

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 2: MAC Enhancements for Robust Audio Video Streaming

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.11aaTM-2012
(Amendment to
IEEE Std 802.11TM-2012,
as amended by IEEE Std 802.11aeTM-2012)

29 May 2012

IEEE Std 802.11aa™-2012
(Amendment to
IEEE Std 802.11™-2012,
as amended by IEEE Std 802.11ae™-2012)

**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 2: MAC Enhancements for Robust Audio Video Streaming

Sponsor

**LAN/MAN Standards Committee
of the
IEEE Computer Society**

Approved 29 March 2012

IEEE-SA Standards Board

Abstract: This amendment specifies enhancements to the IEEE 802.11 medium access control (MAC) for robust audio video (AV) streaming, while maintaining coexistence with other types of traffic.

Keywords: audio, IEEE 802.11aa, medium access control, video, wireless LAN

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

Copyright © 2012 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 29 May 2012. 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.

Print: ISBN 978-0-7381-7260-6 STD97235
PDF: ISBN 978-0-7381-7366-5 STDPD97235

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.

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. 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.

Use of an IEEE Standard is wholly voluntary. IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "**AS IS.**"

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. Every IEEE standard is subjected to review at least every ten years. When a document is more than ten 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 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 his or her 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.

Translations: The IEEE consensus development 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 should be considered the approved IEEE standard.

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 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 his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on Standards: Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide 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 to ensure 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 Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at <http://standards.ieee.org/develop/wg/>.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Notice to users

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 imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable 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.

Copyrights

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards 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. 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 the [IEEE-SA website](#) or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit the [IEEE-SA website](#).

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

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. 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 <http://standards.ieee.org/about/sasb/patcom/patents.html>. 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 nondiscriminatory. 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.

Participants

At the time this amendment was sent to sponsor ballot, the IEEE 802.11 Working Group had the following officers:

Bruce P. Kraemer, *Chair*
Adrian P. Stephens and **Jon Walter Rosdahl**, *Vice-Chairs*
Stephen McCann, *Secretary*
Peter Ecclesine, *Technical Editor*

The following were officers of Task Group aa:

Graham K. Smith, *Chair*
Alex Ashley, *Vice-Chair*
Ganesh Venkatesan, *Secretary*
Alex Ashley, *Technical Editor*

When the IEEE 802.11 Working Group first approved this amendment, Task Group aa had the following membership:

Ganesh Venkatesan, *Chair*
Alex Ashley, *Vice Chair*
Hang Lui, *Technical Editor*

Osama S. Aboul-Magd
Santosh P. Abraham
Carlos H. Aldana
David C. Andrus
Lee R. Armstrong
Yusuke Asai
Geert A. Awater
David Bagby
Michael Bahr
Gabor Bajko
Raja Banerjea
Kaberi Banerjee
John R. Barr
Gal Basson
Tuncer Baykas
John L. Benko
Ted Booth
Daniel Borges
Andre Bourdoux
Gregory Breit
Walter Buga
G. Bumiller
Nancy Cam-Winget
Necati Canpolat
Laurent Cariou
Philippe Chambelin
Kapseok Chang
Clint F. Chaplin
Lidong Chen
Minho Cheong
Woong Cho
Chang-Soon Choi
Inhwan Choi
In-Kyeong Choi
Jee-Yon Choi
Liwen Chu

John Coffey
Charles I. Cook
Carlos Cordeiro
Xavier P. Costa
Subir Das
Rolf J. de Vegt
Theodorus Denteneer
Susan Dickey
John Dorsey
Offie Drennan
Roger P. Durand
Donald E. Eastlake
Marc Emmelmann
Vinko Erceg
Leonardo Estevez
Matthew J. Fischer
Wayne K. Fisher
Atsushi Fujimoto
Wen Gao
Matthew Gast
James P. Gilb
Jeffrey Gilbert
Claude Giraud
Ronald Glibbery
Reinhard Gloger
Michelle Gong
David Goodall
Sudheer A. Grandhi
Michael Grigat
Mark Grodzinsky
David Halasz
Mark Hamilton
Christopher J. Hansen
Hiroshi Harada
Dan N. Harkins
Brian D. Hart

Chris Hartman
Amer A. Hassan
Robert F. Heile
Guido R. Hiertz
Garth D. Hillman
Seungeun Hong
Ju-Lan Hsu
Wendong Hu
Tian-Wei Huang
David Hunter
Brima Ibrahim
Akio Iso
Wynona Jacobs
Avinash Jain
Lusheng Ji
Sunggeun Jin
Junho Jo
Vince Jones
Padam Kafle
Carl W. Kain
Naveen K. Kakani
Jeyhan Karaoguz
Assaf Y. Kasher
Shuzo Kato
Tatsuya Kato
Richard H. Kennedy
John Kenney
Stuart J. Kerry
Eung S. Kim
Joonsuk Kim
Kyeongpyo Kim
Yongsun Kim
Youhan Kim
Youngsoo Kim
Yunjoo Kim
Shoichi Kitazawa

Jarkko Knecht
Marm M. Kobayashi
Fumihide Kojima
Tom Kolze
Thomas M. Kurihara
Joseph Kwak
Hyoungjin Kwon
Ui K. Kwon
Ismail Lakkis
Paul Lambert
Zhou Lan
Leonardo Lanante
Jeremy A. Landt
Joseph P. Lauer
Jae S. Lee
Wooyong Lee
Yuro Lee
Pei Liu
Peter Loc
Artyom Lomayev
Hui-Ling Lou
Bradley Lynch
Michael Lynch
Alastair Malarky
Jouni K. Malinen
Alexander Maltsev
Hiroshi Mano
Bill Marshall
Roman M. Maslennikov
Justin P. McNew
Murat Mese
Sven Mesecke
Robert R. Miller
Jochen Miroll
Apurva Mody
Michael Montemurro
Rajendra T. Moorti
Hitoshi Morioka
Yuichi Morioka
Daniel C. Mur
Anthony Murabito
Peter Murray
Andrew Myles
Yuhei Nagao
Hiroki Nakano
Sai S. Nandagopalan
Chiu Ngo

Paul Nikolich
Yujin Noh
Jong-Ee Oh
Youko Omori
Satoshi Oyama
Richard H. Paine
Jaewoo Park
Minyoung Park
Bemini H. Peiris
Eldad Perahia
James E. Petranovich
Albert Petrick
John Petro
Vishakan Ponnampalam
James D. Portaro
Henry S. Ptasinski
Rene Purnadi
Ivan Pustogarov
Emily H. Qi
Huyu Qu
Jim E. Raab
Mohammad Rahman
Harish Ramamurthy
Stephen G. Rayment
Ivan Reede
Alex Reznik
Sandrine Roblot
Randal Roebuck
Richard Roy
Ali Sadri
Kazuyuki Sakoda
Hemant Sampath
Hirokazu Sawada
Jean Schwoerer
Yongho Seok
Huairong Shao
Stephen J. Shellhammer
Bazhong Shen
Ian Sherlock
Nobuhiko Shibagaki
Ashish Shukla
Francois Simon
Shubhranshu Singh
Sudhir Srinivasa
Robert Stacey
Dorothy Stanley

David S. Stephenson
John Stine
Guenael T. Strutt
Chin-Sean Sum
Mohammad H. Taghavi
Mineo Takai
Yasushi Takatori
Teik-Kheong Tan
Alireza Tarighat
Geoffrey Thompson
Allan Thomson
Jerry Thrasher
Eric Tokubo
Ichihiko Toyoda
Jason Trachewsky
Solomon B. Trainin
Jean Tsao
Yung-Szu Tu
Masahiro Umehira
Richard D. Van Nee
Allert Van Zelst
Prabodh Varshney
Sameer Vermani
George A. Vlantis
Jesse R. Walker
Chao-Chun Wang
Haiguang Wang
Junyi Wang
Qi Wang
Craig D. Warren
Fujio Watanabe
Menzo M. Wentink
Pyo C. Woo
James Worsham
Harry R. Worstell
Fonchi Wu
Liuyang Yang
James Yee
Peter Yee
Su K. Yong
Christopher Young
Artur Zaks
Hongyuan Zhang
Ning Zhang
Meiyuan Zhao
Shiwei Zhao
Chunhui Zhu

Major contributions were received from the following individuals:

Osama Aboul-Magd
Alex Ashley
Yonghwan Bang
Matilda Benveniste
Douglas Chan
Liwen Chu
Todor Cooklev
Yacine Ghamri Doudane
Mark Hamilton
Dan N. Harkins
Brian D. Hart
David Hunter
Naveen K. Kakani

Jun Li
Hang Liu
Xiaojun Ma
Ishan Mandrekar
Bill Marshall
Saurabh Mathur
Jochen Miroll
Andrew Myles
Sanjiv Nanda
Ivan Pustogarov
Satish Putta
Luke Qian
Raghuram Rangarajan

Ed Reuss
Kevin Rhee
Alexander Safonov
John Simons
Graham K. Smith
Robert Stacey
Rohit Suri
Allan Thomson
Ganesh Venkatesan
George A. Vlantis
Qi Wang
Mingquan Wu
Jing Zhu

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

Tomoko Adachi	David Hunter	Brian Phelps
Iwan Adhicandra	Tetsushi Ikegami	Clinton Powell
Thomas Alexander	Noriyuki Ikeuchi	Venkatesha Prasad
Richard Alfvn	Yasuhiko Inoue	Michael Probasco
Mark Anderson	Sergiu Iordanescu	Henry S. Ptasinski
Butch Anton	Akio Iso	Jayaram Ramasastry
Lee R. Armstrong	Atsushi Ito	Ivan Reede
Alex Ashley	Mitsuru Iwaoka	Maximilian Riegel
Arthur Astrin	Raj Jain	Robert Robinson
Kwok Shum Au	Junghoon Jee	Jon Rosdahl
Michael Bahr	Tal Kaitz	Randall Safier
Nancy Bravin	Naveen K. Kakani	Shigenobu Sasaki
John Buffington	Shinkyō Kaku	Bartien Sayogo
William Byrd	Ruediger Kays	Shusaku Shimada
William Carney	Stuart J. Kerry	John Short
Clint F. Chaplin	Brian Kiernan	Gil Shultz
Keith Chow	Yongbum Kim	Graham K. Smith
Charles I. Cook	Youhan Kim	Kapil Sood
Ray Davis	Bruce P. Kraemer	Robert Stacey
Wael Diab	Thomas M. Kurihara	Dorothy Stanley
Patrick Diamond	Geoff Ladwig	Kevin B. Stanton
Thomas Dineen	Richard Lancaster	Thomas Starai
Sourav Dutta	Jeremy A. Landt	Adrian P. Stephens
Peter Ecclesine	Jan-Ray Liao	Walter Struppler
Richard Eckard	Arthur Light	Guenaël T. Strutt
Richard Edgar	William Lumpkins	Mark Sturza
Dennis Edwards	Greg Luri	Bo Sun
Matthew J. Fischer	Elvis Maculuba	Joseph Tardo
Andre Fournier	Jouni K. Malinen	Michael Johas Teener
Avraham Freedman	Stephen McCann	Ichihiko Toyoda
Geoffrey Garner	Michael McInnis	Solomon B. Trainin
Matthew Gast	Gary Michel	Mark-Rene Uchida
Pieter-Paul Giesberts	Apurva Mody	Dmitri Varsanofiev
Gregory Gillooly	Michael Montemurro	Prabodh Varshney
Reinhard Gloger	Rick Murphy	Ganesh Venkatesan
David Goodall	Peter Murray	John Vergis
Sudheer A. Grandhi	Nabil Nasser	Bhupender Virk
Randall Groves	Michael S. Newman	George A. Vlantis
Michael Gundlach	Paul Nikolich	Khurram Waheed
C. Guy	Kevin Noll	Lei Wang
Rainer Hach	John Notor	Stanley Wang
Mark Hamilton	Satoshi Obara	Stephen Webb
Rodney Hemminger	Robert O'Hara	Karl Weber
Jerome Henry	Satoshi Oyama	Hung-Yu Wei
Marco Hernandez	Stephen Palm	Oren Yuen

When the IEEE-SA Standards Board approved this amendment on 29 March 2012, it had the following membership:

Richard H. Hulett, *Chair*
John Kulick, *Vice Chair*
Robert M. Grow, *Past Chair*
Judith Gorman, *Secretary*

Satish Aggarwal
Masayuki Ariyoshi
Peter Balma
William Bartley
Ted Burse
Clint Chaplin
Wael Diab
Jean-Philippe Faure

Alexander Gelman
Paul Houzé
Jim Hughes
Young Kuyn Kim
Joseph L. Koepfinger*
David J. Law
Thomas Lee
Hung Ling

Oleg Logvinov
Ted Olsen
Gary Robinson
Jon Walter Rosdahl
Mike Seavey
Yatin Trivedi
Phil Winston
Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Lisa Perry
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of IEEE Std 802.11aa-2012, 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 2: MAC Enhancements for Robust Audio Video Streaming.

This amendment defines enhancements to the IEEE 802.11 medium access control (MAC) to support robust audio video (AV) streaming.

The amendment specifies enhancements to the following standard and amendment to support robust AV streaming:

- IEEE Std 802.11-2012
- IEEE Std 802.11ae-2012

Contents

1.	Overview	2
1.3	Supplementary information on purpose	2
2.	Normative references	2
3.	Definitions, acronyms, and abbreviations	2
3.1	Definitions	2
3.2	Definitions specific to IEEE 802.11	2
3.3	Abbreviations and acronyms	3
4.	General description	4
4.3	Components of the IEEE 802.11 architecture	4
4.3.15	Mesh BSS: IEEE 802.11 wireless mesh network	4
4.3.16	Robust audio video (AV) streaming	4
5.	MAC service definition	6
5.1	Overview of MAC services	6
5.1.1	Data service	6
6.	Layer management	7
6.3	MLME SAP interface	7
6.3.3	Scan	7
6.3.26	TS management interface	7
6.3.29	Block Ack	13
6.3.67	DMS or GCR request and response procedure	16
6.3.72	QoS Map Set element management	21
6.3.84	SCS request and response procedure	22
6.3.85	QLoad report management	27
6.3.86	HCCA TXOP advertisement management	31
6.3.87	Group membership management	35
6.3.88	AP PeerKey management	39
8.	Frame formats	41
8.2	MAC frame formats	41
8.2.4	Frame fields	41
8.3	Format of individual frame types	42
8.3.1	Control frames	42
8.3.2	Data frames	45
8.3.3	Management frames	46
8.4	Management frame body components	46
8.4.1	Fields that are not information elements	46
8.4.2	Information elements	48
8.5	Action frame format details	62
8.5.3	QoS Action frame details	62
8.5.5	Block Ack Action frame details	65
8.5.8	Public Action details	66

8.5.11	Protected Dual of Public Action frames	70
8.5.14	WNM Action details	70
8.5.16	Self-protected Action frame details	71
8.5.19	Robust AV Streaming Action frame details	72
9.	MAC sublayer functional description	75
9.2	MAC architecture	75
9.2.4	Hybrid coordination function (HCF)	75
9.3	DCF	76
9.3.2	Procedures common to the DCF and EDCAF	76
9.3.6	Group addressed MPDU transfer procedure	77
9.4	PCF	78
9.4.3	PCF access procedure	78
9.4.4	PCF transfer procedure	78
9.7	Multirate support	79
9.7.5	Rate selection for data and management frames	79
9.9	HT Control field operation	79
9.11	A-MSDU operation	79
9.19	HCF	79
9.19.2	HCF contention-based channel access (EDCA)	79
9.19.3	HCCA	83
9.21	Block Acknowledgment (Block Ack)	84
9.21.2	Setup and modification of the Block Ack parameters	84
9.21.3	Data and acknowledgment transfer using immediate Block Ack policy and delayed Block Ack policy	84
9.21.5	Teardown of the Block Ack mechanism	85
9.21.6	Selection of BlockAck and BlockAckReq variants	85
9.21.10	GCR Block Ack	85
9.26	PSMP Operation	88
9.26.1	Frame transmission mechanism during PSMP	88
10.	MLME	88
10.2	Power management	88
10.2.1	Power management in an infrastructure network	88
10.4	TS operation	93
10.4.1	Introduction	93
10.4.4	TS setup	93
10.4.8	Data transfer	95
10.5	Block Ack operation	95
10.5.2	Setup and modification of the Block Ack parameters	95
10.5.4	Error recovery upon a peer failure	96
10.18	RSNA A-MSDU procedures	96
10.23	Wireless network management procedures	96
10.23.15	Group addressed transmission service DMS procedures	96
10.25	Quality-of-service management frame (QMF)	107
10.25.2	QMF policy advertisement and configuration procedures	107
10.26	Robust AV streaming	108
10.26.1	Robust AV streaming dependencies	108
10.26.2	SCS procedures	108
10.27	Procedures to manage OBSS	109
10.27.1	General	109
10.27.2	QLoad Report element	110

10.27.3	HCCA TXOP negotiation	112
10.27.4	HCCA AP timing synchronization for HCCA TXOP advertisement	116
11.	Security	117
11.8	Per-frame pseudo-code	117
11.8.2	RSNA frame pseudo-code	117
11.10	AP PeerKey support	118
11.10.1	AP PeerKey overview	118
11.10.2	AP PeerKey protocol	119
	Annex B (normative) Protocol Implementation Conformance Statement (PICS) proforma.....	121
B.2	Abbreviations and special symbols	121
B.2.2	General abbreviations for Item and Support columns	121
B.4	PICS proforma—IEEE Std 802.11-2012.....	121
B.4.3	IUT configuration	121
B.4.25	RobustAVT extensions.....	121
	Annex C (normative) ASN.1 encoding of the MAC and PHY MIB	123
	Annex X (informative) Overlapping BSS (OBSS) management	135
X.1	Introduction	135
X.2	QLoad Report element.....	135
X.2.1	General.....	135
X.2.2	Calculating medium time.....	136
X.2.3	Calculation of potential traffic self.....	136
X.2.4	Calculation of allocated traffic self	138
X.2.5	Calculation of allocated traffic shared	139
X.2.6	Calculation of EDCA Access Factor	139
X.2.7	EDCA Overhead Factor.....	140
X.2.8	Calculation of HCCA Access Factor	141
X.3	Channel selection using QLoad report	141
X.3.1	General.....	141
X.3.2	AP with admission control mandatory	141
X.3.3	AP with an HC.....	142
X.3.4	Channel selection procedures	142
X.4	Sharing in an OBSS situation	143
X.4.1	General.....	143
X.4.2	Sharing schemes	144
X.5	Mitigating consequences of OBSS sharing in presence of noncollaborating devices.....	146

Tables

Table 6-1—Supported TS management primitives	7
Table 8-16—BlockAckReq frame variant encoding	43
Table 8-18—BlockAck frame variant encoding.....	44
Table 8-20—Beacon frame body.....	46
Table 8-27—Probe Response frame body	46
Table 8-37—Status codes	46
Table 8-38—Category values	47
Table 8-54—Element IDs.....	48
Table 8-101—AKM suite selectors	48
Table 8-103—Capabilities field.....	49
Table 8-110—Setting of Schedule subfield.....	50
Table 8-170—Optional Subelement IDs for DMS Descriptor	52
Table 8-170a—GATS Retransmission Policy field values	52
Table 8-170b—GCR Delivery Method field values.....	53
Table 8-171—Response Type field values	53
Table 8-172—Optional Subelement IDs for DMS Status	54
Table 8-183a—Request Type definitions	57
Table 8-183b—Optional Subelement IDs for SCS Descriptor element	57
Table 8-183c—Sharing Policy definitions	59
Table 8-183d—Optional Subelement IDs for QLoad Report element	59
Table 8-183e—Protocol ID definitions	61
Table 8-192—QoS Action field values	62
Table 8-193—ADDTs Request frame Action field format.....	62
Table 8-194—ADDTs Response frame Action field format	63
Table 8-197—QoS Map configure frame body.....	63
Table 8-197a—ADDTs Reserve Request frame Action field format	64
Table 8-197b—ADDTs Reserve Response frame Action field format	64
Table 8-203—ADDBA Request frame Action field format.....	65
Table 8-204—ADDBA Response frame Action field format	65
Table 8-205—DELBA frame Action field values	66
Table 8-210—Public Action field values	66
Table 8-221b—QLoad Report frame Action field format.....	67
Table 8-221a—QLoad Request frame Action field format	67
Table 8-228—Public Action field values defined for Protected Dual of Public Action frames.....	70
Table 8-221c—Request Type definitions	70
Table 8-262—Mesh Peering Open frame Action field format	71
Table 8-263—Mesh Peering Confirm frame Action field format	71
Table 8-264—Mesh Peering Close frame Action field format.....	72
Table 8-281a—Robust AV streaming Robust Action field values.....	72
Table 8-502d—Group Membership Request frame Action field format.....	74
Table 9-1—UP-to-AC mappings	75
Table 10-1—Power Management modes	89
Table 10-2—Types of Block Ack agreement based on capabilities and ADDBA conditions	96
Table 10-9a—STA recovery procedures for a changed retransmission policy	104
Table 10-9b—Non-AP STA recovery procedures for a changed delivery method.....	105
Table 10-14—Contents of HCCA TXOP Response frame	115

Figures

Figure 6-25—DMS or GCR setup protocol exchange.....	16
Figure 6-25a—Example SCS setup and termination protocol exchange	22
Figure 8-20—BAR Control field.....	42
Figure 8-5—HT Control field.....	42
Figure 8-23a—BAR Information field format (GCR BlockAckReq).....	43
Figure 8-24—BA Control field.....	44
Figure 8-28a—BA Information field format (GCR BlockAck).....	45
Figure 8-80a—TXOP Reservation field format	47
Figure 8-346a—GCR Request subelement field format.....	52
Figure 8-348a—GCR Response subelement field format	55
Figure 8-401d—Intra-Access Category Priority element format	55
Figure 8-401e—Intra-Access Priority field format	56
Figure 8-401f—SCS Descriptor element format.....	56
Figure 8-401g—QLoad Report element format	58
Figure 8-401h—QLoad field format.....	59
Figure 8-401i—HCCA TXOP Update Count element format	60
Figure 8-104j—Higher Layer Stream ID element format	60
Figure 8-401k—GCR Group Address element format.....	61
Figure 8-460c—HCCA TXOP Advertisement frame Action field format.....	68
Figure 8-460d—HCCA TXOP Response frame Action field format.....	68
Figure 8-460e—Public Key frame body format	69
Figure 8-502a—SCS Request frame Action field format.....	73
Figure 8-502b—SCS Response frame Action field format.....	73
Figure 8-502c—SCS Status dupe format	73
Figure 8-502e—Group Membership Response frame Action field format.....	74
Figure 9-19—Reference implementation model when dot11AlternateEDCAActivated is false or not present.....	79
Figure 9-19a—Reference implementation model when dot11AlternateEDCAActivated is true.....	80
Figure 9-28a—Example of a frame exchange with GCR Block Ack retransmission policy	87
Figure 10-8a—TS setup when initiated by the AP	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 2: MAC Enhancements for
Robust Audio Video Streaming**

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

(This amendment is based on IEEE Std 802.11™-2012, as amended by IEEE Std 802.11ae-2012.)

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 ~~strike through~~ (to remove old material) and underscore (to add new material). **Delete** removes existing material. **Insert** adds new material without disturbing the existing material. Deletions and 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.¹

¹Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard

1. Overview

1.3 Supplementary information on purpose

Insert the following list item at the end of the dashed list in 1.3:

- Defines mechanisms to improve audio video (AV) streaming quality of service (QoS) while maintaining data and voice performance.

