranging NDP

36.3.19a.1 EHT Ranging NDP

The format of the EHT Ranging NDP is shown in Figure 36-58a.

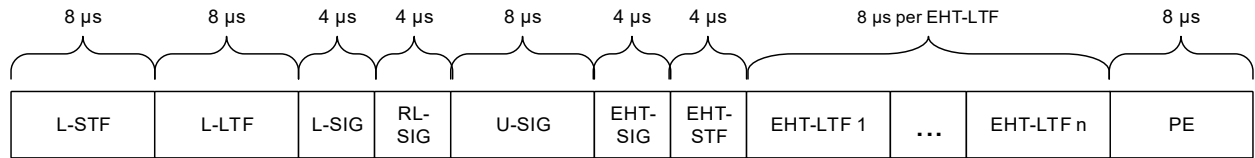


Figure 36-58a—EHT Ranging NDP format

The EHT Ranging NDP has the following properties:

- It is an EHT MU PPDU with a single EHT-SIG symbol encoded using EHT-MCS 0 and no Data field. The EHT-SIG field contains a Common field as defined in Table 36-37 and no User Specific field.
- An EHT Ranging NDP is indicated by setting the PPDU Type And Compression Mode field of the U-SIG to 1. In the EHT Ranging NDP, the only supported Bandwidth field values of the EHT U-SIG are 320 MHz-1 and 320 MHz-2.
- In the EHT Ranging NDP, the 242-tone RUs overlapping the 20 MHz channels that are signaled as punctured through the Punctured Channel Indication field of the U-SIG field are punctured.
- The L-STF and L-LTF fields in an EHT Ranging NDP are the same as the L-STF and L-LTF fields in an EHT MU PPDU. The fields in L-SIG, RL-SIG, U-SIG, and EHT-SIG have the same bit assignments and definitions as the fields in an EHT MU PPDU unless specified otherwise.
- The EHT-STF field in an EHT Ranging NDP is the same as the EHT-STF field in an EHT MU PPDU.
- It uses EHT-LTFs or secure EHT-LTFs when the TXVECTOR parameter SECURE_LTF_FLAG is set to 0 or 1, respectively.
- Secure EHT-LTFs use randomized EHT-LTF sequences, pseudorandom and deterministic per stream phase rotation, and, when the TXVECTOR parameter TX_WINDOW_FLAG is set to 1, use a frequency domain flat top window instead of the frequency domain rectangular window; see 36.3.19b.
- It uses EHT-LTF repetitions, if indicated in the TXVECTOR parameter LTF_REP by values larger than one.
- The number of EHT-LTF User Block fields in the EHT-LTF field is equal to the number of Users, TXVECTOR parameter NUM_USERS.
- The EHT-LTF field consists of one or more EHT-LTF User Block fields; each EHT-LTF User Block field contains one or more EHT-LTF Repetition Blocks, where the number of EHT-LTF Repetition Blocks is equal to LTF_REP. An EHT-LTF Repetition Block in an EHT-LTF User Block field comprises one or more EHT-LTF symbols, $N_{EHT-LTF}$, calculated using the number of space-time streams NUM_STS for this user, as defined in Table 21-13.

- When the TXVECTOR parameter `SECURE_LTF_FLAG` is equal to 0, one EHT-LTF User Block field is present. When the TXVECTOR parameter `SECURE_LTF_FLAG` is equal to 1, each EHT-LTF User Block field contains EHT-LTF symbols for one user.
- No beamforming steering matrix is applied to the waveform. The Beamformed field in the EHT-SIG of an EHT Ranging NDP is always set to 0.
- For transmission of EHT-STFs and EHT-LTFs, if `NSS` equals N_{TX} , the Q matrix shall be an identity matrix, and if `NSS` is less than N_{TX} , the Q matrix shall be based on an antenna selection matrix with no antenna swapping. The Q matrix becomes an identity matrix when all 0 rows are removed.
- The only supported mode is 2x EHT-LTF with 1.6 μ s GI. The other combinations of EHT-LTF modes and GI duration shall not be used. No energy is transmitted during the GI of the EHT-LTF symbols when secure EHT-LTF are used, which is referred to as a zero power GI.
- Has a Packet Extension (PE) field that is 8 μ s in duration. No energy is transmitted during the first 1.6 μ s of the PE field, if the EHT-LTF field is using the secure EHT-LTF, similar to no energy being transmitted during the GI of EHT-LTF symbols.
- For decoding the EHT-LTF fields, a PHY-RXLTFSEQUENCE.request primitive issued from the MAC provides the `LTF_REP`, `LTF_NSTS`, and `LTF_OFFSET` parameters, which are not encoded in the EHT-SIG, but are included in the preceding Ranging NDP Announcement frame. The `LTF_OFFSET` parameter indicates the number of secure EHT-LTF symbols to skip for receiving the corresponding user's EHT-LTF User Block field.
- When the TXVECTOR parameter `NUM_USERS` is equal to 1, the TXVECTOR parameter `NUM_STS` is used to set the `NSS` field and the Number of EHT-LTF Symbols field within the Common field of the EHT-SIG, as defined in Table 36-37. The Number of EHT-LTF Symbols field is set according to Table 21-13. Otherwise, when the TXVECTOR parameter `NUM_USERS` is greater than 1 and the TXVECTOR parameter `NUM_STS` is an array, `NUM_STS[1]`, i.e., the first element in the array, is used instead.
- The number of EHT-LTF symbols in the EHT-LTF field in an EHT Ranging NDP depends on the number of space-time streams `NUM_STS`, the number of EHT-LTF repetitions `LTF-REP`, and when secure EHT-LTFs are used, the number of users `NUM_USERS`.