2. Normative references

Insert the following reference into Clause 2 in alphanumeric order:

IEEE Std 802.1Q™-2011, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks.^{2,3}

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Change the definition of service period in 3.1 as follows:

service period (SP): A contiguous time during which one or more downlink unicast frames are transmitted to a quality of service (QoS) station (STA) and/or one or more transmission opportunities (TXOPs) are granted to the same STA. SPs can be scheduled or unscheduled. For a non-access point (non-AP) STA, there can be at most one nongroupcast with retries SP (non-GCR-SP) active at any time.

3.2 Definitions specific to IEEE 802.11

Insert the following definitions into 3.2 in alphabetic order:

advanced groupcast with retries (GCR): A set of features comprising the GCR block acknowledgment retransmission policy and the GCR service period (GCR-SP) delivery method.

concealed groupcast with retries (GCR) frame: A group addressed frame that is transmitted using the aggregate medium access control (MAC) service data unit (A-MSDU) frame format with the destination address (DA) field set to the GCR concealment address.

group addressed transmission service (GATS): A mechanism comprising directed multicast service (DMS) and groupcast with retries (GCR), for delivery of group addressed frames.

groupcast with retries (GCR) active (GCR-A) delivery: A delivery method for a group addressed stream subject to a GCR agreement wherein the frames may be transmitted without regard to the power state of non-access point (non-AP) stations (STAs).

²The IEEE standards or products referred to in this clause are trademarks owned by The Institute of Electrical and Electronics Engineers, Inc.

³IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

groupcast with retries (GCR) concealment address: A medium access control (MAC) address that is used to prevent group addressed frames transmitted via the GCR unsolicited retry or GCR Block Ack retransmission policies from being passed up the medium access control service access point (MAC_SAP) of GCR-incapable stations (STAs).

groupcast with retries (GCR) frame: A group addressed frame subject to a GCR agreement between the access point (AP) and at least one station (STA) within the infrastructure basic service set (BSS) or between peer mesh STAs in a mesh BSS.

groupcast with retries (GCR) group address: A group address subject to a GCR agreement between the access point (AP) and at least one station (STA) within the basic service set (BSS) or between peer mesh STAs in a mesh BSS.

groupcast with retries (GCR) service: A means for transmission and retransmission of medium access control (MAC) service data units (MSDUs) to a destination that is a group address. The GCR service provides greater reliability by using group addressed retransmissions, concealed from GCR-incapable stations (STAs).

groupcast with retries (GCR) service period (GCR-SP) aggregate medium access control (MAC) service data unit (A-MSDU): An A-MSDU subject to the GCR service with delivery method equal to GCR-SP.

groupcast with retries (GCR) service period (GCR-SP) frame: A frame subject to the GCR service when delivery method is GCR-SP.

groupcast with retries (GCR) service period (GCR-SP) medium access control (MAC) service data unit (MSDU): An MSDU subject to the GCR service with delivery method equal to GCR-SP.

groupcast with retries (GCR) transmission opportunity (TXOP): An interval of time when an access point (AP) or a mesh station (STA) has the right to initiate frame exchange sequences onto the wireless medium (WM) for the purpose of transmitting multiple frames that are subject to the GCR service.

no acknowledgment/no retry (No-Ack/No-Retry): A retransmission policy for group addressed frames in which each frame is transmitted once and without acknowledgment.

nonconcealed groupcast with retries (GCR) frame: A group addressed frame that is not transmitted to the GCR concealment address.

nongroupcast with retries (non-GCR): A method for delivering group addressed frames without using the GCR unsolicited retry retransmission policy, the GCR block acknowledgment retransmission policy, or the GCR service period (GCR-SP) delivery method.

nongroupcast with retries service period (non-GCR-SP): A method for the delivery of group addressed frames without the use of a GCR service period (GCR-SP).

3.3 Abbreviations and acronyms

Insert the following abbreviations into 3.3 in alphabetic order:

AV	audio visual
GATS	group addressed transmission service
GCR	groupcast with retries
GCR-SP	groupcast with retries service period

DEI	drop eligibility indicator
QLDRC	QoS long drop-eligible retry counter
QSDRC	QoS short drop-eligible retry counter
SCS	stream classification service
SCSID	stream classification service identifier

4. General description

4.3 Components of the IEEE 802.11 architecture

4.3.15 Mesh BSS: IEEE 802.11 wireless mesh network

4.3.15.3 Mesh STA

Change 4.3.15.3 as follows:

A STA that belongs to a mesh BSS is termed a “mesh station” (mesh STA). Mesh STAs are QoS STAs that support mesh services, i.e., they participate in formation and operation of a mesh basic service set (MBSS). A mesh STA implements a subset of the QoS functionality. This subset is as follows:

- Use of QoS frame format
- EDCA (as a part of MCF)
- Block acknowledgment (optional)
- No acknowledgment (optional)
- Use of TSPEC, TCLAS, and TCLAS Processing elements to establish DMS or GCR agreements (optional)

A mesh BSS does not incorporate the full hybrid coordinator (HC) and BSS QoS functionality. MBSSs do not incorporate the following:

- HCCA
- ~~Traffic specification (TSPEC)~~
- Traffic stream (TS) management
- Admission control
- Automatic power save delivery (APSD)
- Direct-link setup (DLS)
- Tunneled direct-link setup (TDLS)

Insert the following subclauses, 4.3.16 to 4.3.16.5, after 4.3.15.3.13:

4.3.16 Robust audio video (AV) streaming

Robust AV streaming improves AV streaming performance when using IEEE 802.11 for consumer and enterprise applications.

4.3.16.1 Groupcast with retries (GCR)

The GCR service allows a STA to request greater reliability for one or more group addressed streams that the STA receives. Greater reliability is provided via unsolicited retries or the Block Ack mechanism. A non-AP STA may request delivery so that the AP transmits the frames via EDCA within GCR service periods when all associated non-AP STAs are in active mode or the Awake state of the PS mode.

4.3.16.2 Stream classification service (SCS)

SCS enables the establishment of a classification using layer 2 and/or layer 3 signaling to match incoming unicast MSDUs. Once classified, unicast MSDUs matching the classification are assigned to an access category and are tagged with their drop eligibility. When intra-access category prioritization is enabled (see 4.3.16.5), SCS allows MSDUs matching the classification to be assigned to the primary or alternate transmit queues so that finer grained prioritization can be applied.

4.3.16.3 Overlapping BSS (OBSS) management

The objective of OBSS management is to facilitate cooperative sharing of the medium between APs that operate in the same channel and that are able to receive or obtain frames from each other, including Beacon frames. These frames might be received directly or via associated STAs that support the Beacon request capability (see 10.11.10).

OBSS management provides the means to

- Provide additional information for channel selection
- Extend the admission control mechanism to a distributed environment
- Enable the coordination of scheduled TXOPs between OBSSs

OBSS management enables stationary and portable APs to provide to neighboring APs information for the selection of a channel and for the cooperative sharing of that channel. The main component of OBSS management is the QLoad report that provides information on

- The reporting AP's overlap situation
- The reporting AP's QoS traffic load
- The total QoS traffic load of BSSs directly overlapping the reporting AP's BSS

This information might be used to aid an AP when searching for a channel and also when sharing a channel in an overlap situation.

To coordinate the TXOPs of overlapping HCCA APs, OBSS management provides a means for an AP to advertise its TXOP allocations so another AP might schedule its own TXOPs to avoid those already scheduled.

4.3.16.4 Interworking with IEEE 802.1Q Stream Reservation Protocol (SRP)

Support for SRP from IEEE Std 802.1Q-2011 enables integration of the TSPEC ADDTS request/response protocol with IEEE 802.1Q SRP to enable end-to-end SRP reservations when one or more IEEE 802.11 links are part of a path from IEEE 802.1Q Talker to IEEE 802.1Q Listener.

4.3.16.5 Intra-access category prioritization

Intra-access category prioritization provides six transmit queues that map to four enhanced distributed channel access functions (EDCAFs) to enable differentiation between traffic streams that are in the same access category in order for finer grained prioritization to be applied between individual AV streams or voice streams.

5. MAC service definition

5.1 Overview of MAC services

5.1.1 Data service

5.1.1.2 Determination of UP

Change 5.1.1.2 as follows:

The QoS facility supports eight priority values, referred to as UPs. The values a UP may take are the integer values from 0 to 7 and are identical to the IEEE 802.1D priority tags. An MSDU with a particular UP is said to belong to a traffic category (TC) with that UP. The UP is provided with each MSDU at the medium access control service access point (MAC_SAP) either directly, in the UP parameter, or indirectly, in a TSPEC or SCS Descriptor element designated by the UP parameter.

5.1.1.5 Interpretation of service class parameter in MAC service primitives in a STA

Change 5.1.1.5 as follows:

In QoS STAs, the value of the service class parameter in the MAC service primitive (see 5.2) may be a noninteger value of QoSAck or QoSNoAck.

When an MSDU is received from the MAC_SAP and the recipient STA is a QoS STA with the service class set to

- QoSAck, the MSDU is transmitted using a QoS data frame with the Ack Policy subfield in the QoS Control field set to either Normal Ack (normal acknowledgment) or Block Ack.
- QoSNoAck, the MSDU is transmitted using a QoS data frame with the Ack Policy subfield in the QoS Control field set to No Ack (no acknowledgment). ~~If the sender STA is contained within an AP and the frame has a group DA, then the MSDU is buffered for transmission and is also sent to the DS.~~

If the sender STA is an AP and the frame has a group DA that is not the GCR concealment address, then the MSDU is buffered for transmission and is also sent to the DS.

When an MSDU is received from the MAC_SAP and the recipient STA is not a QoS STA, the MSDU is transmitted using a non-QoS data frame.

When a QoS data frame is received from another STA, the service class parameter in the MA-UNITDATA.indication primitive is set to

- QoSAck, if the frame is a QoS data frame with the Ack Policy subfield in the QoS Control field equal to either Normal Ack or Block Ack.
- QoSAck, if the frame was delivered via the DMS or the GCR Block Ack retransmission policy.
- QoSNoAck, if the frame is a QoS data frame with the Ack Policy subfield in the QoS Control field equal to No Ack. This service class is also used ~~where~~ when the DA parameter is a group address unless the frame was delivered via DMS or the GCR Block Ack retransmission policy.

When a non-QoS data frame is received from a STA, the service class parameter in the MA-UNITDATA.indication primitive is set to

- QoSAck, if the frame is an individually addressed frame and is acknowledged by the STA.
- QoSNoAck, if the frame is a group addressed frame and is not acknowledged by the STA.

Note that the group addressed frames sent by a non-QoS STA are not acknowledged regardless of the value of the service class parameter in the MA-UNITDATA.indication primitive.

NOTE—GCR frames are transmitted only by an AP for which dot11GCRActivated is true or by a mesh STA for which dot11MeshGCRActivated is true.

6. Layer management

6.3 MLME SAP interface

6.3.3 Scan

6.3.3.3 MLME-SCAN.confirm

6.3.3.3.2 Semantics of the service primitive

Insert the following row at the end of the untitled table describing BSSDescriptions in 6.3.3.3.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description	IBSS adoption
QLoad Report	As defined in frame format	As defined in 8.4.2.125	The values from the QLoad Report element if such an element was present in the probe response frame, else null.	Do not adopt.

6.3.26 TS management interface

6.3.26.1 General

Change Table 6-1 as follows:

Table 6-1—Supported TS management primitives

Primitive	Request	Confirm	Indication	Response
ADDTS	non-AP QoS STA	non-AP QoS STA	HC	HC
DELTS	non-AP QoS STA and HC	non-AP QoS STA and HC	non-AP QoS STA and HC	—
<u>ADDTSRESERVE</u>	<u>HC</u>	<u>HC</u>	<u>non-AP QoS STA</u>	<u>non-AP QoS STA</u>

6.3.26.2 MLME-ADDTS.request

6.3.26.2.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.26.2.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDTS.request(
    DialogToken,
    TSPEC,
    TCLAS,
    TCLASProcessing,
    ADDTSFailureTimeout,
    U-APSD Coexistence,
    EBR,
    IntraAccessCategoryPriority,
    HigherLayerStreamID,
    VendorSpecificInfo
)
```

Insert the following rows before the VendorSpecificInfo row of the untitled table in 6.3.26.2.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
IntraAccessCategoryPriority	Intra-Access Category Priority element	As defined in 8.4.2.123	Specifies the intra-AC priorities the STA should use.
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Identifies the higher layer stream.

6.3.26.3 MLME-ADDTS.confirm

6.3.26.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.26.3.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDTS.confirm(
    ResultCode,
    DialogToken,
    TSDelay,
    TSPEC,
    Schedule,
    TCLAS,
    TCLASProcessing,
    EBR,
    HigherLayerStreamID,
    VendorSpecificInfo
)
```


Insert the following row before the VendorSpecificInfo row of the untitled table in 6.3.26.3.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Identifies the higher layer stream.

6.3.26.4 MLME-ADDTS.indication

6.3.26.4.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.26.4.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDTS.indication (
    DialogToken,
    STAAddress,
    TSPEC,
    TCLAS,
    TCLASProcessing,
    U-APSD Coexistence,
    EBR,
    IntraAccessCategoryPriority,
    HigherLayerStreamID,
    VendorSpecificInfo
)
```

Insert the following rows before the VendorSpecificInfo row of the untitled table in 6.3.26.4.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
IntraAccessCategoryPriority	Intra-Access Category Priority element	As defined in 8.4.2.123	Specifies the intra-AC priorities the STA should use.
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Identifies the higher layer stream.

6.3.26.5 MLME-ADDTS.response

6.3.26.5.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.26.5.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDTS.response (
    ResultCode,
    DialogToken,
    STAAddress,
    TSDelay,
```

TSPEC,
Schedule,
TCLAS,
TCLASProcessing,
EBR,
HigherLayerStreamID,
VendorSpecificInfo
)

Insert the following row before the VendorSpecificInfo row in the untitled table in 6.3.26.5.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Identifies the higher layer stream.

Insert the following subclauses, 6.3.26.8 to 6.3.26.11.4, after 6.3.26.7.4:

6.3.26.8 MLME-ADDTSRESERVE.request

6.3.26.8.1 Function

This primitive request is used by the SME at the AP to start the AP-initiated TS setup procedure.

6.3.26.8.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-ADDTSRESERVE.request (
 TSPEC,
 HigherLayerStreamID,
 Schedule,
 VendorSpecificInfo
)

Name	Type	Valid range	Description
TSPEC	TSPEC element	As defined in 8.4.2.32	Specifies the QoS parameters of the TS.
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Stream identifier assigned by a higher layer protocol.
Schedule	Schedule element	As defined in 8.4.2.36	Specifies the schedule information, service start time, SI, and the specification interval.
VendorSpecificInfo	A set of elements	As defined in 8.4.2.28	Zero or more elements.

6.3.26.8.3 When generated

This primitive is generated by the SME at the AP to start the AP-initiated TS setup procedure. If the parameter validation on the parameters used in this primitive succeeds, an ADDTS Reserve Request action frame is transmitted from the AP to a non-AP STA.

6.3.26.8.4 Effect of receipt

The STA operates according to the procedures defined in 10.4.4.3.

6.3.26.9 MLME-ADDTSRESERVE.confirm**6.3.26.9.1 Function**

This primitive is an indication to the SME that is generated by the MLME as a result of receiving an ADDTS Reserve Response action frame from the non-AP STA to which the AP sent a corresponding ADDTS Reserve Request action frame.

6.3.26.9.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-ADDTSRESERVE.confirm (
    ResultCode,
    StreamID
)
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the results of the corresponding MLME-ADDTSReserve.request primitive.
StreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Stream identifier specified in the corresponding MLME-ADDTSReserve.request primitive.

6.3.26.9.3 When generated

This primitive is generated by the MLME as a result of receiving an ADDTS Reserve Response action frame from the non-AP STA to which the AP sent a corresponding ADDTS Reserve Request action.

6.3.26.9.4 Effect of receipt

The SME is notified of the results of the AP-initiated TS setup procedure.

6.3.26.10 MLME-ADDTSRESERVE.indication**6.3.26.10.1 Function**

This primitive reports to the non-AP STA's SME the initiation of AP-initiated TS setup procedure.

6.3.26.10.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-ADDTSRESERVE.indication (
    APAddress,
    TSPEC,
    Schedule,
    HigherLayerStreamID,
    VendorSpecificInfo
)
```

Name	Type	Valid range	Description
APAddress	MAC Address	—	Contains the MAC address of the AP initiating the TS setup procedure.
TSPEC	TSPEC element	As defined in 8.4.2.32	Specifies the QoS parameters of the TS.
Schedule	Schedule element	As defined in 8.4.2.36	Specifies the schedule information, service start time, SI, and the specification interval.
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Stream identifier in the received ADDTS Reserve Request action frame.
VendorSpecificInfo	A set of elements	As defined in 8.4.2.28	Zero or more elements.

6.3.26.10.3 When generated

This primitive is generated by the MLME at the non-AP STA as a result of the receipt of an ADDTS Reserve Request action frame from the AP to which the non-AP STA is associated.

6.3.26.10.4 Effect of receipt

The SME is notified of the receipt of the ADDTS Reserve Request action frame from the AP. This primitive solicits the SME to participate in the AP-initiated TS setup procedure.

The SME should operate according to the procedures defined in 10.4.4.3.

6.3.26.11 MLME-ADDTSRESERVE.response

6.3.26.11.1 Function

This primitive is used by a non-AP STA to indicate to the HC the completion of an AP-initiated TS setup procedure.

6.3.26.11.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-ADDTSRESERVE.response (
    HigherLayerStreamID,
    ResultCode,
    VendorSpecificInfo
)
```

Name	Type	Valid range	Description
HigherLayerStreamID	Higher Layer Stream ID element	As defined in 8.4.2.127	Stream identifier specified in the corresponding MLME-ADDTSReserve.indication primitive.
ResultCode	Enumeration	0 or 1 (as defined in Table 8-37)	Indicates the result of the AP-initiated TS setup procedure.
VendorSpecificInfo	A set of elements	As defined in 8.4.2.28	Zero or more elements.

6.3.26.11.3 When generated

This primitive is generated by the SME at the non-AP STA to indicate to a HC that the non-AP STA has setup a TS in response to a higher layer protocol.

6.3.26.11.4 Effect of receipt

The STA operates according to the procedures defined in 10.4.4.3.

6.3.29 Block Ack**6.3.29.2 MLME-ADDBA.request****6.3.29.2.2 Semantics of the service primitive**

Change the primitive parameter list in 6.3.29.2.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDBA.request(
    PeerSTAAddress,
    DialogToken,
    TID,
    BlockAckPolicy,
    BufferSize,
    BlockAckTimeout,
    ADDBAFailureTimeout,
    BlockAckStartingSequenceControl,
    GCRGroupAddress,
    VendorSpecificInfo
)
```

Insert the following row before the VendorSpecificInfo row in the untitled table in 6.3.29.2.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
GCRGroupAddress	GCR Group Address element	As defined in 8.4.2.128	Specifies the group address for which a Block Ack agreement is requested. If the element is present, a GCR Group Address element is included in the transmitted ADDBA Request frame.

6.3.29.3 MLME-ADDDBA.confirm

6.3.29.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.29.3.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDDBA.confirm(
    PeerSTAAddress,
    DialogToken,
    TID,
    ResultCode,
    BlockAckPolicy,
    BufferSize,
    BlockAckTimeout,
    GCRGroupAddress,
    VendorSpecificInfo
)
```

Insert the following row before the VendorSpecificInfo row in the untitled table in 6.3.29.3.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
GCRGroupAddress	GCR Group Address element	As defined in 8.4.2.128	Specifies the group address for which a Block Ack agreement was requested.

6.3.29.4 MLME-ADDDBA.indication

6.3.29.4.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.29.4.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDDBA.indication(
    PeerSTAAddress,
    DialogToken,
    TID,
```

BlockAckPolicy,
 BufferSize,
 BlockAckTimeout,
GCRGroupAddress,
 VendorSpecificInfo
)

Insert the following row before the VendorSpecificInfo row in the untitled table in 6.3.29.4.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
GCRGroupAddress	GCR Group Address element	As defined in 8.4.2.128	Specifies the group address for which a Block Ack agreement is requested. This element is present if a GCR Group Address element was included in the transmitted ADDBA Request frame.

6.3.29.5 MLME-ADDDBA.response

6.3.29.5.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.29.5.2 as follows:

The primitive parameters are as follows:

```
MLME-ADDDBA.response(
    PeerSTAAddress,
    DialogToken,
    TID,
    ResultCode,
    BlockAckPolicy,
    BufferSize,
    BlockAckTimeout,
    GCRGroupAddress,
    VendorSpecificInfo
)
```

Insert the following row before the VendorSpecificInfo row in the untitled table in 6.3.29.5.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
GCRGroupAddress	GCR Group Address element	As defined in 8.4.2.128	Specifies the group address for which a Block Ack agreement was requested.

Change the title of 6.3.67 as follows:

6.3.67 DMS or GCR request and response procedure

6.3.67.1 General

Change the first paragraph of 6.3.67.1 as follows:

The following MLME primitives support the signaling of DMS or GCR request and response procedure. The informative diagram shown in Figure 6-25 depicts the DMS or GCR request and response process and is not meant to be exhaustive of all possible protocol uses.

Change Figure 6-25 as follows:

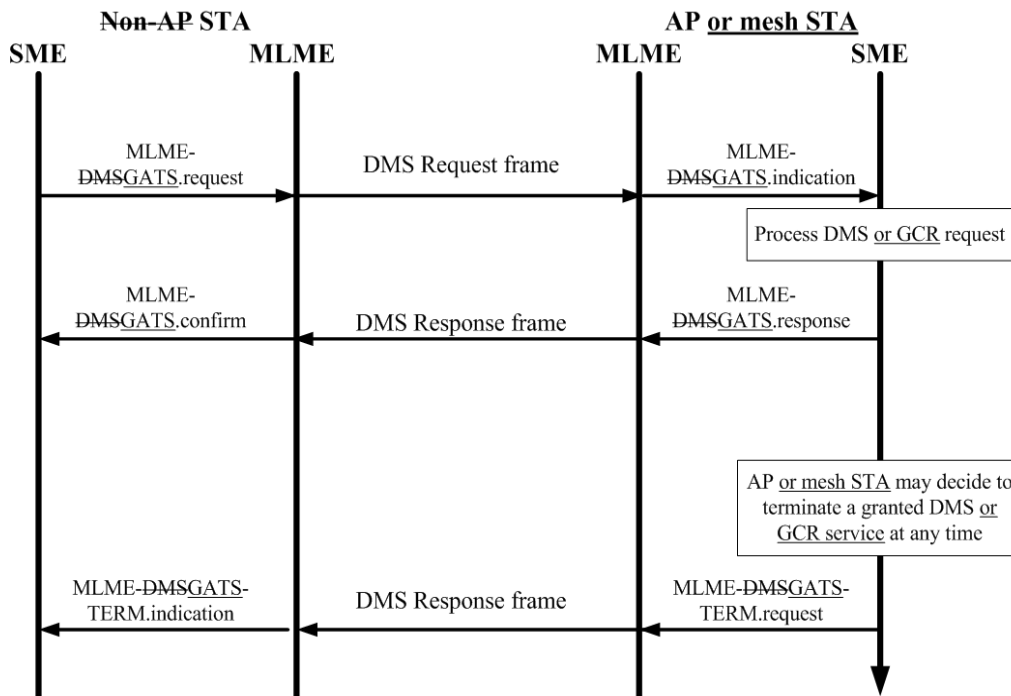


Figure 6-25—DMS or GCR setup protocol exchange

Change the title of 6.3.67.2 as follows:

6.3.67.2 MLME-DMSGATS.request

6.3.67.2.2 Semantics of the service primitive

Change 6.3.67.2.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS.request(
    PeerSTAAddress,
    Dialog Token,
    DMSRequest
)
```


Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC address	Specifies the address of the peer MAC entity with which to perform the DMS <u>or</u> GCR process.
Dialog Token	Integer	1–255	The Dialog Token to identify the DMS <u>or</u> GCR request and response transaction.
DMSRequest	DMS Request element	As defined in 8.4.2.90	Specifies group addressed frames <u>and</u> parameters for the requested DMS <u>or</u> GCR stream.

Change the title of 6.3.67.3 as follows:

6.3.67.3 MLME-~~DMSGATS~~.confirm

6.3.67.3.1 Function

Change 6.3.67.3.1 as follows:

This primitive reports the result of a DMS or GCR procedure.

6.3.67.3.2 Semantics of the service primitive

Change 6.3.67.3.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS.confirm(
    PeerSTAAddress,
    Dialog Token,
    DMSResponse
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC address	Specifies the address of the peer MAC entity with which to perform the DMS <u>or</u> GCR process.
Dialog Token	Integer	1–255	The Dialog Token to identify the DMS <u>or</u> GCR request and response transaction.
DMSResponse	DMS Response element	As defined in 8.4.2.91	Specifies the status returned by the AP responding to the STA's requested DMS <u>or</u> GCR stream.

6.3.67.3.3 When generated

Change 6.3.67.3.3 as follows:

This primitive is generated by the MLME as a result of an MLME-~~DMSGATS~~.request and indicates the results of the request.

This primitive is generated when the MLME-~~DMSGATS~~.request contains invalid parameters, when a timeout or failure occurs, or when the STA receives a DMS Response frame from the AP.

Change the title of 6.3.67.4 as follows:

6.3.67.4 MLME-~~DMSGATS~~.indication

6.3.67.4.2 Semantics of the service primitive

Change 6.3.67.4.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS.indication(
    PeerSTAAddress,
    DialogToken,
    DMSRequest
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity from which a DMS Request frame was received.
DialogToken	Integer	1–255	The Dialog Token to identify the DMS or GCR request and response transaction.
DMSRequest	DMS Request element	As defined in 8.4.2.90	Specifies group addressed frames for the requested DMS or GCR stream.

Change the title of 6.3.67.5 as follows:

6.3.67.5 MLME-~~DMSGATS~~.response

6.3.67.5.1 Function

Change 6.3.67.5.1 as follows:

This primitive is generated in response to an MLME-~~DMSGATS~~.indication requesting a DMS Response frame be sent to a non-AP STA.

6.3.67.5.2 Semantics of the service primitive

Change 6.3.67.5.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS.response(  
    PeerSTAAddress,  
    DialogToken,  
    DMSResponse  
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity from which a DMS Request frame was received.
DialogToken	Integer	1–255	The Dialog Token to identify the DMS <u>or</u> GCR request and response transaction.
DMSResponse	DMS Response element	As defined in 8.4.2.91	Specifies the status returned by the AP responding to the STA’s requested DMS <u>or</u> GCR stream.

6.3.67.5.3 When generated

Change 6.3.67.5.3 as follows:

This primitive is generated by the SME in response to an MLME-~~DMSGATS~~.indication requesting a DMS Response be sent to a non-AP STA.

Change the title of 6.3.67.6 as follows:

6.3.67.6 MLME-~~DMSGATS~~-TERM.request

6.3.67.6.1 Function

Change 6.3.67.6.1 as follows:

This primitive requests the transmission of a DMS Response frame to ~~non-AP~~ STAs to terminate a granted DMS or GCR service.

6.3.67.6.2 Semantics of the service primitive

Change 6.3.67.6.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS-TERM.request(  
    PeerSTAAddress,  
    DialogToken,  
    DMSResponse  
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity from which a DMS Request frame was received.
DialogToken	Integer	0	Set to 0 for an autonomous DMS Response frame.
DMSResponse	DMS Response element	As defined in 8.4.2.91	Specifies the requested DMS <u>or GCR</u> stream that is cancelled by the AP.

6.3.67.6.3 When generated

Change 6.3.67.6.3 as follows:

This primitive is generated by the SME to terminate DMS or GCR service.

Change the title of 6.3.67.7 as follows:

6.3.67.7 MLME-~~DMSGATS~~-TERM.indication

6.3.67.7.2 Semantics of the service primitive

Change 6.3.67.7.2 as follows:

The primitive parameters are as follows:

```
MLME-DMSGATS-TERM.indication(
    PeerSTAAddress,
    DialogToken,
    DMSResponse
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC address	Specifies the address of the peer MAC entity with which to perform the <u>DMS or GCR</u> process.
DialogToken	Integer	0	Set to 0 for an autonomous DMS Response frame.
DMSResponse	DMS Response element	As defined in 8.4.2.91	Specifies the requested DMS <u>or GCR</u> stream that is cancelled by the AP.

6.3.72 QoS Map Set element management

6.3.72.2 MLME-QoSMap.request

6.3.72.2.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.72.2.2 as follows:

```
MLME-QoSMap.request (
    Non-APSTAAddress,
    QoSMapSet,
    IntraAccessCategoryPriority
)
```

Insert the following row after the QoSMapSet row of the untitled table in 6.3.72.2.2 (note that entire table is not shown here):

Name	Type	Valid range	Description
IntraAccessCategoryPriority	Intra-Access Category Priority element	As defined in 8.4.2.123	Specifies the intra-AC priorities the STA should use. The parameter is present only if dot11SCSActivated is true.

6.3.72.3 MLME-QoSMap.indication

6.3.72.3.2 Semantics of the service primitive

Change the primitive parameter list in 6.3.72.3.2 as follows:

```
MLME-QoSMap.indication (
    QoSMapSet,
    IntraAccessCategoryPriority
)
```

Insert the following row after the QoSMapSet row of the untitled table in 6.3.72.3.2 (note that the entire table is not shown here):

Name	Type	Valid range	Description
IntraAccessCategoryPriority	Intra-Access Category Priority element	As defined in 8.4.2.123	Specifies the intra-AC priorities the STA should use.

Insert the following subclauses, 6.3.84 to 6.3.88.3.4 (including Figure 6-25a), after 6.3.83.8.4:

6.3.84 SCS request and response procedure

6.3.84.1 General

The following MLME primitives support the signaling of the SCS request and response procedure. The informative diagram shown in Figure 6-25a depicts the SCS request and response process and is not meant to be exhaustive of all possible protocol uses.

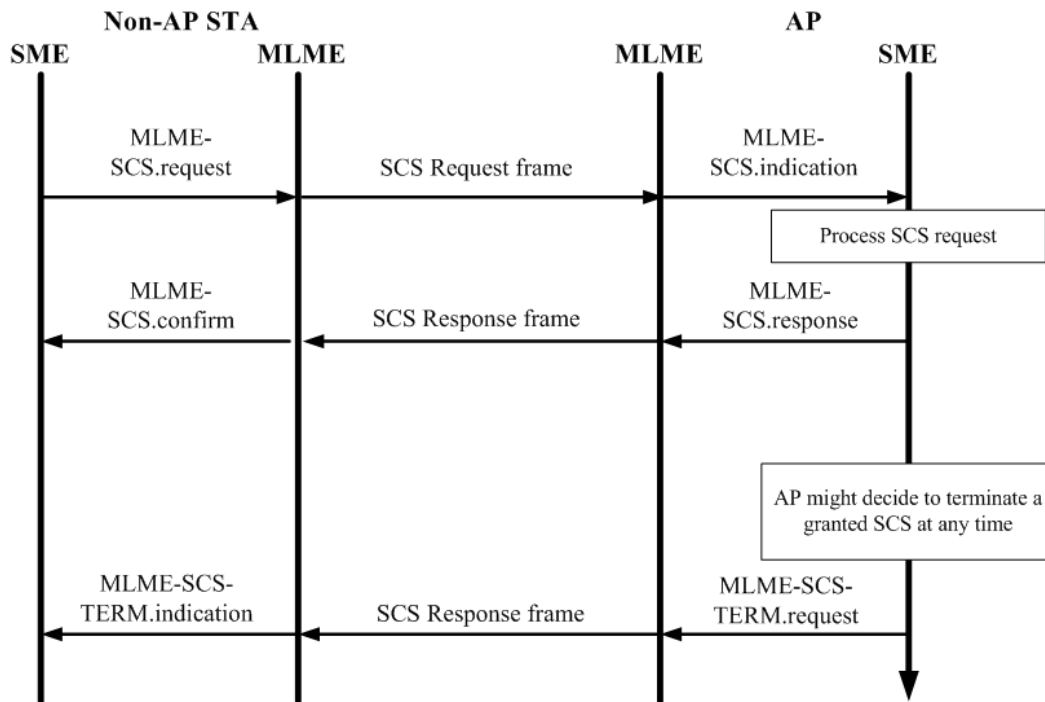


Figure 6-25a—Example SCS setup and termination protocol exchange

6.3.84.2 MLME-SCS.request

6.3.84.2.1 Function

This primitive requests transmission of an SCS Request frame to an AP.

6.3.84.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS.request(
    PeerSTAAddress,
    DialogToken,
    SCSRequest
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MAC Address	Any valid individual MAC address	Specifies the address of the peer MAC entity with which to perform the SCS process.
DialogToken	Integer	1–255	The dialog token to identify the SCS request and response transaction.
SCSRequest	SCS Descriptor element	SCS Descriptor element, as defined in 8.4.2.124	Specifies frame classifiers and priority for the requested SCS stream.

6.3.84.2.3 When generated

This primitive is generated by the SME to request that a SCS Request frame be sent to the AP with which the STA is associated.

6.3.84.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a SCS Request action management frame. The STA then attempts to transmit this frame to the AP with which the STA is associated.

6.3.84.3 MLME-SCS.confirm

6.3.84.3.1 Function

This primitive reports the result of a SCS procedure.

6.3.84.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS.confirm(
    ResultCode,
    PeerSTAAddress,
    DialogToken,
    SCSResponse
)
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, DECLINED, TCLAS_PROCESSING_NOT_SUPPORTED, INSUFFICIENT_TCLAS_PROCESSING, TIMEOUT	Reports the outcome of a request to send a SCS Request frame.
PeerSTAAddress	MAC Address	Any valid individual MAC address	Specifies the address of the peer MAC entity with which to perform the SCS process.

Name	Type	Valid range	Description
DialogToken	Integer	1–255	The dialog token to identify the SCS request and response transaction.
SCSResponse	SCS Status duple	SCS Status duple, as defined in 8.5.19.3	Specifies the status returned by the AP responding to the STA's requested SCSID.

6.3.84.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-SCS.request primitive and indicates the results of the request.

This primitive is generated when the MLME-SCS.request primitive contains invalid parameters, when a timeout or failure occurs, or when the STA receives a SCS Response frame from the AP.

6.3.84.3.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 10.26.2.

6.3.84.4 MLME-SCS.indication

6.3.84.4.1 Function

This primitive indicates that an SCS Request frame was received from a non-AP STA.

6.3.84.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS.indication(
    PeerSTAAddress,
    DialogToken,
    SCSRequest
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity from which an SCS Request frame was received.
DialogToken	Integer	1–255	The dialog token to identify the SCS request and response transaction.
SCSRequest	SCS Descriptor element	SCS Descriptor element, as defined in 8.4.2.124	Specifies frame classifiers and priority for the requested SCS stream.

6.3.84.4.3 When generated

This primitive is generated by the MLME when a valid SCS Request frame is received.

6.3.84.4.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 10.26.2.

6.3.84.5 MLME-SCS.response**6.3.84.5.1 Function**

This primitive is generated in response to an MLME-SCS.indication primitive requesting an SCS Response frame be sent to a non-AP STA.

6.3.84.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS.response(
    PeerSTAAddress,
    DialogToken,
    SCSResponse
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity from which a SCS Request frame was received.
DialogToken	Integer	1–255	The dialog token to identify the SCS request and response transaction.
SCSResponse	SCS Status duple	SCS Status duple, as defined in 8.5.19.3	Specifies the status returned by the AP responding to the STA's requested SCSID.

6.3.84.5.3 When generated

This primitive is generated by the SME in response to an MLME-SCS.indication primitive requesting an SCS Response frame be sent to a non-AP STA.

6.3.84.5.4 Effect of receipt

On receipt of this primitive, the MLME constructs a SCS Response frame. The STA then attempts to transmit this frame to the non-AP STA indicated by the PeerSTAAddress parameter.

6.3.84.6 MLME-SCS-TERM.request**6.3.84.6.1 Function**

This primitive requests the transmission of a SCS Response frame to a non-AP STA to terminate an established SCS stream.

6.3.84.6.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS-TERM.request(
    PeerSTAAddress,
    DialogToken,
    SCSResponse
)
```

Name	Type	Valid range	Description
PeerSTAAddress	MACAddress	Any valid individual MAC address	The address of the non-AP STA MAC entity to which the SCS Response frame is to be sent.
DialogToken	Integer	0	Set to 0 for an autonomous SCS Response frame.
SCSResponse	SCS Status duple	SCS Status duple, as defined in 8.5.19.3	Specifies the requested SCSID that is cancelled by the AP.

6.3.84.6.3 When generated

This primitive is generated by the SME to terminate an SCS stream.

6.3.84.6.4 Effect of receipt

On receipt of this primitive, the MLME constructs an SCS Response frame. The STA then attempts to transmit this frame to the non-AP STA indicated by the PeerSTAAddress parameter.

6.3.84.7 MLME-SCS-TERM.indication

6.3.84.7.1 Function

This primitive is generated by the MLME when a valid unsolicited SCS Response frame is received.

6.3.84.7.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-SCS-TERM.indication(
    ResultCode,
    DialogToken,
    SCSResponse
)
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME-SCS-TERM.request primitive.
DialogToken	Integer	0	Set to 0 for an autonomous SCS Response frame.
SCSResponse	SCS Status duple	SCS Status duple, as defined in 8.5.19.3	Specifies the requested SCSID that is cancelled by the AP.

6.3.84.7.3 When generated

This primitive is generated when the STA receives an unsolicited SCS Response frame from the AP.

6.3.84.7.4 Effect of receipt

On receipt of this primitive, the SME should operate according to the procedure in 10.26.2.

6.3.85 QLoad report management

6.3.85.1 General

The QLoad report management primitives support the process of QLoad reporting between APs as described in 10.27.2.

6.3.85.2 MLME-QLOAD.request

6.3.85.2.1 Function

This primitive is used by an AP to transmit a QLoad Request frame to a specified AP.

6.3.85.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QLOAD.request(
    PeerMACAddress,
    DialogToken,
    Protected
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the QLoad Request frame is sent.
DialogToken	Integer	1–255	Specifies a number unique to the MLME-QLOAD.request primitive.
Protected	Boolean	true, false	If true, the request is sent using the Protected QLoad Request frame. If false, the request is sent using the QLoad Request frame.

6.3.85.2.3 When generated

This primitive is generated by the SME at an AP to request the transmission of a QLoad Request frame to the AP indicated by the PeerMACAddress parameter.

6.3.85.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a QLoad Request action management frame if the Protected parameter is false or a Protected QLoad Request frame if the Protected parameter is true. The AP then attempts to transmit this frame to the AP indicated by the PeerMACAddress parameter.

6.3.85.3 MLME-QLOAD.confirm

6.3.85.3.1 Function

This primitive reports the result of a request to send a QLoad Request frame.

6.3.85.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QLOAD.confirm(
    ResultCode,
    PeerMACAddress,
    DialogToken,
    Protected,
    QLoadReport
)
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, UNSPECIFIED_FAILURE	Reports the outcome of a QLoad request.
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the QLoad Request frame was sent.

Name	Type	Valid range	Description
DialogToken	Integer	0–255	Specifies a number unique to the QLoad Report request and response transaction or 0 when an unsolicited report was sent.
Protected	Boolean	true, false	If true, the response was sent using the Protected QLoad Report frame. If false, the response was sent using the QLoad Report frame.
QLoadReport	Set of reports, each as defined in the QLoad Report element	Set of reports, each as defined in the QLoad Report element	Set of reports, each as defined in the QLoad Report element.

6.3.85.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-QLOAD.request primitive indicating the results of that request. This primitive is generated when an MLME-QLOAD.request primitive contains invalid parameters or when the STA receives a response in the form of a QLoad Report frame in the corresponding Robust AV Streaming Action frame.

6.3.85.3.4 Effect of receipt

The SME is notified of the results of the QLoad request procedure.

The SME should operate according to the procedures defined in 10.27.2.

6.3.85.4 MLME-QLOAD.indication

6.3.85.4.1 Function

This primitive indicates that a QLoad Request frame has been received.

6.3.85.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QLOAD.indication(
    PeerMACAddress,
    DialogToken,
    Protected
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity from which the QLoad Request frame was received.
DialogToken	Integer	1–255	Specifies a number unique to the MLME-QLOAD.request primitive.
Protected	Boolean	true, false	If true, the request was sent using the Protected QLoad Request frame. If false, the request was sent using the QLoad Request frame.

6.3.85.4.3 When generated

This primitive is generated by the MLME when a valid (Protected) QLoad Request frame is received.

6.3.85.4.4 Effect of receipt

On receipt of this primitive, the SME either rejects the request or commences the transaction as described in 10.27.2.

6.3.85.5 MLME-QLOAD.response

6.3.85.5.1 Function

This primitive is used by an AP to transmit a QLoad Report frame to a specified AP in response to a QLoad Request frame.

6.3.85.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QLOAD.response(
    PeerMACAddress,
    DialogToken,
    Protected,
    QLoadReport
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the QLoad Report frame is sent.
DialogToken	Integer	0–255	The dialog token of the matching MLME-QLOAD.indication primitive or 0 when sending an unsolicited report.

Name	Type	Valid range	Description
Protected	Boolean	true, false	If true, the response is sent using the Protected QLoad Report frame. If false, the response is sent using the QLoad Report frame.
QLoadReport	Set of reports, each as defined in the QLoad Report element	Set of reports, each as defined in the QLoad Report element	Set of reports, each as defined in the QLoad Report element.

6.3.85.5.3 When generated

This primitive is generated by the SME at an AP in response to the reception of a QLoad Request frame from the AP indicated by the PeerMACAddress parameter.

6.3.85.5.4 Effect of receipt

On receipt of this primitive, the MLME constructs a QLoad Report action management frame if the Protected parameter is false or a Protected QLoad Report frame if the Protected parameter is true. The AP then attempts to transmit this frame to the other AP indicated by the PeerMACAddress parameter.

6.3.86 HCCA TXOP advertisement management

6.3.86.1 General

The TXOP advertisement management primitives support the process of TSPEC schedule negotiation between APs, as described in 10.27.

6.3.86.2 MLME-TXOPADVERTISEMENT.request

6.3.86.2.1 Function

This primitive is used by an AP to transmit an HCCA TXOP advertisement to a specified AP.

6.3.86.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-TXOPADVERTISEMENT.request(
    PeerMACAddress,
    DialogToken,
    Protected,
    ActiveTXOPReservations,
    PendingTXOPReservations
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the TXOP Advertisement frame is sent.
DialogToken	Integer	0–255	Specifies a number unique to the TXOPAdvertisement.request primitive.
Protected	Boolean	true, false	If true, the request is sent using the Protected HCCA TXOP Advertisement frame. If false, the request is sent using the HCCA TXOP Advertisement frame.
ActiveTXOPReservations	TXOP Reservation	As defined in 8.4.1.43	Specifies the HCCA TXOPs that have been created.
PendingTXOPReservations	TXOP Reservation	As defined in 8.4.1.43	Specifies the HCCA TXOPs that are in the process of being created.

6.3.86.2.3 When generated

This primitive is generated by the SME at an AP to request a (Protected) HCCA TXOP Advertisement frame be sent to the AP indicated by the PeerMACAddress parameter.

6.3.86.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs an HCCA TXOP Advertisement frame if the Protected parameter is false or constructs a Protected HCCA TXOP Advertisement frame if the Protected parameter is true. This frame is then scheduled for transmission.

6.3.86.3 MLME-TXOPADVERTISEMENT.confirm

6.3.86.3.1 Function

This primitive reports the result of a request to perform HCCA TXOP negotiation.

6.3.86.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-TXOPADVERTISEMENT.confirm(
    ResultCode,
    PeerMACAddress,
    DialogToken,
    Protected,
    AlternateSchedule,
    AvoidanceRequest
)
```


Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, TS_SCHEDULE_ CONFLICT, UNSPECIFIED_FAILURE	Reports the outcome of a request to send a TXOP advertisement. Indicates the results of the corresponding MLME-TXOPADVERTISE.request primitive.
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity from which the Scheduled TXOP Response frame was received.
DialogToken	Integer	0–255	The dialog token to identify the scheduled TXOP advertisement and scheduled TXOP response transaction.
Protected	Boolean	true, false	If true, the response was sent using the Protected HCCA TXOP Response frame. If false, the response was sent using the HCCA TXOP Response frame.
AlternateSchedule	TXOP Reservation	As defined in 8.4.1.43	Specifies an alternate TXOP when status code is nonzero.
AvoidanceRequest	TXOP Reservation	As defined in 8.4.1.43	Specifies a TXOP to avoid when status code is nonzero.

6.3.86.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-TXOPADVERTISE.request primitive indicating the results of that request. This primitive is generated when an MLME-TXOPADVERTISE.request primitive contains invalid parameters, when the STA receives a response in the form of an HCCA TXOP Response frame in the corresponding Public Action frame, or when the STA receives a response in the form of a Protected HCCA TXOP Response frame in the corresponding frame.

6.3.86.3.4 Effect of receipt

On receipt of this primitive, the SME performs the behavior defined in 10.27.3.

6.3.86.4 MLME-TXOPADVERTISE.indication

6.3.86.4.1 Function

This primitive indicates that an HCCA TXOP Advertisement frame has been received from a peer entity.

6.3.86.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-TXOPADVERTISE.indication(
    PeerMACAddress,
    DialogToken,
```

Protected,
ActiveTXOPReservations,
PendingTXOPReservations
)

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity from which the HCCA TXOP Advertisement frame was sent.
DialogToken	Integer	0–255	Specifies a number unique to the MLME-TXOPADVERTISEMENT.request primitive.
Protected	Boolean	true, false	If true, the request was sent using the Protected HCCA TXOP Request frame. If false, the request was sent using the HCCA TXOP Request frame.
ActiveTXOPReservations	TXOP Reservation	As defined in 8.4.1.43	Specifies the HCCA TXOPs that have been created.
PendingTXOPReservations	TXOP Reservation	As defined in 8.4.1.43	Specifies the HCCA TXOPs that are in the process of being created.

6.3.86.4.3 When generated

This primitive is generated by the MLME when a valid HCCA TXOP Advertisement frame is received.

6.3.86.4.4 Effect of receipt

On receipt of this primitive, the SME performs the behavior defined in 10.27.3.

6.3.86.5 MLME-TXOPADVERTISEMENT.response

6.3.86.5.1 Function

This primitive is used by an AP to transmit an HCCA TXOP Response frame to a specified AP.