NOTE 1—See examples in Figure 36-58b and Figure 36-58c.

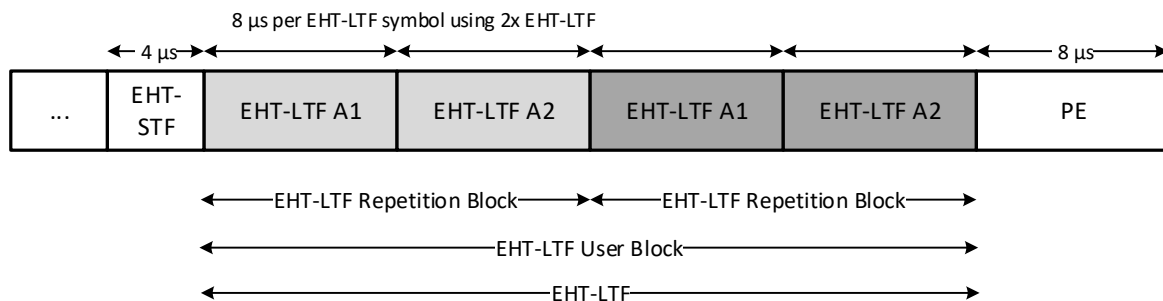


Figure 36-58b—An example of an EHT-LTF field in an EHT Ranging NDP with `NUM_USERS = 1`, `NUM_STS = 2`, and `LTF_REP = 2`

IEEE Std 802.11bk-2025
 IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—
 Local and Metropolitan Area Networks—Specific Requirements
 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
 Amendment 3: 320 MHz Positioning

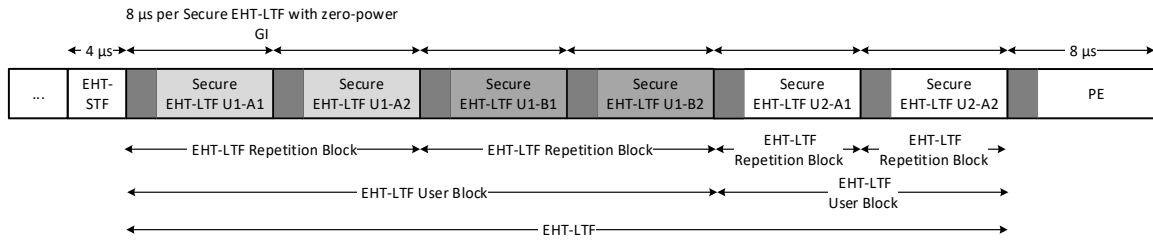


Figure 36-58c—An example of a secure EHT-LTF field with NUM_USERS=2, NUM_STS = [2,1], and LTF_REP = [2,2]

When the TXVECTOR parameter `SECURE_LTF_FLAG` is equal to 0, EHT-LTFs as defined in 36.3.19a are used in the EHT Ranging NDP. There is a single EHT-LTF User Block field in an EHT-LTF field, and the total number of EHT-LTF symbols in the EHT-LTF field is the product of the number of symbols in an EHT-LTF Repetition Block, $N_{EHT-LTF}$, and the number of EHT-LTF repetitions, given in `LTF_REP`.

The construction of the EHT-LTFs in an EHT Ranging NDP is done by repeating the steps in 36.3.19a `LTF_REP` times, i.e., the value of `LTF_REP` is the number of EHT-LTF Repetition Blocks in the EHT-LTF User Block field. If the TXVECTOR parameter `SECURE_LTF_FLAG` is equal to 0, all the EHT-LTF symbols belong to a single EHT-LTF User Block field.

When the TXVECTOR parameter `SECURE_LTF_FLAG` is equal to 1, secure EHT-LTFs as defined in 36.3.19b are used, and the Packet Extension field is partially replaced by a zero power GI in its first 1.6 μs, see Figure 36-58d. For the secure EHT-LTF symbol or Packet Extension field with zero power GI, the time domain signal has zero power during the period of the GI. The repetitions of the EHT-LTF symbols are repetitions of the EHT-LTF Repetition Block. The randomized EHT-LTF sequences are different in each of the EHT-LTF Repetition Blocks. The total number of EHT-LTF symbols in an EHT-LTF User Block field is the product of the number of symbols in an EHT-LTF Repetition Block, $N_{EHT-LTF}$, and the number of EHT-LTF repetitions given in `LTF_REP`.

For secure EHT-LTF transmissions, the number of EHT-LTF repetitions given in `LTF_REP` shall be greater than 1.

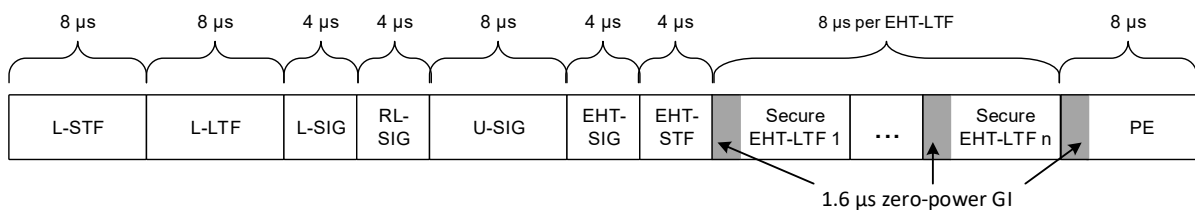


Figure 36-58d—EHT Ranging NDP format with secure EHT-LTFs

NOTE 2—The intended receiver of the Secure EHT-LTFs can use implementation-specific methods to detect the occurrence of an attack. It can explore the EHT-LTF repetitions to check the consistency of the channel estimation or the signal-to-interference ratio (SIR) drop from the impact of an attack. See Annex AE for more details on the SIR drop due to an attack.

The secure EHT-LTFs of each User Block field are concatenated and form the EHT-LTF field of an EHT Ranging NDP; the total number of EHT-LTF symbols in an EHT-LTF field shall not exceed a maximum of 64 secure EHT-LTF symbols over all users, all space time streams, and the number of EHT-LTF repetitions.

In each EHT-LTF User Block field within the EHT-LTF field, the number of transmit antennas shall be equal to the number indicated in NUM_STS for the corresponding EHT-LTF User Block field and may vary from one EHT-LTF User Block field to another. Within the EHT-STF field, the number of transmit antennas should match the number of transmit antennas in the first EHT-LTF User Block field. In the pre-EHT modulated fields, the number of transmit antennas shall be no less than the minimum number of transmit antennas in any of the EHT modulated fields. The sum of the transmit power across all transmit antennas shall remain constant throughout the entire EHT Ranging NDP.

36.3.19a.2 EHT TB Ranging NDP

The format of an EHT TB Ranging NDP is shown in Figure 36-58e.

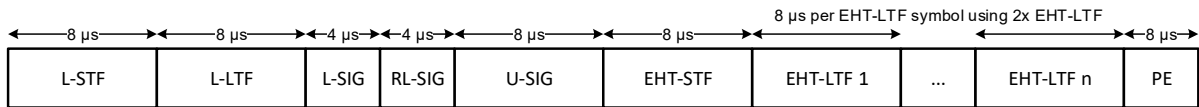


Figure 36-58e—EHT TB Ranging NDP format

The EHT TB Ranging NDP has the following properties:

- Uses the EHT TB PPDU format but without the Data field.
- The U-SIG field is encoded in the same way as in the EHT TB PPDU, i.e, the UL/DL field is set to 1 and the PPDU Type And Compression Mode field is set to 0.
- The EHT-STF field in EHT TB Ranging NDP is the same as the EHT-STF field in an EHT TB PPDU.
- Uses EHT-LTFs or secure EHT-LTFs when the TXVECTOR parameter SECURE_LTF_FLAG is set to 0 or 1, respectively.
- Secure EHT-LTFs use randomized EHT-LTF sequences, pseudorandom and deterministic per stream phase rotation and, when the TXVECTOR parameter TX_WINDOW_FLAG is set to 1, a frequency domain flat top window is used instead of the frequency domain rectangular window; see 36.3.19b.
- It uses EHT-LTF repetitions, if indicated in the TXVECTOR parameter LTF_REP by values larger than one.
- The EHT-LTF field of an EHT TB Ranging NDP consists of a single EHT-LTF User Block field. The EHT-LTF User Block field contains one or more EHT-LTF Repetition Blocks, and the number of EHT-LTF Repetition Blocks is equal to LTF_REP. Each EHT-LTF Repetition Block in the EHT-LTF User Block field comprises of one or more EHT-LTF symbols, NEHT-LTF specified in the Common Info field within the Sounding Ranging Trigger frame.
- The only supported mode is the 2x EHT-LTF with 1.6 μs GI. The other combinations of EHT-LTF modes and GI duration are disallowed. No energy is transmitted during the GI of the EHT-LTF symbols when secure EHT-LTF are used, which is referred to as a zero power GI.
- Has a Packet Extension (PE) field that is 8 μs in duration. No energy is transmitted during the first 1.6 μs of the PE field if the EHT-LTF field is using the secure EHT-LTF, similar to no energy being transmitted during the GI of EHT-LTF symbols.
- No beamforming steering matrix is applied to the waveform.

- For transmission of EHT-LTFs, if NSS equals N_{TX} , the Q matrix shall be an identity matrix, and if NSS is less than N_{TX} , the Q matrix shall be an antenna selection matrix with no antenna swapping. The Q matrix becomes an identity matrix when all 0 rows are removed.

The number of EHT-LTF symbols in an EHT TB Ranging NDP is the product of the number of EHT-LTF symbols in an EHT-LTF Repetition Block, $N_{\text{EHT-LTF}}$, and the number of EHT-LTF repetitions, given in LTF_REP. A value of LTF_REP equal to 1 indicates no repetition, i.e., a single EHT-LTF Repetition Block is included in the EHT-LTF User Block field, and a value of LTF_REP greater than 1 indicates the use of repetitions, i.e., multiple EHT-LTF Repetition Blocks are included in the EHT-LTF User Block field. The sum of transmit power shall remain constant throughout the entire EHT TB Ranging NDP.