6.3.86.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-TXOPADVERTISEMENT.response(
    PeerMACAddress,
    DialogToken,
    Protected,
    StatusCode,
    ScheduleConflict,
```

AlternateSchedule,
AvoidanceRequest
)

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the HCCA TXOP Response frame is sent.
DialogToken	Integer	0–255	The dialog token to identify the TXOP advertisement and TXOP response transaction.
Protected	Boolean	true, false	If true, the response is sent using the Protected HCCA TXOP Response frame. If false, the response is sent using the HCCA TXOP Response frame.
StatusCode	Enumeration	SUCCESS, TS_SCHEDULE_CONFLICT (as defined in 8.4.1.9)	The result of checking the TXOP reservation from the corresponding TXOP advertisement.
ScheduleConflict	Integer	1–number of TXOP reservations	The TXOP reservation from the HCCA TXOP Advertisement frame that conflicts with an existing or in-progress schedule.
AlternateSchedule	TXOP Reservation	As defined in 8.4.1.43	Specifies an alternate TXOP when status code is nonzero.
AvoidanceRequest	TXOP Reservation	As defined in 8.4.1.43	Specifies a TXOP to avoid when status code is nonzero.

6.3.86.5.3 When generated

This primitive is generated by the SME at an AP to request the sending of an HCCA TXOP Response frame to another AP indicated by the PeerMACAddress parameter.

6.3.86.5.4 Effect of receipt

On receipt of this primitive, the MLME constructs an HCCA TXOP Response frame if the Protected parameter is false or constructs a Protected HCCA TXOP Response frame if the Protected parameter is true. The AP then attempts to transmit this frame to the AP indicated by the PeerMACAddress parameter.

6.3.87 Group membership management

6.3.87.1 General

The group membership primitives support the process of group membership requesting and reporting between an AP and its associated STAs as described in 10.23.15.3.2.

6.3.87.2 MLME-GROUP-MEMBERSHIP.request

6.3.87.2.1 Function

This primitive is used by an AP to initiate a Group Membership Request frame to a specified associated STA.

6.3.87.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-GROUP-MEMBERSHIP.request(
    PeerMACAddress,
    DialogToken
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the Group Membership Request frame is to be sent.
DialogToken	Integer	0–255	Specifies a number unique to the MLME-GROUP-MEMBERSHIP.request primitive.

6.3.87.2.3 When generated

This primitive is generated by the SME at an AP to request the sending of a Group Membership Request frame to the associated STA indicated by the PeerMACAddress parameter.

6.3.87.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a Group Membership Request frame. The AP then attempts to transmit this frame to the STA indicated by the PeerMACAddress parameter.

6.3.87.3 MLME-GROUP-MEMBERSHIP.confirm

6.3.87.3.1 Function

This primitive reports the result of a request for a STA's group membership.

6.3.87.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-GROUP-MEMBERSHIP.confirm(
    ResultCode,
    GroupAddress
)
```

Name	Type	Valid range	Description
ResultCode	Enumeration	SUCCESS, UNSPECIFIED_FAILURE	Reports the outcome of a group membership request.
GroupAddress	MAC Address	Any valid MAC address that has the Individual/Group Address bit set	Zero or more MAC addresses that correspond to the contents of the dot11GroupAddressesTable of the STA that responded to the group address request.

6.3.87.3.3 When generated

This primitive is generated by the MLME as a result of an MLME-GROUP-MEMBERSHIP.request primitive indicating the results of that request.

This primitive is generated when an MLME-GROUP-MEMBERSHIP.request primitive contains invalid parameters or when the STA receives a response in the form of a Group Membership Response frame in the corresponding Robust Action frame from the associated STA.

6.3.87.3.4 Effect of receipt

The SME is notified of the results of the group membership request procedure.

The SME should operate according to the procedures defined in 10.23.15.3.2.

6.3.87.4 MLME-GROUP-MEMBERSHIP.indication

6.3.87.4.1 Function

This primitive indicates that a Group Membership Request frame has been received from a peer entity.

6.3.87.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-GROUP-MEMBERSHIP.indication(
    PeerMACAddress,
    DialogToken
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity from which the Group Membership Request frame was sent.
DialogToken	Integer	0–255	Specifies a number unique to the MLME-GROUP-MEMBERSHIP primitive.

6.3.87.4.3 When generated

This primitive is generated by the MLME when a valid Group Membership Request frame is received.

6.3.87.4.4 Effect of receipt

On receipt of this primitive, the SME performs the behavior defined in 10.23.15.3.2.

6.3.87.5 MLME-GROUP-MEMBERSHIP.response

6.3.87.5.1 Function

This primitive responds to the request for the contents of the group address table by a specified STA's MAC entity.

6.3.87.5.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-GROUP-MEMBERSHIP.response(
    PeerMACAddress,
    DialogToken,
    GroupAddress
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the Group Membership Response frame is sent.
DialogToken	Integer	0–255	Specifies a number unique to the MLME-GROUP-MEMBERSHIP primitive.
GroupAddress	MAC Address	Any valid MAC address that has the Individual/Group Address bit set	Zero or more MAC addresses that correspond to the contents of the dot11GroupAddressesTable of the STA that is responding to the group address request.

6.3.87.5.3 When generated

This primitive is generated by the MLME as a result of an MLME-GROUP-MEMBERSHIP.indication primitive.

6.3.87.5.4 Effect of receipt

On receipt of this primitive, the SME performs the behavior defined in 10.23.15.3.2.

6.3.88 AP PeerKey management

6.3.88.1 General

The AP PeerKey management primitives support the AP PeerKey protocol to provide session identification and data confidentiality for an AP-to-AP connection, as described in 11.10.

6.3.88.2 MLME-APPEERKEY.request

6.3.88.2.1 Function

This primitive is used by an AP to transmit a public key to a specified AP and to request the peer's public key.

6.3.88.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-APPEERKEY.request(  
    PeerMACAddress,  
    RequestType,  
    Group,  
    PublicKey  
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity to which the Public Key frame is sent.
RequestType	Integer	As defined in Table 8-221c	Specifies the type of request.
Group	Finite Cyclic Group field	As defined in 8.4.1.40	Specifies cyclic group from which the public key was generated.
PublicKey	Scalar field	As defined 8.4.1.39	The public key of the AP sending this Public Key frame.

6.3.88.2.3 When generated

This primitive is generated by the SME at an AP to request the sending of a Public Key frame to another AP indicated by the PeerMACAddress parameter.

6.3.88.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a Public Key frame. The AP then attempts to transmit this frame to the AP indicated by the PeerMACAddress parameter.

6.3.88.3 MLME-APPEERKEY.indication

6.3.88.3.1 Function

This primitive indicates that a Public Key frame has been received from a peer entity.