When the TXVECTOR parameter SECURE_LTF_FLAG is set to 0, EHT-LTFs as defined in 36.3.19a are used in each EHT-LTF Repetition Block.

When the TXVECTOR parameter SECURE_LTF_FLAG is set to 1, secure EHT-LTFs as defined in 36.3.19b are used in the EHT-LTF Repetition Blocks, and the Packet Extension field shall be partially replaced by a zero power GI in its first 1.6 μs ; see Figure 36-58f. The repetitions of the EHT-LTF symbols form the EHT-LTF Repetition Blocks. The randomized EHT-LTF sequences are different in each EHT-LTF Repetition Block.

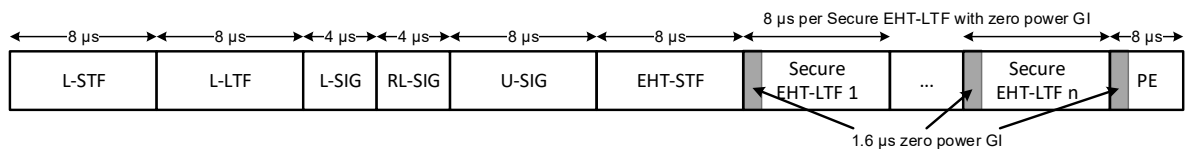


Figure 36-58f—EHT TB Ranging NDP with secure EHT-LTFs

36.3.19b EHT-LTF field using secure EHT-LTF

36.3.19b.1 Introduction

The EHT-LTF field using secure EHT-LTF is similar to the EHT-LTF field, see 36.3.19a, with the following differences:

- The EHT-LTF sequence is replaced by the randomized LTF sequence described in 36.3.19b.2.
- The conventional GI is replaced by a zero power GI.
- There are no single stream pilot subcarriers in the secure EHT-LTFs, all subcarriers are mapped using the $P_{\text{EHT-LTF}}$ matrix.
- No CSD is applied to the space-time streams.
- Each spatial stream has a per stream pseudorandom and deterministic phase rotation applied to all the subcarriers.
- A frequency domain flat top window is applied to the secure EHT-LTF when configured.

36.3.19b.2 Generation of a randomized secure EHT-LTF sequence for the 320 MHz secure NDP

The secure EHT-LTF sequence is constructed using pseudorandom 64-QAM modulation. Pseudorandom octets defined in 11.21.6.4.5.4 are used in the construction of the pseudorandom 64-QAM values.

The first seven pseudorandom octets ($Octet_0-Octet_6$) in the secure NDP are used for per stream phase rotations, see 27.3.20.3. Starting with $Octet_7$, these pseudorandom octets are used for the construction of pseudorandom 64-QAM values in the secure EHT-LTF sequences.

The following text describes the mapping of pseudorandom octets to the nonzero entries of the 320 MHz secure 2x EHT-LTF sequence, and then the construction of the 64-QAM values for each nonzero entry of the secure EHT-LTF sequence.

The construction of the 320 MHz secure LTF sequence uses a segment parser to divide the pseudorandom octets between the four sequences, one for each of the four 80 MHz subblocks. The subblocks are enumerated first to last, starting from the lowest frequencies to the highest. Figure 36-58g illustrates the segment parser distribution of pseudorandom octets between the sequences for each of the 80 MHz subblocks.

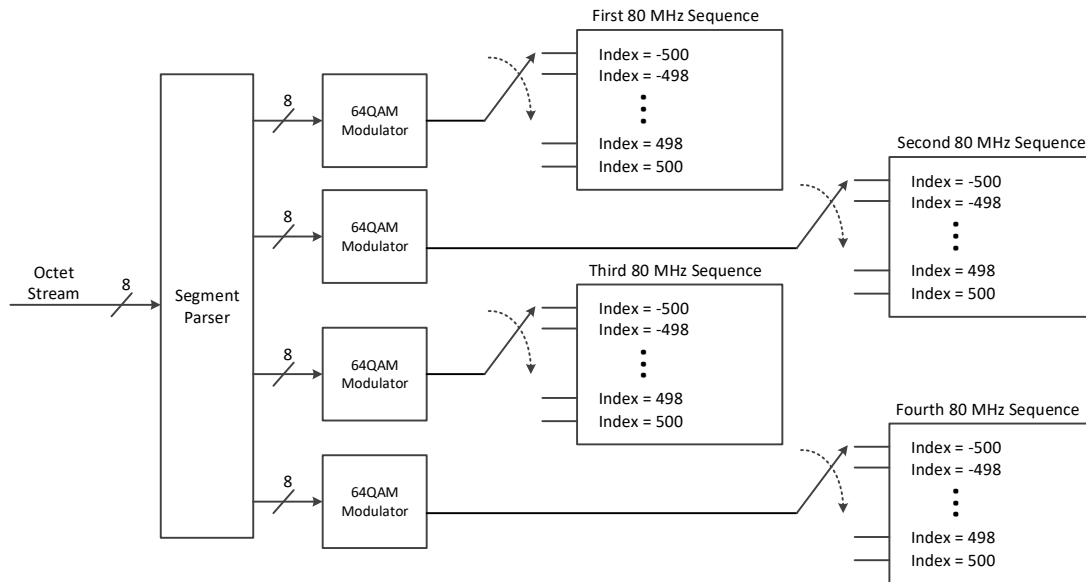


Figure 36-58g—Segment parser distributing pseudorandom octets to the sequences for each of the four 80 MHz subblocks in the 320 MHz secure EHT-LTF