6.3.88.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-APPEERKEY.indication(
    PeerMACAddress,
    RequestType,
    Group,
    PublicKey
)
```

Name	Type	Valid range	Description
PeerMACAddress	MACAddress	Any valid individual MAC address	The address of the peer MAC entity from which the Public Key frame has been received.
RequestType	Integer	As defined in Table 8-221c	Specifies the type of request.
Group	Finite Cyclic Group field	As defined in 8.4.1.40	Specifies cyclic group from which the public key was generated.
PublicKey	Scalar field	As defined 8.4.1.49	The public key of the AP that sent this Public Key frame.

6.3.88.3.3 When generated

This primitive is generated by the MLME when a valid Public Key frame is received.

6.3.88.3.4 Effect of receipt

On receipt of this primitive, the SME performs the behavior defined in 11.10.

8. Frame formats

8.2 MAC frame formats

8.2.4 Frame fields

8.2.4.1 Frame Control field

8.2.4.1.8 More Data field

Change the seventh paragraph of 8.2.4.1.8 as follows:

The More Data field is set to 1 in group addressed frames transmitted by the AP when additional group addressed bufferable units (BUs) that are not part of an active GCR-SP remain to be transmitted by the AP during this beacon interval. The More Data field is set to 0 in group addressed frames transmitted by the AP when no more group addressed BUs that are not part of an active GCR-SP remain to be transmitted by the AP during this beacon interval and in all group addressed frames transmitted by non-AP STAs.

Insert the following paragraph after the seventh paragraph of 8.2.4.1.8:

The More Data field is set to 1 in group addressed frames transmitted by the AP when additional group addressed BUs that are part of an active GCR-SP remain to be transmitted by the AP during this GCR-SP. The More Data field is set to 0 in group addressed frames transmitted by the AP when no more group addressed BUs that are part of an active GCR-SP remain to be transmitted by the AP during this GCR-SP.

8.2.4.4 Sequence Control field

8.2.4.4.2 Sequence Number field

Change the last paragraph of 8.2.4.4.2 as follows:

Each fragment of an MSDU or MMPDU contains a copy of the sequence number assigned to that MSDU or MMPDU. The sequence number remains constant in all retransmissions of an MSDU, MMPDU, or fragment thereof, except when the MSDU is delivered via both DMS and group addressed delivery via NoAck, GCR unsolicited retry, or GCR Block Ack retransmission policies. In such cases, the sequence numbers assigned to the MSDUs (re)transmitted using group addressed delivery need not match the sequence number of the corresponding individually addressed A-MSDUs delivered via DMS.

8.2.4.5 QoS Control field

8.2.4.5.3 EOSP (end of service period) subfield

Insert the following paragraph at the end of 8.2.4.5.3:

If dot11RobustAVStreamingImplemented is true, then the HC sets the EOSP field to 1 in a GCR-SP group addressed frame in order to indicate that no more GCR-SP frames of that group address are to be transmitted by the AP until the next scheduled SP for this GCR-SP stream. The EOSP field is set to 0 in a group addressed frame delivered using the GCR-A procedures described in 10.23.15.3.8.

8.2.4.6 HT Control field

Change Figure 8-5 as shown:

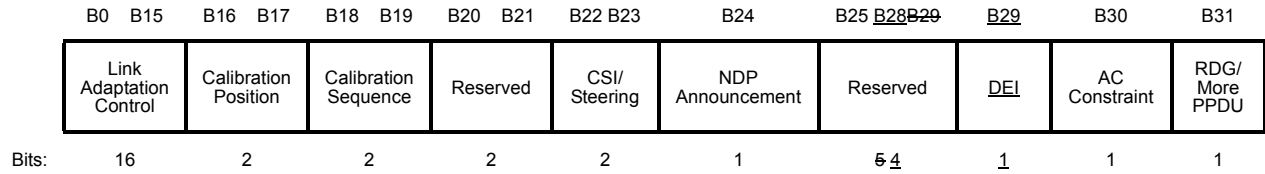


Figure 8-5—HT Control field

Insert the following paragraph after the tenth paragraph (“The NDP Announcement subfield ...”) of 8.2.4.6:

The DEI subfield is 1 bit in length and is set by the transmitting STA to indicate the suitability of the corresponding MSDU or A-MSDU to be discarded if there are insufficient resources at the receiving STA. If there are insufficient resources, a STA that receives an MPDU whose DEI subfield is equal to 1 carrying all or part of an MSDU or A-MSDU should discard the MSDU or any MSDUs contained within the A-MSDU in preference to MSDUs carried in MPDUs whose DEI subfield is equal to 0. See 10.26.2. In an MMPDU, the DEI subfield is reserved. The mechanisms for determining whether the resources are insufficient or when to discard MSDUs or A-MSDUs are beyond the scope of this standard.

8.3 Format of individual frame types

8.3.1 Control frames

8.3.1.8 BlockAckReq frame format

8.3.1.8.1 Overview

Change Figure 8-20 as indicated:

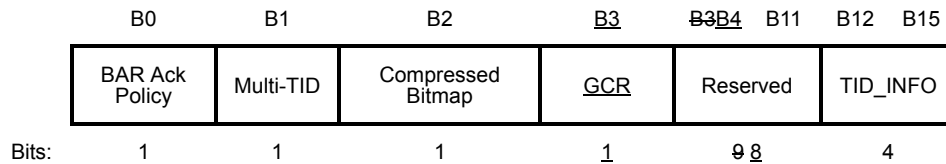


Figure 8-20—BAR Control field

Change the seventh paragraph of 8.3.1.8.1 as indicated:

The values of the Multi-TID, ~~and~~ Compressed Bitmap, ~~and~~ GCR subfields determine which of ~~three~~ four possible BlockAckReq frame variants is represented, as indicated in Table 8-16.

Change Table 8-16 as indicated:

Table 8-16—BlockAckReq frame variant encoding

Multi-TID subfield value	Compressed Bitmap subfield value	<u>GCR subfield value</u>	BlockAckReq frame variant
0	0	<u>0</u>	Basic BlockAckReq
0	1	<u>0</u>	Compressed BlockAckReq
1	0	<u>0</u>	Reserved
1	1	<u>0</u>	Multi-TID BlockAckReq
<u>0</u>	<u>0</u>	<u>1</u>	<u>Reserved</u>
<u>0</u>	<u>1</u>	<u>1</u>	<u>GCR BlockAckReq</u>
<u>1</u>	<u>0</u>	<u>1</u>	<u>Reserved</u>
<u>1</u>	<u>1</u>	<u>1</u>	<u>Reserved</u>

Insert the following subclause, 8.3.1.8.5 (including Figure 8-23a), after 8.3.1.8.4:

8.3.1.8.5 GCR BlockAckReq variant

The TID_INFO subfield of the BAR Control field of the GCR BlockAckReq frame is set to 0.

The BAR Information field of the GCR BlockAckReq frame contains the Block Ack Starting Sequence Control subfield and GCR Group Address subfield, as shown in Figure 8-23a. The Block Ack Starting Sequence Control subfield is shown in Figure 8-21. The Starting Sequence Number subfield of the Block Ack Starting Sequence Control subfield contains the sequence number of the first MSDU or A-MSDU for which this BlockAckReq frame is sent. The Fragment Number subfield of the Block Ack Starting Sequence Control subfield is set to 0.

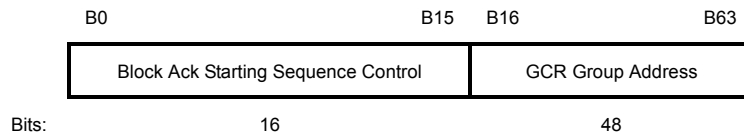


Figure 8-23a—BAR Information field format (GCR BlockAckReq)

The GCR Group Address subfield contains the MAC address of the group for which reception status is being requested.

8.3.1.9 Block Ack frame format

8.3.1.9.1 Overview

Change Figure 8-25 as indicated:

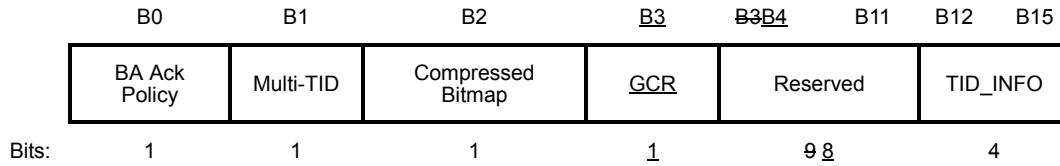


Figure 8-25—BA Control field

Change the seventh paragraph of 8.3.1.9.1 as indicated:

The values of the Multi-TID, GCR, and Compressed Bitmap subfields of the BA Control field determine which of ~~three~~ four possible BlockAck frame variants is represented, as indicated in the Table 8-18.

Change Table 8-18 as indicated:

Table 8-18—BlockAck frame variant encoding

Multi-TID subfield value	Compressed Bitmap subfield value	<u>GCR subfield value</u>	BlockAck frame variant
0	0	<u>0</u>	Basic BlockAck
0	1	<u>0</u>	Compressed BlockAck
1	0	<u>0</u>	Reserved
1	1	<u>0</u>	Multi-TID BlockAck
<u>0</u>	<u>0</u>	1	<u>Reserved</u>
<u>0</u>	1	1	<u>GCR BlockAck</u>
1	<u>0</u>	1	<u>Reserved</u>
1	1	1	<u>Reserved</u>

Insert the following paragraph into 8.3.1.9.1 after the note starting “NOTE—Reference to “a BlockAck” frame without...”:

When the GCR field is equal to 1, the BlockAck is sent in response to a BlockAckReq that had the GCR field with a value of 1 in the BAR Control field.

Insert the following subclause, 8.3.1.9.5 (including Figure 8-28a), after 8.3.1.9.4:

8.3.1.9.5 GCR Block Ack variant

The TID_INFO subfield of the BA Control field of the GCR BlockAck frame contains the TID for which this BlockAck frame is sent.

The BA Information field of the GCR BlockAck frame comprises the Block Ack Starting Sequence Control, GCR Group Address, and the Block Ack Bitmap subfields, as shown in Figure 8-28a. The Block Ack Starting Sequence Control subfield is shown in Figure 8-21. The Starting Sequence Number subfield of the Block Ack Starting Sequence Control subfield contains the sequence number of the first A-MSDU for which this BlockAck frame is sent. The value of this subfield is defined in 9.21.10. The Fragment Number subfield of the Block Ack Starting Sequence Control subfield is set to 0.

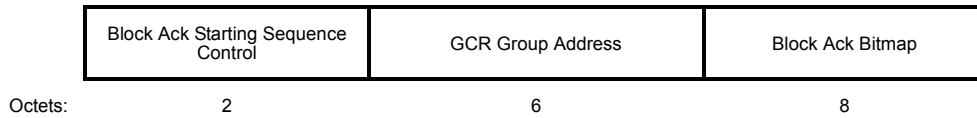


Figure 8-28a—BA Information field format (GCR BlockAck)

The GCR Group Address subfield is set to the value from the Group Address subfield of the GCR BAR Information field in the BlockAckReq frame to which the BlockAck frame is sent in response.

The Block Ack Bitmap subfield is 8 octets in length and is used to indicate the received status of up to 64 MSDUs and A-MSDUs. Each bit that is equal to 1 in the Block Ack bitmap acknowledges the successful reception of a single MSDU or A-MSDU in the order of sequence number, with the first bit of the Block Ack bitmap corresponding to the MSDU or A-MSDU with the sequence number that matches the value of the Starting Sequence Number subfield of the Block Ack Starting Sequence Control subfield.

8.3.2 Data frames

8.3.2.1 Data frame format

Change the third paragraph of 8.3.2.1 as follows:

A QoS STA always uses QoS data frames for data transmissions to other QoS STAs. A QoS STA uses frames with the QoS subfield of the Subtype field set to 0 for data transmissions to non-QoS STAs. A non-QoS STA always uses frames with the QoS subfield of the Subtype field set to 0 for data transmissions to other STAs. All STAs use frames with the QoS subfield of the Subtype field set to 0 for nonconcealed GCR broadcast data frames unless a transmitting STA knows that all STAs in a BSS have QoS capability, in which case the transmitting STAs use QoS data frames. All STAs use frames with the QoS subfield of the Subtype field set to 0 for nonconcealed GCR group addressed data frames unless it is known to the transmitter that all STAs in the BSS that are members of the multicast group have QoS capability, in which case STAs use QoS data frames. APs where dot11RobustAVStreamingImplemented is true or mesh STAs where dot11MeshGCRImplemented is true use frames with the QoS subfield of the Subtype field set to 1 for concealed GCR frames, as described in 10.23.15.3.5.

8.3.3 Management frames

8.3.3.2 Beacon frame format

Insert the following rows into Table 8-20 before the Last row (note that the entire table is not shown here):

Table 8-20—Beacon frame body

Order	Information	Notes
57	QLoad Report	The QLoad Report element is present every dot11QLoadReportIntervalDTIM DTIMs if dot11QLoadReportActivated is true.
58	HCCA TXOP Update Count	The HCCA TXOP Update Count element is present if both dot11PublicHCCATXOPNegotiationActivated is true and an HC is collocated with the AP.

8.3.3.10 Probe Response frame format

Insert the following row into Table 8-27 before the Last-1 row (note that the entire table is not shown here):

Table 8-27—Probe Response frame body

Order	Information	Notes
56	QLoad Report	The QLoad Report element is present if dot11QLoadReportActivated is true.

8.4 Management frame body components

8.4.1 Fields that are not information elements

8.4.1.9 Status Code field

In Table 8-37, change status codes 37, 56, and 57 as indicated; insert status codes 97 and 98 in numeric order; and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-37—Status codes

Status code	Name	Meaning
37	<u>REQUEST_DECLINED</u>	The request has been declined.
56	<u>REQUESTED_TCLAS_NOT_SUPPORTED_BY_AP</u>	Requested TCLAS processing is not supported by the AP.
57	<u>INSUFFICIENT_TCLAS_PROCESSING_RESOURCES</u>	The AP has insufficient TCLAS processing resources to satisfy the request.

Table 8-37—Status codes (continued)

Status code	Name	Meaning
97	<u>TCLAS_PROCESSING_</u> <u>TERMINATED</u>	<u>Requested TCLAS processing has been terminated by the AP.</u>
98	<u>TS_SCHEDULE_CONFLICT</u>	<u>The TS schedule conflicts with an existing schedule; an alternative schedule is provided.</u>

8.4.1.11 Action field

In Table 8-38, insert category code 19 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

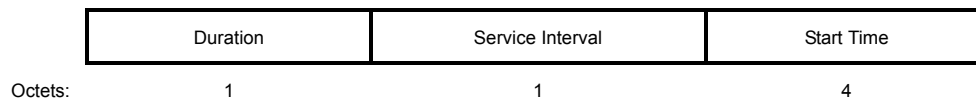
Table 8-38—Category values

Code	Meaning	See subclause	Robust	Group addressed privacy
19	Robust AV Streaming	8.5.19	Yes	—

Insert the following subclause, 8.4.1.43, after 8.4.1.42:

8.4.1.43 TXOP Reservation field

The format of the TXOP Reservation field is shown in Figure 8-80a.

**Figure 8-80a—TXOP Reservation field format**

The Duration subfield specifies the duration of the TXOP in units of 32 μ s.

The Service Interval subfield contains an 8-bit unsigned integer that specifies the service interval (SI) of the reservation in units of milliseconds.

The Start Time subfield is the offset from the next TBTT to the start of the first SP and indicates the anticipated start time, expressed in microseconds, of the first TXOP after the TBTT.

8.4.2 Information elements

8.4.2.1 General

In Table 8-54, insert element IDs 184 to 189 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-54—Element IDs

Element	Element ID	Length of indicated element (in octets)	Extensible
Intra-Access Category Priority (see 8.4.2.123)	184	3	Yes
SCS Descriptor (see 8.4.2.124)	185	4 to 257	Subelements
QLoad Report (see 8.4.2.125)	186	23	Subelements
HCCA TXOP Update Count (see 8.4.2.126)	187	3	No
Higher Layer Stream ID (see 8.4.2.127)	188	Variable	Yes
GCR Group Address (see 8.4.2.128)	189	8	No

8.4.2.27 RSNE

8.4.2.27.3 AKM suites

In Table 8-101, insert suite type 10 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-101—AKM suite selectors

OUI	Suite type	Meaning		
		Authentication type	Key management type	Key derivation type
00-0F-AC	10	APPeerKey Authentication with SHA-256 or using PMKSA caching as defined in 11.5.9.3 with SHA-256 Key Derivation	RSNA key management as defined in 11.6 or using PMKSA caching as defined in 11.5.9.3 with SHA256 Key Derivation	Defined in 11.6.1.7.2

8.4.2.29 Extended Capabilities element

In Table 8-103, insert bits 51 to 58 and bit 60 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-103—Capabilities field

Bit	Information	Notes
51	Robust AV Streaming	The STA sets the Robust AV Streaming field to 1 when dot11RobustAVStreamingImplemented is true and sets it to 0 otherwise. See 10.26.
52	Advanced GCR	The STA sets the Advanced GCR field to 1 when dot11AdvancedGCRActivated is true and sets it to 0 otherwise. See 10.23.15.3.
53	Mesh GCR	The STA sets the mesh GCR field to 1 when dot11MeshGCRActivated is true and sets it to 0 otherwise. See 10.23.15.3.
54	SCS	The STA sets the SCS field to 1 when dot11SCSActivated is true and sets it to 0 otherwise. See 10.26.2.
55	QLoad Report	The STA sets the QLoad Report field to 1 when dot11QLoadReportActivated is true and sets it to 0 otherwise. See 10.27.2.
56	Alternate EDCA	The STA sets the Alternate EDCA field to 1 when dot11AlternateEDCActivated is true and sets it to 0 otherwise. See 9.2.4.2.
57	Unprotected TXOP Negotiation	The STA sets the Unprotected TXOP Negotiation field to 1 when dot11PublicTXOPNegotiationActivated is true and sets it to 0 otherwise. See 10.27.3.
58	Protected TXOP Negotiation	The STA sets the Protected TXOP Negotiation field to 1 when dot11ProtectedTXOPNegotiationActivated is true and sets it to 0 otherwise. See 10.27.3.
60	Protected QLoad Report	The STA sets the Protected QLoad Report field to 1 when dot11ProtectedQLoadReportActivated is true and sets it to 0 otherwise. See 10.27.2.

8.4.2.32 TSPEC element

Change the first paragraph of 8.4.2.32 as follows:

The TSPEC element contains the set of parameters that define the characteristics and QoS expectations of a traffic flow, in the context of a particular STA, for use by the HC and STA(s) or a mesh STA and its peer mesh STAs in support of QoS traffic transfer using the procedures defined in 10.4 and 10.23.15.3. The element information format comprises the items as defined in this subclause, and the structure is defined in Figure 8-196.

Change the fourth paragraph of 8.4.2.32 as follows:

The subfields of the TS Info field are defined as follows:

- The Traffic Type subfield is a single bit and is set to 1 for a periodic traffic pattern (e.g., isochronous TS of MSDUs or A-MSDUs, with constant or variable sizes, that are originated at fixed rate) or set to 0 for an aperiodic, or unspecified, traffic pattern (e.g., asynchronous TS of low-duty cycles).

- The TSID subfield is 4 bits in length and contains a value that is a TSID. Note that the MSB (bit 4 in TS Info field) of the TSID subfield is always set to 1 when the TSPEC element is included within an ADDTS Response Action frame.
- The Direction subfield specifies the direction of data carried by the TS as defined in Table 8-107.

Change Table 8-110 as follows:

Table 8-110—Setting of Schedule subfield

APSD	Schedule	Usage
0	0	No Schedule
1	0	Unscheduled APSD
0	1	Scheduled PSMP <u>or GCR-SP</u>
1	1	Scheduled APSD

Change paragraphs 7 and 8 of 8.4.2.32 as follows:

The Minimum Service Interval field is 4 octets long and contains an unsigned integer that specifies the minimum interval, in microseconds, between the start of two successive SPs. If the TSPEC element is included within a GCR Request subelement that has the GCR delivery method equal to GCR-SP, a Minimum Service Interval field value of 0 indicates that SPs up to the maximum service interval are requested, including the continuous SP used by the GCR-A delivery method.

The Maximum Service Interval field is 4 octets long and contains an unsigned integer that specifies the maximum interval, in microseconds, between the start of two successive SPs. The Maximum Service Interval field is greater than or equal to the Minimum Service Interval field. If the TSPEC element is included within a GCR Request subelement that has the GCR delivery method equal to GCR-SP, a Maximum Service Interval field value of 0 indicates that the continuous SP used by the GCR-A delivery method is requested.

Change paragraph 11 of 8.4.2.32 as follows:

The Service Start Time field is 4 octets and contains an unsigned integer that specifies the time, expressed in microseconds, when the first scheduled SP starts. The service start time indicates to the AP the time when a STA first expects to be ready to send frames and a power-saving STA needs to be awake to receive frames. This may help the AP to schedule service so that the MSDUs encounter small delays in the MAC and help the power-saving STAs to reduce power consumption. The field represents the four lower order octets of the TSF timer at the start of the SP. If APSD and Schedule subfields ~~is~~ are 0, this field is also set to 0 (unspecified).

8.4.2.36 Schedule element

Change the first paragraph of 8.4.2.36 as follows:

The Schedule element is transmitted by the HC to a STA to announce the schedule that the HC/AP follows for admitted streams originating from or destined to that STA, or GCR-SP streams destined to that STA, in the future. The information in this element may be used by the STA for power management, internal scheduling, or any other purpose. The element information format is shown in Figure 8-211.

Change the third paragraph of 8.4.2.36 as follows:

The Aggregation subfield is set to 1 if the schedule is an aggregate schedule for all TSIDs associated with the STA to which the frame is directed. It is set to 0 otherwise. The TSID subfield is as defined in 8.2.4.5.2 and indicates the TSID for which this schedule applies. The TSID subfield is reserved when the Schedule element is included within a GCR Response subelement. The Direction subfield is as defined in 8.4.2.32 and defines the direction of the TSPEC associated with the schedule. For a Schedule element sent within a GCR Response subelement, the Direction subfield is set to “Downlink.” The TSID and Direction subfields are valid only when the Aggregation subfield is 0. If the Aggregation subfield is 1, the TSID and Direction subfields are reserved.

Change the fifth paragraph of 8.4.2.36 as follows:

The Service Interval field is 4 octets and indicates the time, expressed in microseconds, between two successive SPs and represents the measured time from the start of one SP to the start of the next SP. If the Schedule element is included within a GCR Response subelement that has the GCR delivery method equal to GCR-SP, a value of 0 in the Service Interval field indicates the delivery method is GCR-A.

Change the seventh paragraph of 8.4.2.36 as follows:

The HC may set both the Service Start Time field and the Service Interval field to 0 (unspecified) for non-powersaving STAs, except when the Schedule element is included within a GCR Response subelement that has the GCR delivery method equal to GCR-SP. When the Schedule element is included within a GCR Response subelement that has the GCR delivery method equal to GCR-SP, the Service Start Time field is not set to 0 and the Service Interval field might be set to 0.

8.4.2.90 DMS Request element

Change paragraphs 8, 9, and 10 of 8.4.2.90 as follows:

When the Request Type field contains “Add,” the TCLAS Elements field contains one or more TCLAS elements to specify group addressed frames as defined in 8.4.2.33. When a GCR Request subelement is included in the DMS Descriptor and the Request Type field is equal to “Add,” the TCLAS Elements field contains at least a TCLAS element with frame classifier type set to 0 (Ethernet parameters) to specify a destination group address as defined in 8.4.2.33. When the Request Type field contains any value other than “Add,” the TCLAS Elements field contains zero TCLAS elements.

When the Request Type field contains “Add” and when there are two or more TCLAS elements present, the TCLAS Processing Element field contains one TCLAS Processing element to define how these TCLAS elements are to be processed, as defined in 8.4.2.35. Otherwise, the TCLAS Processing Element field contains zero TCLAS Processing elements.

When the Request Type field contains “Add” or “Change,” the TSPEC Element field optionally contains one TSPEC element to specify the characteristics and QoS expectations of the corresponding traffic flow as defined in 8.4.2.32. When a GCR Request subelement is included in the DMS Descriptor and the Request Type field is equal to “Add” or “Change,” the TSPEC Element field contains one TSPEC element. Otherwise, the TSPEC Element field contains zero TSPEC elements.

Change Table 8-170 as follows:

Table 8-170—Optional Subelement IDs for DMS Descriptor

Subelement ID	Name	Length field (octets)	Extensible
0–220	Reserved		
1	<u>GCR Request</u>	2	<u>Yes</u>
2–220	<u>Reserved</u>		
221	Vendor Specific	3 to 248	
222–255	Reserved		

Insert the following paragraphs (including Figure 8-346a, Table 8-170a, and Table 8-170b) before the last paragraph (“The DMS Request element ...”) in 8.4.2.90:

Each DMS Descriptor contains zero or one GCR Request subelements. If present and the Request Type field is equal to “Add” or “Change,” the GCR Request subelement indicates a request by a STA to respectively add or change the GCR service for a group addressed stream identified by the TCLAS element or by the DMSID in the DMS Descriptor. The format of the GCR Request subelement is shown in Figure 8-346a.

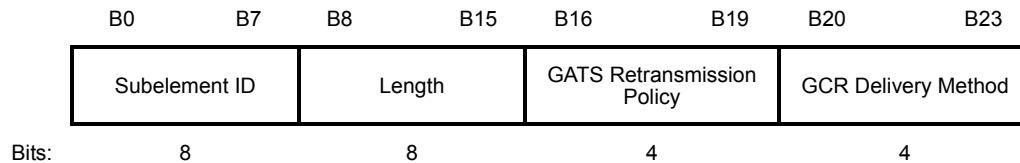


Figure 8-346a—GCR Request subelement field format

The Length field of the GCR Request subelement is set to 1.

The GATS Retransmission Policy field is set to indicate the STA’s preferred retransmission policy for the group address for which the GCR service is requested. The values are shown in Table 8-170a.

Table 8-170a—GATS Retransmission Policy field values

Value	GATS retransmission policy	Notes
0	No preference	
1	DMS	See 10.23.15.2.
2	GCR unsolicited retry	See 10.23.15.3.6.
3	GCR Block Ack	See 10.23.15.3.7.
4–15	Reserved	

The GCR Delivery Method field is set to indicate the STA's preferred delivery method for the group address for which the GCR service is requested. The values are shown in Table 8-170b.

Table 8-170b—GCR Delivery Method field values

Value	GCR delivery method	Notes
0	No preference	
1	Non-GCR-SP	See 10.23.15.3.1.
2	GCR-SP	See 10.23.15.3.8.
3–15	Reserved	

8.4.2.91 DMS Response element

Change the fifth paragraph of 8.4.2.91 as follows:

The DMSID field is assigned by the AP and provides a unique identifier within the BSS for the DMS traffic flow identified by the TCLAS Elements, TCLAS Processing Element, and TSPEC Element fields. The uniqueness of this identifier is independent of the ordering of the TCLAS elements. In a mesh BSS, the DMSID field is assigned by a mesh STA that responds to a GCR request and is unique among all existing DMSIDs used by the mesh STA for its current GCR agreements.

Change the seventh paragraph of 8.4.2.91 as follows:

The Response Type field indicates the response type returned by the AP responding to the non-AP STA's request or by a mesh STA responding to its peer mesh STA's request or indicates the DMS Status is an advertisement of an existing GCR service, as indicated in Table 8-171.

Change Table 8-171 as follows:

Table 8-171—Response Type field values

Field value	Description	Notes
0	Accept	AP STA accepts the DMS <u>or GCR</u> request.
1	Denied	AP STA rejects the DMS <u>or GCR</u> request.
2	Terminate	AP STA terminates the previously accepted DMS <u>or GCR</u> request.
<u>3</u>	<u>GCR Advertise</u>	<u>STA advertises a group addressed stream subject to an existing GCR agreement.</u>
34 –255	Reserved	

Change paragraphs 8 to 12 of 8.4.2.91 as follows:

When the Last Sequence Control field is not supported, the Last Sequence Control field is set to 65 535. When the Last Sequence Control field is supported and the Response Type field does not contain “Terminate;” or “GCR Advertise;” the Last Sequence Control field is reserved.

When the Response Type field is “Terminate” and the Last Sequence Control field is supported, Bit 0 to Bit 3 of the Last Sequence Control field is 0, and Bit 4 to Bit 15 of the Last Sequence Control field contains the sequence number of the last group addressed frame that the AP ~~converted to an individually addressed frame and sent successfully delivered~~ to the non-AP STA that is the recipient of the DMS Response Frame. If the Response Type field is “Terminate” and the this-last frame received by the non-AP STA prior to DMS termination has not also been sent using a group addressed frame, the Last Sequence Control field is set to 65 534.