The indices of the nonzero entries of each 80 MHz subblock’s secure 2x EHT-LTF sequence are given by the nonzero entries of the 2x EHT-LTF sequence in Equation (36-39).

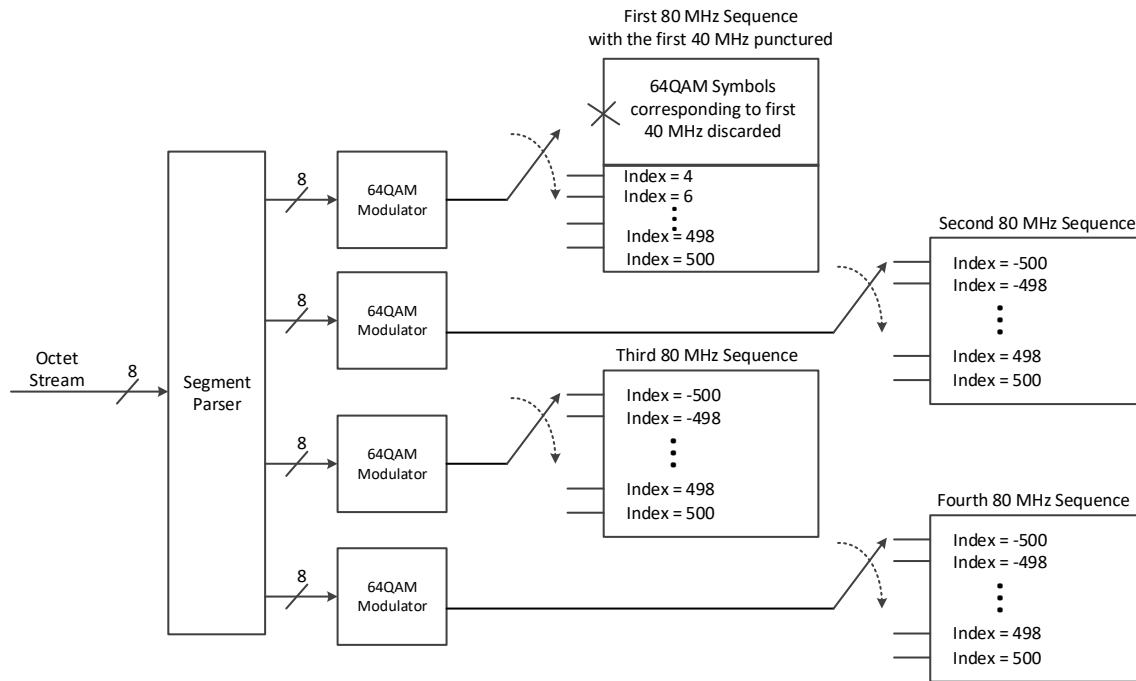


Figure 36-58h—Segment parser example with one 40 MHz subband punctured

Puncturing is applied directly on the subcarriers of the punctured 20 MHz subchannels indicated in the TXVECTOR parameter INACTIVE_SUBCHANNELS and does not affect the 64-QAM values mapped to other 20 MHz subchannels. See Figure 36-58h for an illustration of the mapping of values to subcarriers when the first two 20 MHz subbands are punctured.

There are up to 64 secure EHT-LTF sequences in an NDP. For notational convenience, the EHT-LTF sequence number is indicated with the integer n , which is an integer between one and 64. Since each secure EHT-LTF sequence is used to generate each of the EHT-LTF symbols, n also indicates the EHT-LTF symbol number. Table 36-62a provides the pseudorandom octet index for each nonzero subcarrier index for the n -th quadruplet of 80 MHz subblocks.

Table 36-62a—Pseudorandom octet index for each nonzero subcarrier index in the n -th quadruplet of 80 MHz segments

80 MHz subblocks	Secure EHT-LTF tone index	Pseudorandom octet index
First	-500	$7 + (n - 1) \times 1992$
Second	-500	$8 + (n - 1) \times 1992$
Third	-500	$9 + (n - 1) \times 1992$
Fourth	-500	$10 + (n - 1) \times 1992$
First	-498	$11 + (n - 1) \times 1992$
Second	-498	$12 + (n - 1) \times 1992$
⋮	⋮	⋮
First	-4	$999 + (n - 1) \times 1992$
Second	-4	$1000 + (n - 1) \times 1992$
Third	-4	$1001 + (n - 1) \times 1992$
Fourth	-4	$1002 + (n - 1) \times 1992$
First	4	$1003 + (n - 1) \times 1992$
Second	4	$1004 + (n - 1) \times 1992$
Third	4	$1005 + (n - 1) \times 1992$

80 MHz subblocks	Secure EHT-LTF tone index	Pseudorandom octet index
Fourth	4	$1006 + (n - 1) \times 1992$
⋮	⋮	⋮
Third	498	$1993 + (n - 1) \times 1992$
Fourth	498	$1994 + (n - 1) \times 1992$
First	500	$1995 + (n - 1) \times 1992$
Second	500	$1996 + (n - 1) \times 1992$
Third	500	$1997 + (n - 1) \times 1992$
Fourth	500	$1998 + (n - 1) \times 1992$

All entries in the 320 MHz secure EHT-LTF sequence corresponding to indices of values set to 0 in Equation (36-39) shall be set to 0.