When the Response Type field contains “Accept” or “Denied;” and a GCR Response subelement is not included in the DMS Status field, the TCLAS Elements field contains one or more TCLAS elements to specify group addressed frames as defined in 8.4.2.33. When the Response Type field is equal to “Accept,” “Denied,” or “GCR Advertise” and a GCR Response subelement is included in the DMS Status field, the TCLAS Elements field contains at least one TCLAS element with frame classifier type set to 0 (Ethernet parameters) to specify a destination group address as defined in 8.4.2.33. Otherwise, the TCLAS Elements field contains zero TCLAS elements.

When the Response Type field contains “Accept” or “Denied,” the TCLAS Processing Element field optionally contains one TCLAS Processing element to define how these TCLAS elements are to be processed, as defined in 8.4.2.35. When the Response Type field contains “Terminate” or when there is only one TCLAS element, the TCLAS Processing Element field contains zero TCLAS Processing elements.

When the Response Type field contains “Accept” or “Denied,” the TSPEC Element field optionally contains one TSPEC element to specify the characteristics and QoS expectations of the corresponding traffic flow as defined in 8.4.2.32. When a GCR Response subelement is included in the DMS Status field and the Response Type field is equal to “Accept,” “Denied,” or “GCR Advertise,” the TSPEC Element field contains one TSPEC element. Otherwise, the TSPEC Element field contains zero TSPEC elements.

Change Table 8-172 as follows:

Table 8-172—Optional Subelement IDs for DMS Status

Subelement ID	Name	Length field (octets)	Extensible
0–220	Reserved		
1	<u>GCR Response</u>	<u>1 to 22</u>	<u>Subelements</u>
<u>2–220</u>	<u>Reserved</u>		
221	Vendor Specific	3 to 248	
222–255	Reserved		

Insert the following paragraphs (including Figure 8-348a) before the last paragraph (“The DMS Response element”) in 8.4.2.91:

The GCR Response subelement contains one of the following:

- A response by an AP to a GCR request by a non-AP STA for GCR service for a group address
- A response by a mesh STA to a GCR request by a peer mesh STA for GCR service for a group address
- An unsolicited advertisement for the parameters of a group addressed stream subject to the GCR service

The format of the GCR Response subelement is shown in Figure 8-348a.

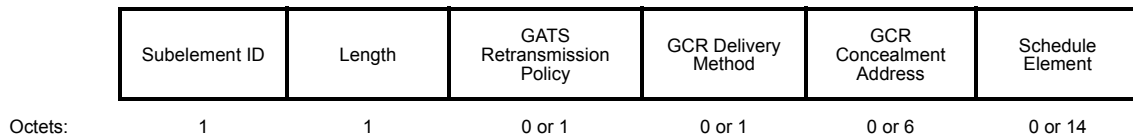


Figure 8-348a—GCR Response subelement field format

The GATS Retransmission Policy, GCR Delivery Method, and GCR Concealment Address fields are present when the Response Type field is not equal to “Denied”; otherwise, they are omitted. The Schedule Element field may be present when the Response Type field is not equal to “Denied.”

The GATS Retransmission Policy field is set to indicate the current GCR retransmission policy for the group address for which the GCR service is requested. The values are shown in Table 8-170a.

The GCR Delivery method field is set to indicate the current GCR Delivery method for the group address for which the GCR service is requested. The values are shown in Table 8-170b.

The GCR Concealment Address field, when present, indicates the GCR concealment address, as described in 10.23.15.3.5.

The Schedule Element field is present if the GCR delivery method is equal to GCR-SP. It indicates the current SP schedule for the group addressed stream (see 8.4.2.36).

Insert the following subclauses, 8.4.2.123 to 8.4.2.128 (including Figure 8-401d to Figure 8-401k and Table 8-183a to Table 8-183e), after 8.4.2.122:

8.4.2.123 Intra-Access Category Priority element

The Intra-Access Category Priority element provides information from a non-AP STA to an AP on the relative priorities of streams within an AC, as described in 9.2.4.2 and 10.26.2. This element may be included in ADDTS Request, QoS Map Configure, or SCS Request frames. The Intra-Access Category Priority element is defined in Figure 8-401d.

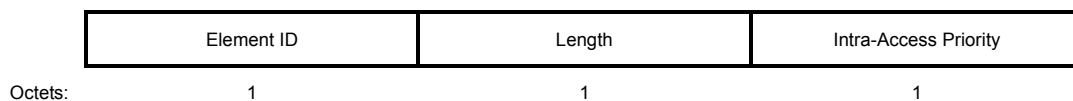


Figure 8-401d—Intra-Access Category Priority element format

The Element ID field is set to the value for Intra-Access Category Priority element as specified in Table 8-54.

The Length field is set to 1.

The Intra-Access Priority field is defined in Figure 8-401e.

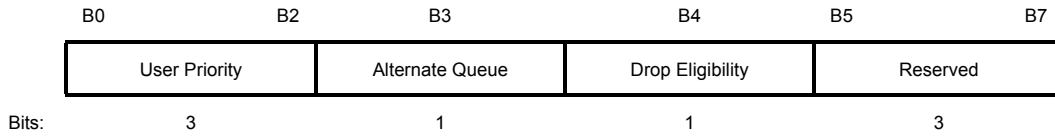


Figure 8-401e—Intra-Access Priority field format

The User Priority subfield indicates the desired UP of MSDUs or A-MSDUs of the stream to which this Intra-Access Category Priority element relates.

The Alternate Queue subfield indicates the intended primary or alternate EDCA queue that is used for this stream. When dot11AlternateEDCAActivated is false, this subfield is reserved. When the Alternate Queue subfield is set to 0, the primary EDCA queue for this AC is used. When the Alternate Queue subfield is equal to 1, the Alternate EDCA queue for this AC (see 9.2.4.2) is used.

The Drop Eligibility subfield is 1 bit in length and is used to indicate the suitability of this TS to be discarded if there are insufficient resources. If there are insufficient resources, a STA should discard the MSDUs or A-MSDUs of a TS with a Drop Eligibility subfield equal to 1, in preference to MSDUs or A-MSDUs of a TS whose Drop Eligibility subfield is equal to 0. See 10.6.2. The mechanisms for determining whether the resources are insufficient or when to discard MSDUs or A-MSDUs are beyond the scope of this standard.

8.4.2.124 SCS Descriptor element

The SCS Descriptor element defines information about the stream that is being classified using the procedures defined in 10.26.2. The format of the SCS Descriptor element is shown in Figure 8-401f.

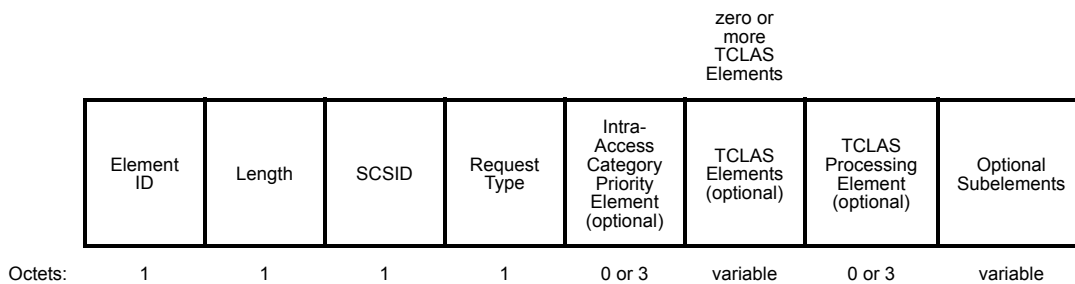


Figure 8-401f—SCS Descriptor element format

The Element ID field is set to the SCS Descriptor value in Table 8-54.

The element is variable in length. The length of the element is indicated by the Length field.

The SCSID field is set to a nonzero value chosen by the non-AP STA identifying the SCS stream specified in this SCS Descriptor element.

The Request Type field is set to a number to identify the type of SCS request. The Request Types are shown in Table 8-183a.

Table 8-183a—Request Type definitions

Name	Usage mode
Add	0
Remove	1
Change	2
Reserved	3–255

The Intra-Access Category Priority Element field is present when Request Type field is equal to “Add” or “Change” and is defined in 8.4.2.123.

The TCLAS Elements field contains zero or more TCLAS elements to specify how incoming MSDUs are classified as part of this SCS stream, as defined in 8.4.2.33. One or more TCLAS elements are present when Request Type field is equal to “Add” or “Change,” and no TCLAS elements are present when Request Type field is equal to “Remove.”

The TCLAS Processing Element field is present when more than one TCLAS elements are present and defines how multiple TCLAS elements are to be processed, as defined in 8.4.2.35.

The Optional Subelements field format contains zero or more subelements, each consisting of a 1-octet Subelement ID field, a 1-octet Length field, and a variable-length Data field, as shown in Figure 8-402. Any optional subelements are ordered by nondecreasing subelement ID.

The Optional Subelement ID field values for the defined optional subelements are shown in Table 8-183b. A “Yes” in the Extensible column of a subelement listed in Table 8-183b indicates that the length of the subelement might be extended in future revisions or amendments of this standard. When the Extensible column of an element is equal to “Subelements,” then the subelement might be extended in future revisions or amendments of this standard by defining additional subelements within the subelement. See 9.24.9.

Table 8-183b—Optional Subelement IDs for SCS Descriptor element

Subelement ID	Name	Length field (octets)	Extensible
0–220	Reserved		
221	Vendor Specific	1 to 244	
222–255	Reserved		

The SCS Descriptor element is included in SCS Request frames, as described in 8.5.19.2. The use of the SCS Descriptor element and SCS Request frames is described in 10.26.2.

8.4.2.125 QLoad Report element

8.4.2.125.1 QLoad Report element format

The QLoad Report element contains the set of parameters necessary to support OBSS management. The format of the QLoad Report element is provided in Figure 8-401g.

	Element ID	Length	Potential Traffic Self	Allocated Traffic Self	Allocated Traffic Shared	EDCA Access Factor	HCCA Peak	HCCA Access Factor	Overlap	Sharing Policy	Optional Subelements
Octets:	1	1	5	5	5	1	2	1	1	1	Variable

Figure 8-401g—QLoad Report element format

The Element ID field is set to the value for QLoad Report element as specified in Table 8-54.

The element is variable in length. The length of the element is indicated by the Length field.

Potential Traffic Self, Allocated Traffic Self, and Allocated Traffic Shared fields use the QLoad field format as described in 8.4.2.125.2.

The Potential Traffic Self field represents the peak composite QoS traffic for this BSS if all the potential admission control and HCCA TSPECs from the non-AP STAs are active. The methods for gathering the total potential TSPEC information are described in 10.27.2.

The Allocated Traffic Self field represents the composite QoS traffic for this BSS based upon all the admission control and HCCA TSPECs admitted within the same BSS, as described in 10.27.2.

The Allocated Traffic Shared field represents the sum of the Allocated Traffic Self field values that have been received or obtained from other APs whose beacons have been detected or obtained within the last 100 beacon periods, plus the Allocated Traffic Self field value of the AP itself. Computation of the values represented in the Allocated Traffic Shared field is described in 10.27.2.

As described in 10.27.2, the EDCA Access Factor field value is the sum of the Potential Traffic Self field values that have been received or obtained from other APs, plus the Potential Traffic Self field value of the AP itself, minus the sum of the HCCA Peak field values that have been received or obtained from overlapping APs, minus the HCCA Peak field value of the AP itself. The EDCA Access Factor is expressed as a fraction rounded down to a multiple of 1/64. When the EDCA Access Factor is greater than 254/64, the EDCA Access Factor field is set to 255.

The HCCA Peak field is the total peak HCCA TXOP requirement, over a period of 1 s, for the AP and BSS, for all the HCCA TSPECs that are included in the QLoad. HCCA Peak is expressed in multiples of 32 μ s over a period of 1 s. The HCCA Peak field is reserved if HCCA is not supported.

NOTE—Because the HCCA peak is calculated over 1 s periods, its value might be an underestimate of the instantaneous peak of interactive variable bit rate (VBR) flows.

The HCCA Access Factor field value is the sum of the HCCA Peak field values in the QLoad Report elements that have been received from the APs of OBSSs, plus the HCCA Peak field value of the AP itself, as described in 10.27.2. It is expressed as a fraction rounded down to a multiple of 1/64. When the HCCA Access Factor is greater than 254/64, the HCCA Access Factor field is set to 255.

The Overlap field indicates the number of other APs that are sharing the same channel and whose beacons have been detected or obtained within the last 100 beacon periods by the AP issuing this beacon.

The Sharing Policy field contains the currently active sharing policy. The values for the Sharing Policy field are described in Table 8-183c.

Table 8-183c—Sharing Policy definitions

Sharing Policy field value	Current sharing policy
0	Not specified
1	Static
2	Dynamic
3–220	Reserved
221	Vendor Specific
222–255	Reserved

The Optional Subelements field format contains zero or more subelements, each consisting of a 1-octet Subelement ID field, a 1-octet Length field, and a variable-length Data field, as shown in Figure 8-402. Any optional subelements are ordered by nondecreasing subelement ID.

The Subelement ID field values for the defined optional subelements are shown in Table 8-183d. A “Yes” in the Extensible column of a subelement listed in Table 8-183d indicates that the length of the subelement might be extended in future revisions or amendments of this standard. When the Extensible column of an element is equal to “Subelements,” then the subelement might be extended in future revisions or amendments of this standard by defining additional subelements within the subelement. See 9.24.9.

Table 8-183d—Optional Subelement IDs for QLoad Report element

Subelement ID	Name	Length field (octets)	Extensible
0–220	Reserved		
221	Vendor Specific	3 to 248	
222–255	Reserved		

8.4.2.125.2 QLoad field format

The QLoad field format is described in Figure 8-401h.

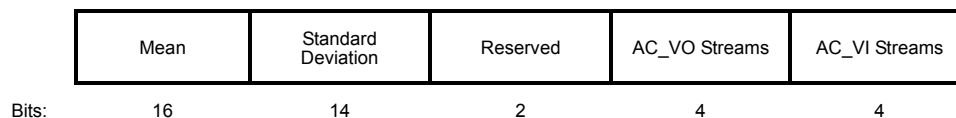


Figure 8-401h—QLoad field format

The Mean subfield represents the amount of time admitted, or the amount of time scheduled traffic requires to access the medium, in units of 32 μ s per second. In the case of EDCA admission control, this value is the sum of the admitted medium times, and for HCCA it is the total TXOP time required per second (see X.2.2).

If the mean medium time is larger than $2\,097\,088\ \mu\text{s}$ ($65\,534 \times 32$), the Mean subfield is set to 0xFFFE. The Mean subfield is set to 0xFFFF to indicate that the mean medium time is unknown.

The Standard Deviation subfield indicates the standard deviation from the mean medium time and is expressed in units of $32\ \mu\text{s}$ per second. If the standard deviation is larger than $8128\ \mu\text{s}$ (254×32), the Standard Deviation subfield is set to 0xFFFE. The Standard Deviation subfield is set to 0x3FFF to indicate that the standard deviation from the mean is unknown.

The AC_VO Streams subfield indicates the number of TSs using explicit admission control for AC_VO in the QoS traffic load report. Bidirectional streams are counted as two streams. If the number of admitted AC_VO streams is larger than 14, the AC_VO Streams subfield is set to 0xE. The AC_VO Streams subfield is set to 0xF to indicate that the number of TSs using explicit admission control for AC_VO is unknown.

The AC_VI Streams subfield indicates the number of TSs using explicit admission control for AC_VI in the QoS traffic load report. Bidirectional streams are counted as two streams. If the number of TSs using explicit admission control for AC_VO is larger than 14, the AC_VI Streams subfield is set to 0xE. The AC_VI Streams subfield is set to 0xF to indicate that the number of TSs using explicit admission control for AC_VI is unknown.

See 10.27.2 and Annex X.

8.4.2.126 HCCA TXOP Update Count element

The HCCA TXOP Update Count element is used by an AP to advertise its change in TXOP schedule. The format is provided in Figure 8-401i.

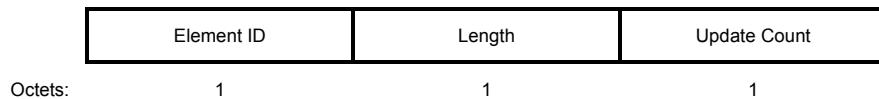


Figure 8-401i—HCCA TXOP Update Count element format

The Element ID field is set to the value given in Table 8-51.

The Length field is set to 1.

The Update Count field is described in 10.27.3 and is used to indicate that a change has occurred in the number of active HCCA or HEMM TSs.

8.4.2.127 Higher Layer Stream ID element

The Higher Layer Stream ID element identifies a stream from a higher layer protocol. This element is used to bind messages that are exchanged in order to complete a procedure, e.g., messages exchanged in an AP-initiated TS setup procedure. See 10.4.4.3. The format is provided in Figure 8-401j.

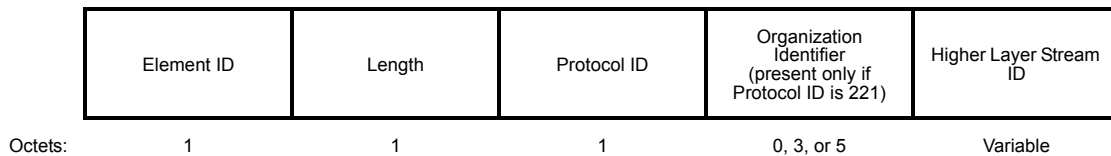


Figure 8-104j—Higher Layer Stream ID element format

The Element ID field is set to the Higher Layer Stream ID value identified in Table 8-54.

The value of the Length field is variable.

The Protocol ID field identifies the higher layer protocol to which the stream belongs. The values defined for the Protocol ID field are described in Table 8-183e.

Table 8-183e—Protocol ID definitions

Protocol ID	Protocol	Description
0	Reserved	
1	IEEE 802.1Q SRP	Protocol is IEEE 802.1Q SRP, and the corresponding Stream ID is 8 octets long.
2–220	Reserved	
221	Vendor Specific	Corresponding Organization Identifier field is included in the element.
222–255	Reserved	

The Organization Identifier field is present when the Protocol ID field is equal to 221 and contains a public OUI assigned by IEEE. The identifier is specified in 8.4.1.31. The order of the Organization Identifier field is described in 8.2.2.

The Higher Layer Stream ID field is an octet string and is defined by the higher layer protocol specified in the Protocol ID field.

8.4.2.128 GCR Group Address element

The GCR Group Address element defines information about group addressed frames to be transmitted using the GCR service. The format of the GCR Group Address element is shown in Figure 8-401k.

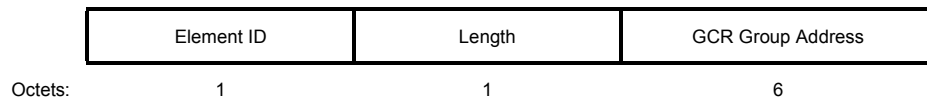


Figure 8-401k—GCR Group Address element format

The Element ID field is set to the GCR Group Address value identified in Table 8-54.

The Length field is set to 6.

GCR Group Address field is the MAC address of the GCR group.

8.5 Action frame format details

8.5.3 QoS Action frame details

8.5.3.1 General

In Table 8-192, insert values 5 and 6 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-192—QoS Action field values

QoS Action field value	Meaning
5	ADDTS Reserve Request
6	ADDTS Reserve Response

8.5.3.2 ADDTS Request frame format

Change Table 8-193 as follows:

Table 8-193—ADDTS Request frame Action field format

Order	Information	Notes
1	Category	
2	QoS Action	
3	Dialog token	
4	TSPEC	
5–n	TCLAS (optional)	<u>Optional</u>
n + 1	TCLAS processing (optional)	<u>Optional</u>
n + 2	U-APSD Coexistence (optional)	<u>Optional</u>
n + 3	Expedited Bandwidth Request element (optional)	<u>Optional</u>
<u>n + 4</u>	<u>Intra-Access Category Priority element</u>	<u>Optional</u>
<u>n + 5</u>	<u>Higher Layer Stream ID element</u>	<u>Only in AP-initiated TS setup</u>

Insert the following paragraphs at the end of 8.5.3.2:

There may be one Intra-Access Category Priority element, which is defined in 8.4.2.123 and described in 10.4.1.

The Higher Layer Stream ID element (8.4.2.127) provides the stream identifier from a higher layer protocol. The Higher Layer Stream ID element is present only in the AP-initiated TS setup (10.4.4.3).

8.5.3.3 ADDTS Response frame format*Change Table 8-194 as follows:***Table 8-194—ADDTS Response frame Action field format**

Order	Information	Notes
1	Category	
2	QoS Action	
3	Dialog Token	
4	Status Code	
5	TS Delay	
6	TSPEC	
7–n	TCLAS (optional)	<u>Optional</u>
n + 1	TCLAS Processing (optional)	<u>Optional</u>
n + 2	Schedule	<u>Only if the status code is equal to 0</u>
n + 3	Expedited Bandwidth Request (optional)	<u>Optional</u>
<u>n + 4</u>	<u>Higher Layer Stream ID</u>	<u>Only in AP-initiated TS setup</u>

Insert the following paragraph at the end of 8.5.3.3:

The Higher Layer Stream ID element is present only in AP-initiated TS setup. The Higher Layer Stream ID element (8.4.2.127) contains the stream identifier provided by a higher layer protocol.

8.5.3.6 QoS Map Configure frame format*Change Table 8-197 as follows:***Table 8-197—QoS Map configure frame body**

Order	Information
0	Category
1	QoS Action
2	QoS Map Set
<u>3–n</u>	<u>Intra-Access Category Priority elements (optional)</u>

Insert the following paragraph at the end of 8.5.3.6:

There may be zero or more Intra-Access Category Priority elements, which are defined in 8.4.2.123.

Insert the following subclauses, 8.5.3.7 and 8.5.3.8 (including Table 8-197a and Table 8-197b), after 8.5.3.6:

8.5.3.7 ADDTS Reserve Request frame format

The ADDTS Reserve Request frame is transmitted by an AP to a non-AP STA in response to a higher layer protocol. See 19.4.4.3.

The Action field of the ADDTS Reserve Request frame contains the information shown in Table 8-197a.

Table 8-197a—ADDTS Reserve Request frame Action field format

Order	Information
1	Category
2	QoS Action
3	TSPEC
4	Schedule
5	Higher Layer Stream ID

The Category field is set to 1 (representing QoS).

The QoS Action field is set to the value in Table 8-192 representing ADDTS Reserve Request.

The TSPEC element contains the QoS parameters that define the TS. The QoS parameters in the TSPEC are equivalent to the QoS parameters of the higher level stream identified by the Higher Level Stream ID. The TS is identified by the TSID and Direction fields within the TSPEC element.

The Schedule element is defined in 8.4.2.36 and set to reflect schedule information corresponding to the TSPEC specification.

The Higher Layer Stream ID element (defined in 8.4.2.127) provides the stream identifier from a higher layer protocol.

8.5.3.8 ADDTS Reserve Response frame format

An ADDTS Reserve Response frame is used by a non-AP STA to indicate the completion of an AP-initiated TS setup procedure (10.4.4.3). The Action field of the ADDTS Reserve Response frame contains the information shown in Table 8-197b.

Table 8-197b—ADDTS Reserve Response frame Action field format

Order	Information
1	Category
2	QoS Action
3	Higher Layer Stream ID
4	Status Code

The Category field is set to 1 (representing QoS).

The QoS Action field is set to the value specified in Table 8-192 representing ADDTS Reserve Response.

The Higher Layer Stream ID is defined in 8.4.2.127.

The Status Code field is defined in 8.4.1.9.

8.5.5 Block Ack Action frame details

8.5.5.1 General

Change the first paragraph of 8.5.5.1 as follows:

The ADDBA frames are used to set up or, if PBAC is used, to modify Block Ack for a specific TC, TS, or GCR group address. A Block Ack Action field, in the octet immediately after the Category field, differentiates the Block Ack Action frame formats. The Block Ack Action field values associated with each frame format within the Block Ack category are defined in Table 8-193.

8.5.5.2 ADDBA Request frame format

Insert order 7 in numeric order into Table 8-203 (note that the entire table is not shown here):

Table 8-203—ADDBA Request frame Action field format

Order	Information
7	GCR Group Address element (optional)

Insert the following paragraphs at the end of 8.5.5.2:

If the GCR Group Address element is present, the TID field within the Block Ack Parameter Set field is reserved.

The GCR Group Address element contains the group address for which a Block Ack agreement is requested.

8.5.5.3 ADDBA Response frame format

Insert order 7 in numeric order into Table 8-204 (note that the entire table is not shown here):

Table 8-204—ADDBA Response frame Action field format

Order	Information
7	GCR Group Address element (optional)

Insert the following paragraphs at the end of 8.5.5.3:

If the GCR Group Address element is present, the TID field within the Block Ack Parameter Set field is reserved.

The GCR Group Address element contains the group address for which a Block Ack agreement is requested.

8.5.5.4 DELBA frame format

Insert order 5 in numeric order into Table 8-205 (note that the entire table is not shown here):

Table 8-205—DELBA frame Action field values

Order	Information
5	DELBA GCR Group Address

Insert the following paragraph at the end of 8.5.5.4:

The DELBA GCR Group Address field is a 6-octet field equal to the GCR group address whose Block Ack agreement is being terminated.

8.5.8 Public Action details

8.5.8.1 Public Action frames

In Table 8-210, insert values 20 to 24 in numeric order, and update the reserve values accordingly (note that the entire table is not shown here):

Table 8-210—Public Action field values

Public Action field value	Description
20	QLoad Request
21	QLoad Report
22	HCCA TXOP Advertisement
23	HCCA TXOP Response
24	Public Key

Insert the following subclauses, 8.5.8.20 to 8.5.8.24 (including Table 8-221a to Table 8-221c and Figure 8-460c to Figure 8-460e), after 8.5.8.19:

8.5.8.20 QLoad Request frame format

The QLoad Request frame is transmitted by an AP to request information from another AP. The Action field format of the QLoad Request frame is shown in Table 8-221a.

Table 8-221a—QLoad Request frame Action field format

Order	Information
1	Category
2	Public Action
3	Dialog Token
4	QLoad Report element

The Category field is set to the value indicating a Public Action frame, as specified in Table 8-38.

The Public Action field is set to the value specified in Table 8-210 for a QLoad Request frame.

The Dialog Token field is defined in 8.4.1.12 and set by the requesting STA to a nonzero value that is used for matching action responses with action requests. See 9.24.5.

The QLoad Report element is defined in 8.4.2.125 and contains the QLoad report corresponding to the AP sending the request.

8.5.8.21 QLoad Report frame format

The QLoad Report frame is transmitted by an AP responding to a QLoad Request frame. The Action field format of the QLoad Report frame is shown in Table 8-221b.

Table 8-221b—QLoad Report frame Action field format

Order	Information
1	Category
2	Public Action
3	Dialog Token
4	QLoad Report element

The Category field is set to the value indicating a Public Action frame, as specified in Table 8-38.

The Public Action field is set to the value specified in Table 8-210 for a QLoad Report frame.

The Dialog Token field is defined in 8.4.1.12 and set by the requesting STA to a nonzero value that is used for matching action responses with action requests. See 9.24.5. The Dialog Token field is set to 0 when an unsolicited QLoad Report frame is sent by the AP.

The QLoad Report element is defined in 8.4.2.125.

8.5.8.22 HCCA TXOP Advertisement frame

The HCCA TXOP Advertisement frame is transmitted by an AP to another AP to inform it of active and pending TXOP reservations. The Action field format of the HCCA TXOP Advertisement frame is shown in Figure 8-460c.

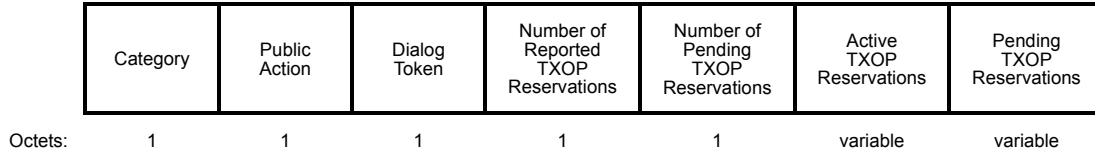


Figure 8-460c—HCCA TXOP Advertisement frame Action field format

The Category field is set to the value indicating a Public Action frame, as specified in Table 8-38.

The Public Action field is set to the value specified in Table 8-210 for an HCCA TXOP Advertisement frame.

The Dialog Token field is defined in 8.4.1.12 and is set by the AP to a nonzero value that is used for matching action responses with action requests. See 9.24.5.

The Number of Reported TXOP Reservations field is 1 octet in length and contains a positive integer that specifies the number of active TXOP reservations reported in this frame. A value of 0 indicates that no TXOP reservations are active.