The six least significant bits $B_0, B_1, B_2, B_3, B_4, B_5$ of an octet are used in the construction of the 64-QAM value, as specified in Table 17-18.

36.3.19b.3 Frequency domain windowing in EHT-LTF field using secure EHT-LTF

The frequency domain windowing function $w_{FD}(k)$ is applied to the subcarriers modulated with the secure EHT-LTF sequence $X_{k,n}^m$. It follows the definition in 27.3.20.4, with the addition of

$$N_{FD} = 8192$$

for the bandwidth of 320 MHz.

36.3.19b.4 Construction of secure EHT-LTF symbols

The construction of the n-th secure EHT-LTF symbol is achieved as follows:

- a) Sequence generation: Construct the n-th randomized EHT-LTF sequence $X_{k,r,n}^u$ in the frequency domain over the bandwidth indicated by CH_BANDWIDTH as described in 36.3.19b.2.
- b) Apply the frequency domain window function $w_{FD}(k)$ to all the tones of the secure EHT-LTF sequence. The frequency domain window can be the rectangular window or flat top window, when the TXVECTOR parameter TX_WINDOW_FLAG is set to 0 or 1, respectively.
- c) Apply the $P_{EHT-LTF}$ matrix to all tones of the secure EHT-LTF sequence.
- d) Apply per spatial stream phase rotation: Generate the pseudorandom phase rotation for each spatial stream. Apply the pseudorandom phase rotation along with the deterministic phase rotation to the spatial streams as described in 27.3.20.3.
- e) Apply a zero CSD on each space-time stream, which is equivalent to no CSD per space-time stream.
- f) There is no spatial mapping; the Q matrix is a block identity matrix.
- g) IDFT: Compute the inverse discrete Fourier transform.
- h) Insert zero power GI: Prepend values of zero of length indicated by the TXVECTOR parameter GI_TYPE.

- i) Analog and RF: Upconvert the resulting complex baseband waveform associated with each transmit chain to an RF signal according to the center frequency of the desired channel and transmit.

36.3.20 Transmit specification

Insert the following new subclause after 36.3.20.4.4.

36.3.20.5 Time of departure accuracy

The Time of Departure accuracy test evaluates TIME_OF_DEPARTURE against aTxPHYTxStartRMS and aTxPHYTxStartRMS against TIME_OF_DEPARTURE_ACCURACY_TEST_THRESH as defined in Annex P with the following test parameters:

- MULTICHANNEL_SAMPLING_RATE is:
$$320 \times 10^6 \left(1 + \left[\frac{f_H - f_L}{320 \text{ MHz}} \right] \right) \text{ sample/s, for a CH_BANDWIDTH parameter equal to CBW320}$$

where

- f_H is the nominal center frequency in Hz of the highest channel in the channel set
- f_L is the nominal center frequency in Hz of the lowest channel in the channel set, the channel set is the set of channels upon which frames providing measurements are transmitted, and the channel set comprises channels uniformly spaced across.
- FIRST_TRANSITION_FIELD is L-STF.
- SECOND_TRANSITION_FIELD is L-LTF.
- TRAINING_FIELD is L-LTF windowed in a manner that should approximate the windowing described in 17.3.2.5 with TTR = 100 ns.
- TIME_OF_DEPARTURE_ACCURACY_TEST_THRESH is 80 ns.

NOTE—The indicated windowing applies to the time of departure accuracy test equipment, and not the transmitter or receiver.

Change 36.3.22 as follows:

36.3.22 EHT transmit procedure

The PHY indicates the state of the primary channel and other channels (if any) via the PHY-CCA.indication primitive (see 36.3.21.6 and 8.3.5.12). Transmission of the PPDU shall be initiated by the PHY after receiving the PHY-TXSTART.request primitive (containing TXVECTOR). The TXVECTOR elements for the PHY-TXSTART.request primitive are specified in Table 36-1.

Transmission of the PHY preamble may start if TIME_OF_DEPARTURE_REQUESTED is false and shall start immediately if TIME_OF_DEPARTURE_REQUESTED is true, based on the parameters passed in the PHY-TXSTART.request primitive.