The Number of Pending Reported TXOP Reservations field is 1 octet in length and contains a positive integer that specifies the number of pending TXOP reservations reported in this frame. A value of 0 indicates that no TXOP reservations are in the process of being activated.

The Active TXOP Reservation field contains zero or more TXOP Reservation fields as defined in 8.4.1.43. This field indicates active HCCA TXOPs that the AP has scheduled. The Start Time subfield of the TXOP Reservation field is relative to the TSF of the sending AP.

The Pending TXOP Reservation field contains zero or more TXOP Reservation fields as defined in 8.4.1.43. This field indicates new HCCA TXOPs that the AP is scheduling. The Start Time subfield of the TXOP Reservation field is relative to the TSF of the sending AP.

The use of the HCCA TXOP Advertisement frame is described in 10.27.3.

8.5.8.23 HCCA TXOP Response frame

The HCCA TXOP Response frame is transmitted by an AP to another AP to respond to a HCCA TXOP Advertisement frame. The Action field format of the HCCA TXOP Response frame is shown in Table 8-460d.

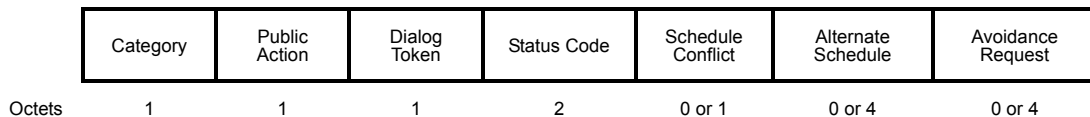


Figure 8-460d—HCCA TXOP Response frame Action field format

The Category field is set to the value indicating a Public Action frame, as specified in Table 8-38.

The Public Action field is set to the value specified in Table 8-210 for a HCCA TXOP Response frame.

The Dialog Token field is set to the value of the Dialog Token field from the corresponding HCCA TXOP Advertisement frame.

The Status Code field is defined in 8.4.1.9 and is set to either the value SUCCESS or TS_SCHEDULE_CONFLICT.

The Schedule Conflict field is present only when the Status Code field is nonzero. The Schedule Conflict field indicates the TXOP reservation from the HCCA TXOP Advertisement frame that conflicts with an existing or in-progress schedule. Its value is between 1 and the summation of the values from the Number of Reported TXOP Reservations and Number of Pending TXOP Reservations fields of the HCCA TXOP Advertisement frame. A value of 1 indicates the first TXOP reservation in the HCCA TXOP Advertisement frame, a value of 2 indicates the second TXOP reservation in the HCCA TXOP Advertisement frame, and so on. The value of zero is reserved.

The optional Alternate Schedule field is defined in 8.4.1.43 and is present only when the Status Code field is nonzero. When the Alternate Schedule field is present, it contains an alternate to the TXOP reservation given in the corresponding HCCA TXOP Advertisement frame. The Start Time subfield of the Alternate Schedule field is relative to the TSF of the destination AP.

The optional Avoidance Request field is defined in 8.4.1.43 and may be present when the Status Code field is nonzero. When the Avoidance Request field is present, it indicates a TXOP schedule that the AP sending the TXOP Response frame is requesting to be avoided by the AP that is the destination of the TXOP Response frame. The Start Time subfield of the Avoidance Request field is relative to the TSF of the destination AP.

The use of the HCCA TXOP Response frame is described in 10.27.3.

8.5.8.24 Public Key frame

The Public Key frame is transmitted by an AP to provide its public key to peer APs and to request the peer's public key. The format of the Public Key frame body is defined in Figure 8-460e.

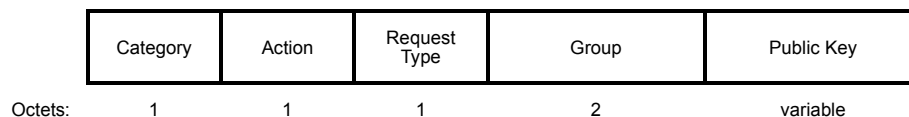


Figure 8-460e—Public Key frame body format

The Category field is set to the value indicating a Public Action frame, as specified in Table 8-38.

The Action field is set to the value specified in Table 8-210 for a Public Key frame.

The Request Type field is set to a number to identify the usage mode of this frame. The Request Types are shown in Table 8-221c.

The Request Type field is set to “Request” to indicate that a public key is being requested from a peer AP.

The Request Type field is set to “Response” to indicate that this frame is in response to a Public Key frame.

The Group field is used to indicate which cryptographic group was used when generating the public key and is defined in 8.4.1.40.

Table 8-221c—Request Type definitions

Name	Usage mode
Request	0
Response	1
Reserved	2–255

The Public Key field contains the public key of the AP that is sending this Public Key frame and is defined in 8.4.1.39.

The use of the Public Key frame is described in 11.10.

8.5.11 Protected Dual of Public Action frames

In Table 8-228, insert values 20 to 23 in numeric order, and update the reserved values accordingly (note that the entire table is not shown here):

Table 8-228—Public Action field values defined for Protected Dual of Public Action frames

Public Action field value	Description	Defined in
20	Protected QLoad Request	8.5.8.20
21	Protected QLoad Report	8.5.8.21
22	Protected HCCA TXOP Advertisement	8.5.8.22
23	Protected HCCA TXOP Response	8.5.8.23

8.5.14 WNM Action details

8.5.14.26 DMS Response frame format

Change the first paragraph of 8.5.14.26 as follows:

The DMS Response frame is sent by an AP or a mesh STA in response to a DMS Request frame, or autonomously to terminate a requested DMS stream, or to advertise the current parameters for one or more GCR streams. The format of the DMS Response frame is shown in Figure 8-497.

8.5.16 Self-protected Action frame details

8.5.16.2 Mesh Peering Open frame format

8.5.16.2.2 Mesh Peering Open frame details

Change Table 8-262 as indicated (note that the entire table is not shown here):

Table 8-262—Mesh Peering Open frame Action field format

Order	Information	Notes
8	RSN	The RSNE is present only if <u>dot11MeshSecurityActivated_</u> <u>dot11ProtectedQLoadReportActivated_</u> <u>dot11ProtectedTXOPNegotiationActivated</u> is true.
9	Mesh ID	The Mesh ID element is set as described in 8.4.2.101 <u>present when</u> <u>dot11MeshActivated</u> is true.
10	Mesh Configuration	The Mesh Configuration element is set as described in 8.4.2.100 <u>present when dot11MeshActivated</u> is true.
Last	Authenticated Mesh Peering Exchange	The Authenticated Mesh Peering Exchange element is present when <u>dot11MeshSecurityActivated_</u> <u>dot11ProtectedQLoadReportActivated_</u> <u>dot11ProtectedTXOPNegotiationActivated</u> is true and a PMK exists between the sender and recipient of this frame.

8.5.16.3 Mesh Peering Confirm frame format

8.5.16.3.2 Mesh Peering Confirm frame details

Change Table 8-263 as indicated (note that the entire table is not shown here):

Table 8-263—Mesh Peering Confirm frame Action field format

Order	Information	Notes
7	RSN	The RSNE is present only when <u>dot11MeshSecurityActivated_</u> <u>dot11ProtectedQLoadReportActivated_</u> <u>dot11ProtectedTXOPNegotiationActivated</u> is true.
8	Mesh ID	The Mesh ID element is set as described in 8.4.2.101 <u>present when</u> <u>dot11MeshActivated</u> is true.
9	Mesh Configuration	The Mesh Configuration element is set as described in 8.4.2.100 <u>present when dot11MeshActivated</u> is true.
Last – 1	MIC element	MIC element is present when <u>dot11MeshSecurityActivated_</u> <u>dot11ProtectedQLoadReportActivated_</u> <u>dot11ProtectedTXOPNegotiationActivated</u> is true and a PMK exists between the sender and recipient of this frame.
Last	Authenticated Mesh Peering Exchange	The Authenticated Mesh Peering Exchange element is present when <u>dot11MeshSecurityActivated_</u> <u>dot11ProtectedQloadReportActivated_</u> <u>dot11ProtectedTXOPNegotiationActivated</u> is true and a PMK exists between the sender and recipient of this frame.

8.5.16.4 Mesh Peering Close frame format

8.5.16.4.2 Mesh Peering Close frame details

Change Table 8-264 as indicated:

Table 8-264—Mesh Peering Close frame Action field format

Order	Information	Notes
1	Category	
2	Self-protected Action	
3	Mesh ID	The Mesh ID element is set as described in 8.4.2.104 present when <u>dot11MeshActivated is true</u> .
4	Mesh Peering Management	The Mesh Peering Management element is set as described in 8.4.2.104 present when <u>dot11MeshActivated is true</u> .
Last – 2	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements except MIC element and Authenticated Mesh Peering Exchange element.
Last – 1	MIC element	MIC element is present when <u>dot11MeshSecurityActivated_ dot11ProtectedQLoadReportActivated_ or dot11ProtectedTXOPNegotiationActivated</u> is true and a PMK exists between the sender and recipient of this frame.
Last	Authenticated Mesh Peering Exchange	The Authenticated Mesh Peering Exchange element is present when <u>dot11MeshSecurityActivated_ dot11ProtectedQLoadReportActivated_ or dot11ProtectedTXOPNegotiationActivated</u> is true and a PMK exists between the sender and recipient of this frame.

Insert the following subclauses, 8.5.19 to 8.5.19.5 (including Table 8-281a and Figure 8-502a to Figure 8-502e), after 8.5.18.3:

8.5.19 Robust AV Streaming Action frame details

8.5.19.1 General

Several Action frame formats are defined to support robust AV streaming. The Robust Action field values associated with each frame format within the robust AV streaming category are defined in Table 8-281a. The frame formats are defined in 8.5.19.2 to 8.5.19.5.

Table 8-281a—Robust AV streaming Robust Action field values

Robust Action field value	Meaning
0	SCS Request
1	SCS Response
2	Group Membership Request
3	Group Membership Response
4–255	Reserved

8.5.19.2 SCS Request frame format

SCS Request frames are used to request the creation, modification, or deletion of a stream classification using the procedures defined in 10.26.2.

The Action field of the SCS Request frame contains the information shown in Figure 8-502a.

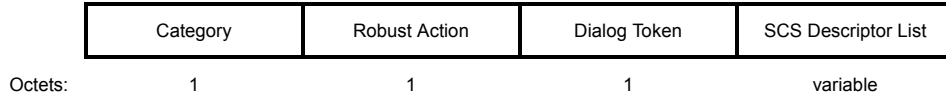


Figure 8-502a—SCS Request frame Action field format

The Category field is set to the value in Table 8-38 representing robust AV streaming.

The Robust Action field is set to the value specified in Table 8-281a for an SCS Request frame.

The Dialog Token field is defined in 8.4.1.12 and set by the requesting STA to a nonzero value that is used for matching action responses with action requests. See 9.24.5.

The SCS Descriptor List field contains one or more SCS Descriptor elements, as defined in 8.4.2.124.

8.5.19.3 SCS Response frame format

The SCS Response frame is sent in response to an SCS Request frame using the procedures defined in 10.26.2. The Action field of an SCS Response frame contains the information shown in Figure 8-502b.

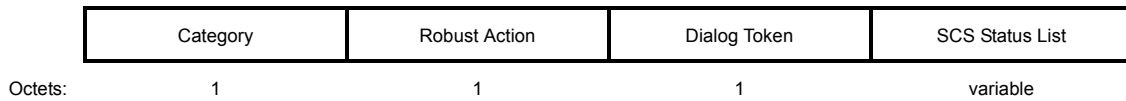


Figure 8-502b—SCS Response frame Action field format

The Category field is set to the value in Table 8-38 representing robust AV streaming.

The Robust Action field is set to the value specified in Table 8-281a for an SCS Response frame.

The Dialog Token field is set to the nonzero value of the corresponding SCS Request frame. If the SCS Report frame is being transmitted for a reason other than in response to an SCS Request frame, then the Dialog Token field is set to 0.

The SCS Status List field contains one or more SCS Status duples. The format of the SCS Status duple is defined in Figure 8-502c.

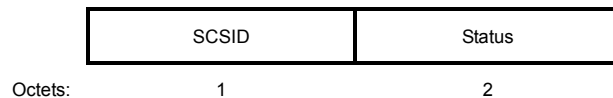


Figure 8-502c—SCS Status duple format

The SCSID field is set to the value of the SCSID field in the SCS Descriptor element received in the SCS Request frame.

The Status field indicates the status of the requested SCSID, as indicated in Table 8-37.

8.5.19.4 Group Membership Request frame format

The Group Membership Request frame is sent to a STA to request the contents of its dot11GroupAddressesTable. The Action field of a Group Membership Request frame contains the information shown in Figure 8-502d.

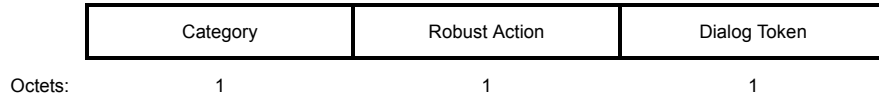


Table 8-502d—Group Membership Request frame Action field format

The Category field is set to the value in Table 8-38 representing robust AV streaming.

The Robust Action field is set to the value specified in Table 8-281a for a Group Membership Request frame.

The Dialog Token field is defined in 8.4.1.12 and set by the requesting STA to a nonzero value that is used for matching action responses with action requests. See 9.24.5.

Usage of the Group Membership Request frame is described in 10.23.15.3.2.

8.5.19.5 Group Membership Response frame format

The Group Membership Response frame is sent in response to a Group Membership Request frame or upon a change in the dot11GroupAddressesTable object, using the procedures defined in 10.23.15.3.2. The Action field of a Group Membership Response frame contains the information shown in Figure 8-502e.

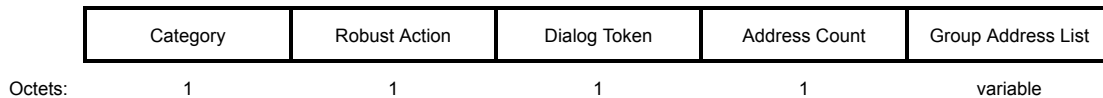


Figure 8-502e—Group Membership Response frame Action field format

The Category field is set to the value in Table 8-38 representing robust AV streaming.

The Robust Action field is set to the value specified in Table 8-281a for a Group Membership Response frame.

The Dialog Token field is set to the nonzero value of the corresponding Group Membership Request frame. If the Group Membership Report frame is being transmitted for a reason other than in response to a Group Membership Request frame, the Dialog Token field is set to 0.

The Address Count field specifies the number of MAC addresses that are in the Group Address List field.

The Group Address List field contains zero or more MAC addresses to indicate the set of group addressed MAC addresses for which the STA receives frames. Each MAC address is 6 octets in length, as described in 8.2.4.3.2.

9. MAC sublayer functional description

9.2 MAC architecture

9.2.4 Hybrid coordination function (HCF)


9.2.4.2 HCF contention-based channel access (EDCA)

Change the first paragraph of 9.2.4.2 as follows:

The EDCA mechanism provides differentiated, distributed access to the WM for STAs using eight different UPs. The EDCA mechanism defines four access categories (ACs) that provide support for the delivery of traffic with UPs at the STAs. Six transmit queues are defined when dot11AlternateEDCAActivated is true, and four transmit queues otherwise. The transmit queue and AC is-are derived from the UPs as shown in Table 9-1.

Change Table 9-1 as follows:

Table 9-1—UP-to-AC mappings

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	<u>Transmit queue (dot11Alternate- EDCAActivated false or not present)</u>	<u>Transmit queue (dot11Alternate- EDCAActivated true)</u>	Designation (informative)
Lowest  Highest	1	BK	AC_BK	<u>BK</u>	<u>BK</u>	Background
	2	—	AC_BK	<u>BK</u>	<u>BK</u>	Background
	0	BE	AC_BE	<u>BE</u>	<u>BE</u>	Best Effort
	3	EE	AC_BE	<u>BE</u>	<u>BE</u>	Best Effort
	4	CL	AC_VI	<u>VI</u>	<u>A_VI</u>	Video (<u>alternate</u>)
	5	VI	AC_VI	<u>VI</u>	<u>VI</u>	Video (<u>primary</u>)
	6	VO	AC_VO	<u>VO</u>	<u>VO</u>	Voice (<u>primary</u>)
	7	NC	AC_VO	<u>VO</u>	<u>A_VO</u>	Voice (<u>alternate</u>)

Insert the following paragraphs at the end of 9.2.4.2:

The alternate video (A_VI) and alternate voice (A_VO) transmit queues share the same EDCAF as VI and VO transmit queues, respectively, as shown in Figure 9-19a. When dot11AlternateEDCAActivated is true, a scheduling function above the VO EDCAF selects from the primary or alternate transmit queue an MSDU, an A-MSDU, an MMPDU, or set of MSDUs to be the next to be passed to the VO EDCAF (as shown in Figure 9-19a) so that the MSDU(s), A-MSDU(s), or MMPDU(s) from the queue with the higher UP are selected with a higher probability than from the queue with the lower UP. When dot11AlternateEDCAActivated is true, a scheduling function above the VI EDCAF selects from the primary or alternate transmit queue an MSDU, an A-MSDU, an MMPDU, or set of MSDUs to be the next to be passed to the VI EDCAF so that the MSDU(s), A-MSDU(s), or MMPDU(s) from the queue with the higher

UP are selected with a higher probability than from the queue with the lower UP. The default algorithm to select an MSDU, A-MSDU, or MMPDU from either the A_VI or VI queue and to select an MSDU, A-MSDU, or MMPDU from either the A_VO or VO queue is as follows:

- a) For each EDCAF, an MSDU, A-MSDU, or MMPDU is selected for transmission using the transmission selection procedures defined in 8.6.8 of IEEE Std 802.1Q-2011 using two queues, the primary and alternate.
- b) For a given AC, the order in which frames are selected for transmission shall maintain the requirements specified in 9.8 of this standard.

Alternative prioritization algorithms that meet the requirements of 9.8 may be used.

All MSDUs, A-MSDUs, and MMPDUs passed to the VO EDCAF are transmitted according to AC_VO EDCAF parameters and rules. All MSDUs, A-MSDUs, and MMPDUs passed to the VI EDCAF are transmitted according to AC_VI EDCAF parameters and rules.

9.3 DCF

Change the eighth paragraph of 9.3 as follows:

Except for MPDUs transmitted via the GCR service, the RTS/CTS mechanism cannot be used for MPDUs with group addressed immediate destination because there are multiple recipients for the RTS and thus potentially multiple concurrent senders of the CTS in response. For MPDUs transmitted via the GCR service, an RTS frame may be used if it is directed to a STA within the GCR group (see 9.19.2.6.2 and 9.21.10). The RTS/CTS mechanism is not used for every data frame transmission. Because the additional RTS and CTS frames add overhead inefficiency, the mechanism is not always justified, especially for short data frames.

9.3.2 Procedures common to the DCF and EDCAF

9.3.2.3 IFS

9.3.2.3.4 PIFS

Insert the following list item at the end of the dashed list after the second paragraph in 9.3.2.3.4:

- An AP continuing to transmit in a GCR Block Ack TXOP after the failure to receive a BlockAck as described in 9.21.10

9.3.2.8 ACK procedure

Insert the following note at the end of 9.3.2.8:

NOTE—The receiver STA performs the ACK procedure on all successfully received frames requiring acknowledgment, even if the frame is subsequently discarded due to drop eligibility (see DEI subfield in 8.2.4.6).

9.3.2.10 Duplicate detection and recovery

Change the seventh and eighth paragraphs of 9.3.2.10 as follows:

A receiving STA shall keep a cache of recently received <Address 2, sequence-number, fragment-number> tuples from frames that are not QoS Data frames. The receiving STA shall keep at least the most recent cache entry per <Address 2> value in this cache. A receiving QoS STA shall also keep a cache of recently received <Address 2, TID, sequence-number, fragment-number> tuples from QoS Data frames ~~for from all~~

STAs from which it has received QoS data frames. The receiving QoS STA shall keep at least the most recent cache entry per <Address 2, TID> pair in this cache. The receiving STA should maintain two additional caches, one containing entries of recently received <Address 2, sequence-number, fragment-number> tuples from received management frames that are not time priority management frames and the other containing entries of recently received <Address 2, sequence-number, fragment-number> tuples from received time priority management frames. The receiving STA should not include the entries in these two additional caches in any other caches. In each of these two caches, the receiving STA should keep at least the most recent cache entry per <Address 2 > value. A receiving STA with `dot11QMFActivated` false or not present and with `dot11RobustAVStreamingImplemented` false or not present should omit tuples obtained from group addressed and ATIM frames from all caches.

A receiving QMF STA shall also keep a cache of recently received <Address 2, AC, sequence-number, fragment-number> tuples from QMFs for all STAs from which the QoS STA has received QMFs. A receiving QMF STA is required to keep only the most recent cache entry per <Address 2, AC, sequence-number, fragment-number> for QMFs. A receiving QMF STA with `dot11RobustAVStreamingImplemented` false or not present shall omit from the caches all tuples obtained from group addressed data frames and tuples obtained from ATIM frames.

Insert the following paragraph after the ninth paragraph (“A receiving STA shall reject”) of 9.3.2.10:

A receiving non-mesh STA with `dot11RobustAVStreamingImplemented` true shall keep a cache entry per <DA, sequence-number> tuple for each group address subject to a GCR agreement. A receiving mesh STA with `dot11MeshGCRImplemented` true shall keep a cache entry per <DA, Address 2, sequence-number> tuple for each group address subject to a GCR agreement.

Insert the following note at the end of 9.3.2.10 after the existing note, and number the existing note as NOTE 1:

NOTE 2—Group addressed retransmissions of BUs use the same sequence number as the initial group addressed transmission of the BU. Unicast retransmissions of a group addressed BU delivered via DMS use the same sequence number as the initial unicast transmission of the BU. When a BU is delivered both using group addressing and unicast (e.g., when DMS is active but there are other associated STAs not using DMS), the sequence number might differ between the group addressed and unicast transmissions of the same BU.

9.3.6 Group addressed MPDU transfer procedure

Change 9.3.6 as follows:

In the absence of a PCF or use of the group addressed transmission service (GATS), when group addressed MPDUs in which the To DS field is 0 are transferred from a STA, only the basic access procedure shall be used. When group addressed MPDUs are not delivered using GATS, Regardless of the length of the frame, no RTS/CTS exchange shall be used, regardless of the length of the frame. In addition, no ACK shall be transmitted by any of the recipients of the frame. Any group addressed MPDUs in which the To DS field is 1 transferred from a STA shall, in addition to conforming to the basic access procedure of CSMA/CA, obey the rules for RTS/CTS exchange and the ACK procedure because the MPDU is directed to the AP. When `dot11SSPNInterfaceActivated` is true, an AP shall distribute the group addressed message into the BSS only if `dot11NonAPStationAuthSourceMulticast` in the `dot11InterworkingEntry` identified by the source MAC address in the received message is true. When `dot11SSPNInterfaceActivated` is false, the group addressed message shall be distributed into the BSS. Unless the MPDU is delivered via DMS, ~~the~~ STA originating the message receives the message as a group addressed message (prior to any filtering). Therefore, all STAs shall filter out group addressed messages that contain their address as the source address. When `dot11SSPNInterfaceActivated` is false, group addressed MSDUs shall be propagated throughout the ESS. When `dot11SSPNInterfaceActivated` is true, group addressed MSDUs shall be propagated throughout the ESS only if `dot11NonAPStationAuthSourceMulticast` in the `dot11InterworkingEntry` identified by the source MAC address in the received message is true.

There is no MAC-level recovery on grouped addressed frames, except for the following: ~~those frames in which the To DS field is 1.~~

- Frames in which the To DS field is 1
- Group addressed frames transmitted via the GATS

As a result, the reliability of this traffic is reduced, relative to the reliability of individually addressed traffic, due to the increased probability of lost frames from interference, collisions, or time-varying channel properties.

An STBC-capable STA shall discard either all received group addressed data frames that are STBC frames or all received group addressed data frames that are non-STBC frames. How it makes this decision is outside the scope of this standard.

A STA shall discard an MPDU with a group address in the Address 1 field if the value in the Address 1 field does not match any value in the dot11GroupAddressesTable and does not match the Broadcast address value.

9.4 PCF

9.4.3 PCF access procedure

9.4.3.2 Fundamental access

Change the second paragraph of 9.4.3.2 as follows:

After the initial Beacon frame, the PC shall wait for one SIFS period and then transmit one of the following: a data frame, a CF-Poll frame, a Data+CF-Poll frame, a management frame, or a CF-End frame. If the CFP is null, i.e., no traffic is buffered and no polls exist to send at the PC, a CF-End frame shall be transmitted immediately after the initial Beacon frame. If there are buffered group addressed MSDUs/MMPDUs that are not being delivered using the GCR-SP delivery method, the PC shall transmit these prior to any individually addressed MSDUs/MMPDUs.

9.4.4 PCF transfer procedure

9.4.4.2 PCF transfers when the PC STA is transmitter or recipient

Change the second paragraph of 9.4.4.2 as follows:

The PC may transmit data or management frames to non-CF-Pollable, non-PS STAs during the CFP. These STAs shall acknowledge receipt with ACK frames after a SIFS, as with the DCF. The PC may also transmit group addressed frames during the CFP. Because the Beacon frame that initiates the CFP contains a DTIM element, if there are associated STAs using PS mode, the buffered group addressed frames that are not delivered via the GCR-SP delivery method shall be sent immediately after any Beacon frame containing a TIM element with a DTIM count field with a value of 0.

9.7 Multirate support

9.7.5 Rate selection for data and management frames

9.7.5.3 Rate selection for other group addressed data and management frames

Change the first paragraph of 9.7.5.3 as follows:

This subclause describes the rate selection rules for group addressed data and management frames, excluding the following:

- Non-STBC Beacon and non-STBC PSMP frames
- STBC group addressed data and management frames
- Data frames located in an FMS stream (see 10.23.7)
- Group addressed frames transmitted to the GCR concealment address (see 10.23.14.2.5)

9.9 HT Control field operation

Change the second paragraph of 9.9 as follows:

A STA that has a value of true for at least one of `dot11RDResponderOptionImplemented`, ~~and~~ `dot11MCSFeedbackOptionImplemented`, and `dot11AlternateEDCAImplemented` shall set `dot11HTControlFieldSupported` to true.

9.11 A-MSDU operation

Change fourth paragraph of 9.11 as indicated:

The Address 1 field of an MPDU carrying an A-MSDU shall be set to an individual address or to the GCR concealment address.

9.19 HCF

9.19.2 HCF contention-based channel access (EDCA)