If all of the following conditions are met:

- if dot11TODImplemented and dot11TODActivated are true or dot11TimingMsmtActivated is true,
- the TXVECTOR parameter TIME_OF_DEPARTURE_REQUESTED is true,

then the PHY shall issue a PHY-TXSTART.confirm primitive (containing TXSTATUS) to the MAC, setting the TIME_OF_DEPARTURE parameter to the value of the time when the first frame energy is sent by the transmitting port and providing the corresponding clock rate in the TIME_OF_DEPARTURE ClockRate parameter within the TXSTATUS vector. If dot11TimingMsmtActivated is true, then the PHY shall also set the value of TX_START_OF_FRAME_OFFSET parameter in the TXSTATUS vector as described in 15.2.4.

36.3.23 EHT receive procedure

Change the second paragraph as follows:

This receive procedure and state machine do not describe the operation of optional features, such as EHT Ranging NDP and EHT TB Ranging NDP. If the detected format indicates a non-HT PPDU, refer to the receive procedure and state machine in Clause 15, Clause 16, Clause 17, and Clause 18. If the detected format indicates an HT PPDU format, refer to the receive procedure and state machine in Clause 19. If the detected format indicates a VHT PPDU format, refer to the receive procedure and state machine in Clause 21. If the detected format indicates an HE PPDU format, refer to the receive procedure and state machine in Clause 27. Through station management (via the PLME), the PHY is set to the appropriate frequency as specified in 36.4. The PHY has also been configured with BSS identification information and STA identification information (i.e., BSS color value and STA-ID) so that it can receive data intended for the STA in the specific BSS. Other receive parameters, such as RSSI and indicated DATARATE, can be accessed via the PHY SAP.

Annex B

(normative)

Protocol Implementation Conformance Statement (PICS)

B.2.2 General abbreviations for Item and Support columns

Insert the definition for EPP in the abbreviation list.

EPP enhanced positioning physical layer (PHY)

Change the text below in B.4.3 IUT configuration:

B.4.3 IUT configuration

Item	IUT configuration	References	Status	Support
*_CFTB	Support for FTM TB sounding	11.21.6.4.3	(<u>CFHE OR CFEHT</u>):O	Yes <input type="checkbox"/> No <input type="checkbox"/>
*_CFNTB	Support for FTM Non TB sounding	11.21.6.4.4	(<u>CFHE OR CFEHT OR CFNGV</u>): :O	Yes <input type="checkbox"/> No <input type="checkbox"/>
*_CFPTB	Support for Passive Sounding	11.21.6.4.8	(<u>CFHE OR CFEHT</u>): O	Yes <input type="checkbox"/> No <input type="checkbox"/>
*_CFPASN	Support for PASN	12.12	PC34:O	Yes <input type="checkbox"/> No <input type="checkbox"/>
*_CFPSEC	Support for PHY security, ability to transmit and receive secure LTF waveforms for TB and non-TB operation.	11.2.6.4.6	PC34 AND (<u>CFHE OR CFEHT</u>):O	Yes <input type="checkbox"/> No <input type="checkbox"/>

B.4.37 Enhanced positioning (Ranging) features

Change the text identified below in B.4.37.2 EP PHY features:

B.4.37.2 EP PHY features

Item	Protocol capability	References	Status	Support
	Are the following PHY protocol features supported?			
EPP1	EP TB and non-TB measurement exchange waveforms	27.3 <u>36.3</u>		
EPP1.1	HE ranging NDP	27.3.19.1	(CFTB OR CFNTB OR CFPFB):M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
EPP1.2	HE ranging NDP with secure LTFs	27.3.19.1	(CFTB OR CFNTB):M CFPASN:M CFPSEC:M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
EPP1.3	HE TB ranging NDP	27.3.19.2	CFTB:M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
EPP1.4	HE TB ranging NDP with secure LTFs	27.3.19.2	CFPASN:M CFPSEC:M CFTB:M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
<u>EPP1.5</u>	<u>EHT ranging NDP</u>	<u>36.3.4.1</u>	<u>(CFTB OR CFNTB OR CFPFB):O</u>	<u>Yes <input type="checkbox"/> No <input type="checkbox"/></u> <u>N/A <input type="checkbox"/></u>
<u>EPP1.6</u>	<u>EHT ranging NDP with secure LTFs</u>	<u>36.3.4.1</u>	<u>(CFTB OR CFNTB):O</u> <u>CFPASN:O</u> <u>CFPSEC:O</u>	<u>Yes <input type="checkbox"/> No <input type="checkbox"/></u> <u>N/A <input type="checkbox"/></u>
<u>EPP1.7</u>	<u>EHT TB ranging NDP</u>	<u>36.3.4.2</u>	<u>CFTB:O</u>	<u>Yes <input type="checkbox"/> No <input type="checkbox"/></u> <u>N/A <input type="checkbox"/></u>
<u>EPP1.8</u>	<u>EHT TB ranging NDP with secure LTFs</u>	<u>36.3.4.2</u>	<u>CFPASN:O</u> <u>CFPSEC:O</u> <u>CFTB:O</u>	<u>Yes <input type="checkbox"/> No <input type="checkbox"/></u> <u>N/A <input type="checkbox"/></u>

Annex C

(normative)

ASN.1 encoding of the MAC and PHY MIB

C.3 MIB detail

Change the text identified below in C.3:

```
dot11SecureLTFImplemented OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This is a capability variable.
Its value is determined by device capabilities.
This attribute, when true, indicates that a secure HE-LTF measurement
exchange protocol (see 11.21.6.4.5 (Secure HE LTF in the TB and non TB
ranging measurement exchange protocol(11az))) is implemented. The
capability is disabled otherwise."
REFERENCE "IEEE Std 802.11-2020 Subclause 11.21.6.4.5"
 ::= { dot11WirelessMgmtOptionsEntry 54 }
```

Annex AE

(informative)

SIR-based attack detection

Change Annex AE as follows:

The presence of attack will cause the receiver SINR drop. Given the measured noise floor, the SINR can map to a signal to interference ratio (SIR). In this annex, an analysis is shown to illustrate the impact of attack on SIR drop.

Assume that an attacker observes the Secure HE-LTF symbol for a duration of T_{ob} , referred to as the observation period; see Figure AE-1. The attacker can use these observations to generate an attack signal over the duration T_c , referred to as the computation period. Finally, the attacker will transmit the attack signal during the attack period, T_a , to create a false first path of arrival that has an earlier arrival time than the true first path of arrival.

Replace Figure AE-1 with the following figure:

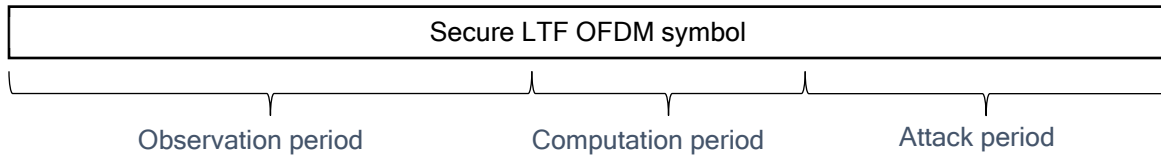


Figure AE-1—Attacking secure HE-LTF symbols

A side effect of creating the false first path of arrival is that the attacker will also generate interference at the intended receiver. If we assume that the attack signal has a correlation of ρ with the true Secure HE-LTF signal and creates a false first path of arrival with a relative power level of FFP (dB), then the signal-to-interference ratio (SIR) that is seen by the intended receiver will be:

$$SIR(\text{dB}) = -FFP(\text{dB}) + 10 \log_{10}(\rho^2 T_a) - 10 \log_{10}(1 - \rho^2 T_a)$$

When an attacker is present, the interference introduced by the attacker will lead to an SIR drop and the value will depend on the relative power level of FFP , correlation, and attack period.

For example, if $FFP = -10$ dB, then the expected SIR levels for different values of ρ and T_a are shown in the Figure AE-2.

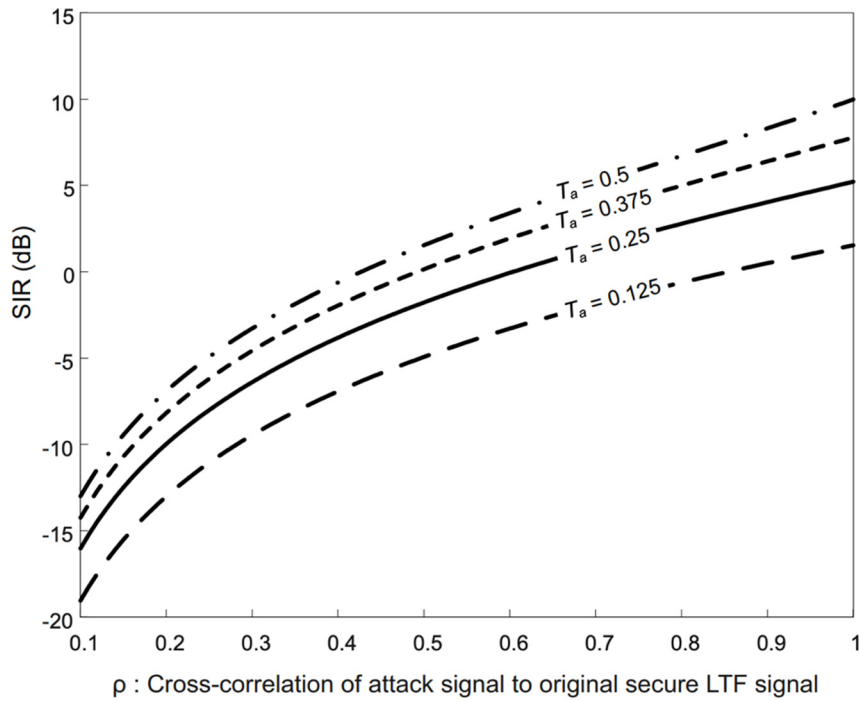


Figure AE-2—Received SIR after attack

From this figure, ~~we see~~ it can be seen that as the correlation of the attack signal decreases or the attack duration decreases, the SIR will drop even further.

Therefore, the presence of an attacker can be detected by looking for drops in the SIR over a single, or multiple, HE-LTF repetitions. The exact details of the algorithm are left to the implementer.



RAISING THE WORLD'S STANDARDS

Connect with us on:



Facebook: facebook.com/ieeesa



LinkedIn: linkedin.com/groups/1791118



Beyond Standards blog: beyondstandards.ieee.org



YouTube: youtube.com/ieeesa

standards.ieee.org

Phone: +1 732 981 0060