9.19.2.1 Reference implementation

Change the second paragraph of 9.19.2.1 as follows:

A model of the reference implementation is shown in Figure 9-19 for the case in which `dot11AlternateEDCAActivated` is false or not present and in Figure 9-19a for the case in which `dot11AlternateEDCAActivated` is true. ~~These figures illustrate and illustrates~~ a mapping from frame type or UP to ~~AC~~ the four transmit queues and the four independent EDCAFs, ~~one for each queue~~. The mapping of UP to the ~~AC transmit queue and the mapping to AC~~ are ~~is~~ described in 9.2.4.2 and Table 9-1. The mapping of frame types to ACs is described in 9.2.4.2.

Change title of Figure 9-19 as shown:

Figure 9-19—Reference implementation model when `dot11AlternateEDCAActivated` is false or not present

Insert Figure 9-19a after Figure 9-19:

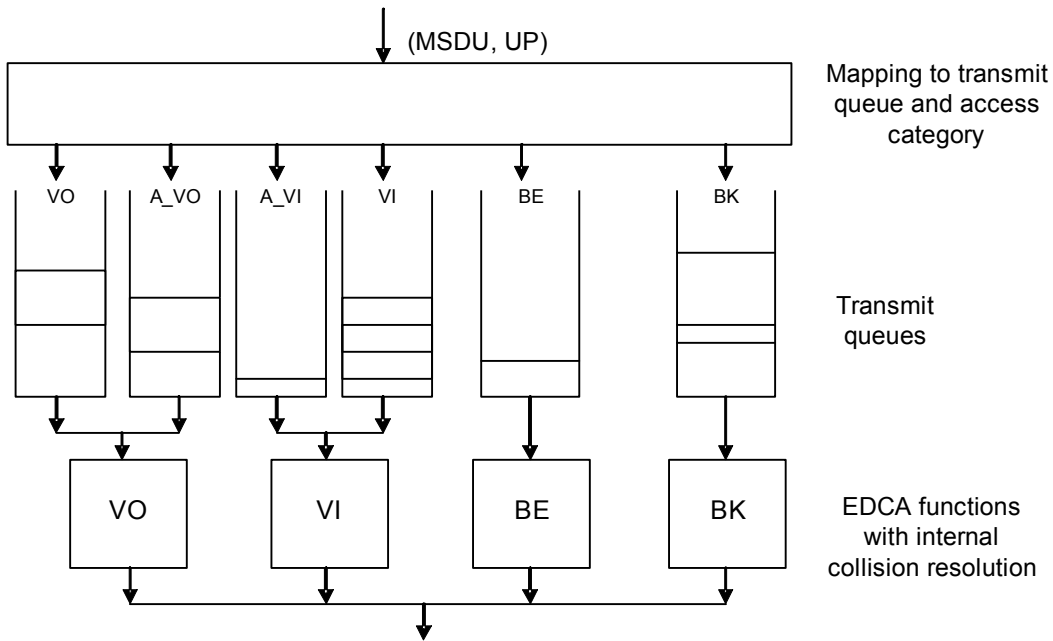


Figure 9-19a—Reference implementation model when `dot11AlternateEDCAActivated` is true

9.19.2.5 EDCA backoff procedure

Change the second paragraph of 9.19.2.5 as follows:

For the purposes of this subclause, successful transmission and transmission failure are defined as follows:

- After transmitting an MPDU (regardless of whether it is carried in an A-MPDU) that requires an immediate frame as a response, the STA shall wait for a timeout interval of duration of `aSIFSTime` + `aSlotTime` + `aPHY-RX-START-Delay`, starting at the `PHY-TXEND.confirm` primitive. If a `PHY-RXSTART.indication` primitive does not occur during the timeout interval, the STA concludes that the transmission of the MPDU has failed.
- If a `PHY-RXSTART.indication` primitive does occur during the timeout interval, the STA shall wait for the corresponding `PHY-RXEND.indication` primitive to determine whether the MPDU transmission was successful. The recognition of a valid response frame sent by the recipient of the MPDU requiring a response, corresponding to this `PHY-RXEND.indication` primitive, shall be interpreted as a successful response.
- ~~The recognition of anything else, including any other valid frame, shall be interpreted as failure of the MPDU transmission.~~ The recognition of a valid data frame sent by the recipient of a PS-Poll frame shall also be accepted as successful acknowledgment of the PS-Poll frame.
- A transmission that does not require an immediate frame as a response is defined as a successful transmission, unless it is one of the nonfinal (re)transmissions of an MPDU that is delivered using the GCR unsolicited retry retransmission policy (9.19.2.6.2).
- The nonfinal (re)transmission of an MPDU that is delivered using the GCR unsolicited retry retransmission policy (9.19.2.6.2) is defined to be a failure.
- The final (re)transmission of an MPDU that is delivered using the GCR unsolicited retry retransmission policy (9.19.2.6.2) is defined as a successful transmission.

- The recognition of anything else, including any other valid frame, shall be interpreted as failure of the MPDU transmission.

Insert the following paragraph after the sixth paragraph (“If the backoff procedure”) of 9.19.2.5:

QoS STAs shall maintain a short retry counter and a long retry counter for each MSDU, A-MSDU, or MMPDU that belongs to a TC that requires acknowledgment. The initial value for the short and long retry counters shall be 0. QoS STAs also maintain a short retry counter and a long retry counter for each AC. They are defined as QSRC[AC] and QLRC[AC], respectively, and each is initialized to a value of 0. When dot11RobustAVStreamingImplemented is true, QoS STAs shall maintain a short drop-eligible retry counter and a long drop-eligible retry counter for each AC. They are defined as QSDRC[AC] and QLDRC[AC], respectively, and each is initialized to a value of zero. APs with dot11RobustAVStreamingImplemented true and mesh STAs with dot11MeshGCRImplemented true, shall maintain an unsolicited retry counter.

Change the now eighth paragraph of 9.19.2.5 as follows:

If the backoff procedure is invoked because of a failure event [reason c) or d) above or the transmission failure of a non-initial frame by the TXOP holder], the value of CW[AC] shall be updated as follows before invoking the backoff procedure:

- If the QSRC[AC] or the QLRC[AC] for the QoS STA has reached dot11ShortRetryLimit or dot11LongRetryLimit, respectively, CW[AC] shall be reset to CWmin[AC].
- If the QSDRC[AC] or the QLDRC[AC] for the QoS STA in which dot11RobustAVStreamingImplemented is true has reached dot11ShortDEIRetryLimit or dot11LongDEIRetryLimit, respectively, CW[AC] shall be reset to CWmin[AC].
- Otherwise,
 - If CW[AC] is less than CWmax[AC], CW[AC] shall be set to the value $(CW[AC] + 1) \times 2 - 1$.
 - If CW[AC] is equal to CWmax[AC], CW[AC] shall remain unchanged for the remainder of any retries.

9.19.2.6 Retransmit procedures

Change 9.19.2.6 as follows (including creating a new subclause, 9.19.2.6.1):

9.19.2.6.1 General

~~QoS STAs shall maintain a short retry counter and a long retry counter for each MSDU, A-MSDU, or MMPDU that belongs to a TC that requires acknowledgment. The initial value for the short and long retry counters shall be 0. QoS STAs also maintain a short retry counter and a long retry counter for each AC. They are defined as QSRC[AC] and QLRC[AC], respectively, and each is initialized to a value of 0.~~

After transmitting a frame that requires an immediate acknowledgment, the STA shall perform either of the acknowledgment procedures, as appropriate, that are defined in 9.3.2.8 and 9.21.3. The short retry count for an MSDU or A-MSDU that is not part of a Block Ack agreement or for an MMPDU shall be incremented every time transmission of a frame of length less than or equal to dot11RTSThreshold fails for that MSDU, A-MSDU, or MMPDU. The unsolicited retry counter shall be incremented after the transmission of every A-MSDU that is transmitted using the GCR unsolicited retry retransmission policy.

QSRC[AC] shall be incremented every time transmission of an A-MPDU or frame of length less than or equal to dot11RTSThreshold fails, regardless of the presence or value of the DEI field. When dot11RobustAVStreamingImplemented is true, QSDRC[AC] shall be incremented every time transmission of an A-MPDU or frame in which the HT Control field is present, the DEI field is equal to 1 and the length of the frame is less than or equal to dot11RTSThreshold fails. This short retry count and the QoS STA

QSRC[AC] shall be reset when an A-MPDU or frame of length less than or equal to dot11RTSThreshold succeeds. When dot11RobustAVStreamingImplemented is true, the QSDRC[AC] shall be reset when an A-MPDU or frame of length less than or equal to dot11RTSThreshold succeeds, regardless of the presence or value of the DEI field.

The long retry count for an MSDU or A-MSDU that is not part of a Block Ack agreement or for an MMPDU shall be incremented every time transmission of a MAC frame of length greater than dot11RTSThreshold fails for that MSDU, A-MSDU, or MMPDU.

QLRC[AC] shall be incremented every time transmission of an A-MPDU or frame of length greater than or equal to dot11RTSThreshold fails, regardless of the presence or value of the DEI field. This long retry count and the QLRC[AC] shall be reset when an A-MPDU or frame of length greater than dot11RTSThreshold succeeds. When dot11RobustAVStreamingImplemented is true, QLDRC[AC] shall be incremented every time transmission fails for an A-MPDU or frame of length greater than dot11RTSThreshold in which the HT Control field is present and the DEI field is equal to 1. The QLDRC[AC] shall be reset when an A-MPDU or frame of length greater than dot11RTSThreshold succeeds, regardless of the presence or value of the DEI field.

All retransmission attempts for an MPDU that is not sent under a Block Ack agreement and that has failed the acknowledgment procedure one or more times shall be made with the Retry field set to 1 in the data or management frame.

Retries for failed transmission attempts shall continue until one or more of the following conditions occurs:

- ~~until~~ The short retry count for the MSDU, A-MSDU, or MMPDU is equal to MPDUDot11ShortRetryLimit.
- ~~until~~ The long retry count for the MSDU, A-MSDU, or MMPDU is equal to dot11LongRetryLimit.
- The short drop-eligible retry count for the MSDU, A-MSDU, or MMPDU is equal to dot11ShortDEIRetryLimit.
- The long drop-eligible retry count for the MSDU, A-MSDU, or MMPDU is equal to dot11LongDEIRetryLimit.
- The unsolicited retry count for the A-MSDU is equal to dot11UnsolicitedRetryLimit.

When ~~either~~ any of these limits is reached, retry attempts shall cease, and the MSDU, A-MSDU, or MMPDU shall be discarded.

For internal collisions occurring with the EDCA access method, the appropriate retry counters (short retry counter for MSDU, A-MSDU, or MMPDU and QSRC[AC] or long retry counter for MSDU, A-MSDU, or MMPDU and QLRC[AC]) are incremented. For internal collisions occurring with the EDCA access method where dot11RobustAVStreamingImplemented is true, the appropriate drop-eligible retry counters (QSDRC[AC], and QLDRC[AC]) are incremented when the collision occurs for MSDU, A-MSDU, or MMPDU that has drop eligibility equal to 1. For transmissions that use Block Ack, the rules in 9.21.3 also apply. STAs shall retry failed transmissions until the transmission is successful or until the relevant retry limit is reached.

With the exception of a frame belonging to a TID for which Block Ack is set up, a QoS STA shall not initiate the transmission of any management or data frame to a specific RA while the transmission of another management or data frame with the same RA and having been assigned its sequence number from the same sequence counter has not yet completed to the point of success, retry fail, or other MAC discard (e.g., lifetime expiry).

QoS STAs shall maintain a transmit MSDU timer for each MSDU passed to the MAC. dot11EDCATableMSDULifetime specifies the maximum amount of time allowed to transmit an MSDU for

a given AC. The transmit MSDU timer shall be started when the MSDU is passed to the MAC. If the value of this timer exceeds the appropriate entry in dot11EDCA_{TableMSDULifetime}, then the MSDU, or any remaining, undelivered fragments of that MSDU, shall be discarded by the source STA without any further attempt to complete delivery of that MSDU.

When A-MSDU aggregation is used, the HT STA maintains a single timer for the whole A-MSDU. The timer is restarted each time an MSDU is added to the A-MSDU. The result of this procedure is that no MSDU in the A-MSDU is discarded before a period of dot11EDCA_{TableMSDULifetime} has elapsed.

Insert the following subclause, 9.19.2.6.2, after 9.19.2.6.1:

9.19.2.6.2 Unsolicited retry procedure

When using the GCR unsolicited retry retransmission policy for a group address, the AP or mesh STA may retransmit an MPDU to increase the probability of correct reception at the STAs that are listening to this group address (i.e., the group address is in their dot11GroupAddressesTable). The set of MPDUs that may be retransmitted is dependent upon whether Block Ack agreements are active with the STAs that are listening to this group address and is defined in 10.23.15.3.6. How an AP or a mesh STA chooses which MPDUs to retransmit is an implementation decision and beyond the scope of this standard.

A protective mechanism (such as a mechanism described in 9.22) should be used to reduce the probability of other STAs transmitting during the GCR TXOP. When using a protection mechanism that requires a response from another STA, the AP should select a STA that is a member of the GCR group.

The TXOP initiation rules defined in 9.19.2.2 and 9.19.3.3 shall be used for initiating a GCR TXOP. The duration of a GCR TXOP shall be subject to the TXOP limits defined in 9.19.2.2.

When transmitting MPDUs using the GCR service with retransmission policy equal to GCR unsolicited retry, the following rules apply:

- Following a MAC protection exchange that includes a response frame, in all GCR unsolicited retry retransmissions, the STA shall either transmit the frames within a GCR TXOP separated by SIFS or invoke its backoff procedure as defined in 9.19.2.5. The STA shall not transmit an MPDU and a retransmission of the same MPDU within the same GCR TXOP. The final frame transmitted within a GCR TXOP shall follow the backoff procedure defined in 9.19.2.5.
- Without MAC protection or with MAC protection that lacks a response frame, in all transmissions, the STA shall invoke the backoff procedure defined in 9.19.2.5, using a value of CW_{min}[AC] for CW, at the PHY-TXEND.confirm primitive that follows the transmission of each unsolicited retry GCR MPDU.
- All retransmissions of an MPDU shall have the Retry field in their Frame Control fields set to 1.
- During a GCR TXOP, frames may be transmitted within the GCR TXOP that do not use the GCR unsolicited retry retransmission policy.

9.19.3 HCCA

9.19.3.1 General

Change the fifth paragraph of 9.19.3.1 as follows:

The HC shall perform delivery of buffered non-GCR-SP group addressed MSDUs/MMPDUs following DTIM Beacon frames. The HC may also operate as a PC, providing (non-QoS) CF-Polls to associated CF-Pollable STAs using the frame formats, frame exchange sequences, and other applicable rules for PCF specified in 9.4.²⁸

9.21 Block Acknowledgment (Block Ack)

9.21.1 Introduction

Change the third paragraph of 9.21.1 as follows:

The Block Ack mechanism does not require the setting up of a TS; however, QoS STAs using the TS facility may choose to signal their intention to use Block Ack mechanism for the scheduler's consideration in assigning TXOPs. The Block Ack mechanism is also used by the GCR service. Acknowledgments of frames belonging to the same TID, but transmitted during multiple TXOPs, may also be combined into a single BlockAck frame. This mechanism allows the originator to have flexibility regarding the transmission of data MPDUs. The originator may split the block of frames across TXOPs, separate the data transfer and the Block Ack exchange, and interleave blocks of MPDUs carrying all or part of MSDUs or A-MSDUs for different TIDs or RAs.

9.21.2 Setup and modification of the Block Ack parameters

Change the second-to-last paragraph of 9.21.2 as follows:

If the Block Ack mechanism is being set up for a TS, bandwidth negotiation (using ADDTS Request and Response frames) should precede the setup of the Block Ack mechanism. If the Block Ack mechanism is being set up for the GCR service, then the following steps apply:

- One or more GCR Request/Response exchanges precede the setup of the Block Ack mechanism.
- The ADDBA Request and Response frames exchanged to set up the Block ACK shall include the GCR Group Address element indicating the group address of the GCR service.

9.21.3 Data and acknowledgment transfer using immediate Block Ack policy and delayed Block Ack policy

Change the first paragraph of 9.21.3 as follows:

After setting up either an immediate Block Ack agreement or a Delayed Block agreement following the procedure in 9.21.2 and having gained access to the medium and established protection, if necessary, the originator may transmit a block of QoS data frames separated by SIFS period, with the total number of frames not exceeding the Buffer Size subfield value in the associated ADDBA Response frame and subject to any additional duration limitations based on the channel access mechanism. Each of the frames shall have the Ack Policy subfield in the QoS Control field set to "Block Ack." The RA field of the frames that are not delivered using the GCR Block Ack retransmission policy shall be the recipient's individual address. For GCR frames delivered using the GCR Block Ack retransmission policy, the RA field of the frames shall be the GCR concealment address. The originator requests acknowledgment of outstanding QoS data frames by sending a Basic BlockAckReq frame. The recipient shall maintain a Block Ack record for the block.

Change the fifth paragraph of 9.21.3 as follows:

The recipient of an accepted Block Ack agreement that did not contain a GCR Group Address element in the ADDBA Request frame shall maintain a Block Ack record consisting of originator address, TID, and a record of reordering buffer size indexed by the received MPDU sequence control value. This record holds the acknowledgment state of the data frames received from the originator. The recipient of an accepted Block Ack agreement that contained a GCR Group Address element in the ADDBA Request frame shall maintain a Block Ack record consisting of the DA address from the A-MSDU subframe header, TID, and a record of reordering buffer size indexed by the received MPDU sequence control value. This record holds the acknowledgment state of the group addressed data frames received from the originator.

9.21.5 Teardown of the Block Ack mechanism

Insert the following paragraph at the end of 9.21.5:

The DELBA Frame transmitted to release the Block Ack setup of a GCR service shall include the GCR Group Address element to indicate the group address of the GCR service.

9.21.6 Selection of BlockAck and BlockAckReq variants

Insert the following paragraph at the end of 9.21.6:

The GCR subfield of the BAR Control field shall be set to 1 in all BlockAckReq frames where the Block Ack agreement is for a group address delivered using the GCR Block Ack retransmission policy and shall be set to 0 otherwise. The GCR subfield of the BA Control field shall be set to 1 in all BlockAck frames where the Block Ack agreement is for a group address delivered using the GCR Block Ack retransmission policy and shall be set to 0 otherwise.

Insert the following subclauses, 9.21.10 to 9.21.10.3 (including Figure 9-28a), after 9.21.9:

9.21.10 GCR Block Ack

9.21.10.1 Introduction

Subclause 9.21.10 extends the Block Ack mechanism to group addressed frames that are transmitted using the GCR Block Ack retransmission policy.

9.21.10.2 Scoreboard context control during GCR Block Ack

For each GCR Block Ack agreement, each recipient shall maintain a block acknowledgment record as defined in 9.21.3. This record includes the following information:

- A bitmap, indexed by sequence number
- A 12-bit unsigned integer starting sequence number
- $WinStart_R$, representing the lowest sequence number position in the bitmap
- A variable $WinEnd_R$
- The maximum transmission window size, $WinSize_R$

$WinSize_R$ is set to the smaller of 64 and the value of the Buffer Size field of the associated ADDBA Response frame that established the Block Ack agreement. $WinEnd_R$ is defined as the highest sequence number in the current transmission window. A STA implementing a GCR Block Ack agreement shall maintain the block acknowledgment record for that agreement according to the following rules:

- a) At GCR Block Ack agreement establishment:
 - 1) $WinStart_R$ = the Starting Sequence Number subfield value (SSN) from the ADDBA Request frame that elicited the ADDBA Response frame that established the GCR Block Ack agreement.
 - 2) $WinEnd_R = WinStart_R + WinSize_R - 1$.
- b) For each received data MPDU that is related with a specific GCR Block Ack agreement, the block acknowledgment record for that agreement is modified as follows, where SN is the value of the Sequence Number subfield of the received data MPDU:
 - 1) If $WinStart_R \leq SN \leq WinEnd_R$, set to 1 the bit in position SN within the bitmap.
 - 2) If $WinEnd_R < SN < WinStart_R + 2^{11}$,

- i) Set to 0 the bits corresponding to MPDUs with Sequence Number subfield values from $WinEnd_R + 1$ to $SN - 1$.
 - ii) Set $WinStart_R = SN - WinSize_R + 1$.
 - iii) Set $WinEnd_R = SN$.
 - iv) Set to 1 the bit at position SN in the bitmap.
- 3) If $WinStart_R + 2^{11} \leq SN \leq WinStart_R$, make no changes to the record.
- c) For each received BlockAckReq frame that is related with a specific GCR Block Ack agreement, the block acknowledgment record for that agreement is modified as follows, where SSN is the value from the Starting Sequence Number subfield of the received BlockAckReq frame:
 - 1) If $WinStart_R < SSN \leq WinEnd_R$,
 - i) Set $WinStart_R = SSN$.
 - ii) Set to 0 the bits corresponding to MPDUs with Sequence Number subfield values from $WinEnd_R + 1$ through $WinStart_R + WinSize_R - 1$.
 - iii) Set $WinEnd_R = WinStart_R + WinSize_R - 1$.
 - 2) If $WinEnd_R < SSN < WinStart_R + 2^{11}$,
 - i) Set $WinStart_R = SSN$.
 - ii) Set $WinEnd_R = WinStart_R + WinSize_R - 1$.
 - iii) Set to 0 bits the corresponding to MPDU with Sequence Number subfield values from $WinStart_R$ to $WinEnd_R$.
 - 3) If $WinStart_R + 2^{11} \leq SSN \leq WinStart_R$, make no changes to the record.

9.21.10.3 GCR Block Ack BlockAckReq and BlockAck frame exchanges

A protective mechanism (such as transmitting an HCCA CAP, MCCA, or RTS/CTS; setting the Duration field in the first frame and response frames to update the NAVs of STAs in the BSS and OBSS(s); or using another mechanism described in 9.13 and 9.3.2.5) should be used to reduce the probability of other STAs transmitting during the GCR TXOP.

When the retransmission policy for a group address is GCR Block Ack, an originator may transmit no more than GCR buffer size A-MSDUs with RA set to the GCR concealment address and the DA field of the A-MSDU subframe set to the GCR group address before sending a BlockAckReq frame to one of the STAs that has a GCR Block Ack agreement for this group address. The RA field of the BlockAckReq frame shall be set to the MAC address of the destination STA. Upon reception of the BlockAck frame, an AP may send a BlockAckReq frame to another STA that has a Block Ack agreement for this group address, and this process may be repeated multiple times.

NOTE—If the originator sends a BlockAckReq frame to a STA with a MAC address that matches the SA in any of the A-MSDUs transmitted during the GCR TXOP, the Block Ack bitmap does not indicate the MSDUs sourced from this STA. This is because the STA will have discarded all group addressed MPDUs transmitted by the AP that have the source address equal to their MAC address (see 9.3.6).

When a recipient receives a BlockAckReq frame with the GCR Group Address subfield equal to a GCR group address, the recipient shall transmit a BlockAck frame at a delay of SIFS after the BlockAckReq frame. The BlockAck frame acknowledges the STA's reception status of the block of group addressed frames requested by the BlockAckReq frame.

Figure 9-28a shows an example of a frame exchange when the GCR Block Ack retransmission policy is used. The AP sends several A-MSDUs using the GCR Block Ack retransmission policy. The AP then sends a BlockAckRequest frame to group member 1 of the GCR group, waits for the BlockAck frame, and then sends a BlockAckRequest frame to group member 2. After receiving the BlockAck frame from GCR group member 2, the AP determines whether any A-MSDUs need to be retransmitted and sends additional

A-MSDUs (some of which might be retransmissions of previous A-MSDUs) using the GCR Block Ack retransmission policy.

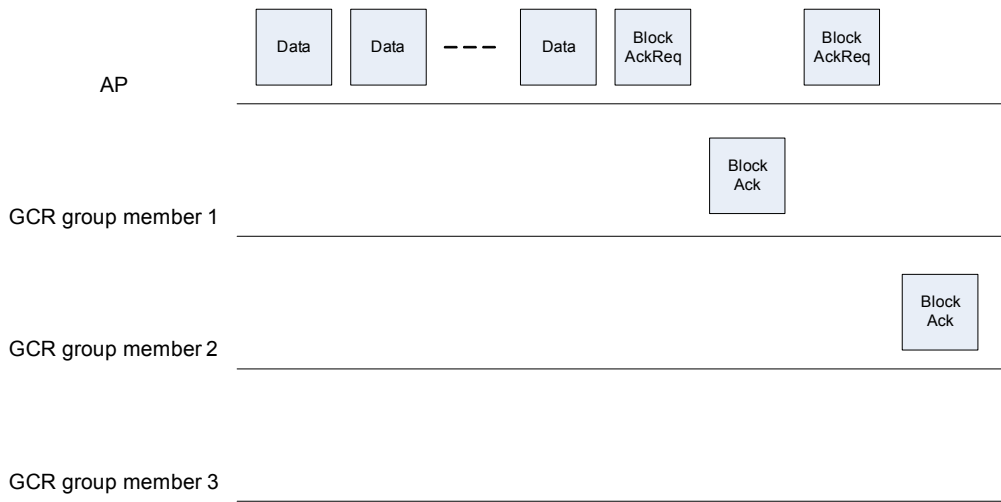


Figure 9-28a—Example of a frame exchange with GCR Block Ack retransmission policy

After completing the BlockAckReq and BlockAck frame exchanges, the originator determines from the information provided in the BlockAck bitmap and from the missing BlockAck frames which, if any, A-MSDUs need to be retransmitted.

An originator adopting the GCR Block Ack retransmission policy for a GCR group address chooses a lifetime limit for the group address. The originator may vary the lifetime limit for the group address at any time and may use different lifetime limits for different GCR group addresses. The originator transmits and retries each A-MSDU until the appropriate lifetime limit is reached or until each one has been received by all group members to which a BlockAckReq frame has been sent, whichever occurs first.

For GCR streams with retransmission policy equal to GCR Block Ack, an originator may regularly send a BlockAckReq frame with the GCR Group Address subfield in the BAR Information field set to the GCR group address and the Block Ack Starting Sequence Control field set to the Sequence Number field of the earliest A-MSDU of the GCR stream that has not been acknowledged by all group members and has not expired due to lifetime limits, in order to minimize buffering latency at receivers in the GCR group.

NOTE 1—This is because an originator might transmit management frames, QoS data frames with a group address in the Address 1 field (including different GCR streams), and non-QoS data frames intermingled. Since these are transmitted using a single sequence counter, missing frames or frames sent to group addresses absent from a receiving STA’s dot11GroupAddresses table complicate receiver processing for GCR streams with a GCR Block Ack retransmission policy since the cause of a hole in a receiver’s Block Ack bitmap is ambiguous: it is due either to an MPDU being lost from the GCR stream or to transmissions of MPDUs not related to the GCR service using the same sequence number counter.

NOTE 2—If an originator accepts two GCR agreements with two STAs where the GCR agreements have the same Ethernet classifiers, but different additional classifiers, then the following effects are observed: Each STA receives both GCR flows from the originator and sends them to upper layers where the MSDUs irrelevant to the STA are discarded, in the same manner that non-GCR MSDUs irrelevant to the STA are discarded. In the Block Ack bitmap sent to the originator, each STA sets bits to 1 corresponding to MPDUs received from either GCR stream. The originator is responsible for recognizing that these bit positions apply to MPDUs irrelevant to the STA and for not spuriously retrying MPDUs.

The beginning of reception of an expected response to a BlockAckRequest frame is detected by the occurrence of a PHY-CCA.indication(BUSY,channel-list) primitive at the STA that is expecting the response where one of the following conditions exists:

- The channel-list parameter is absent; or
- The channel-list is equal to {primary}, and the HT STA expected to transmit the expected response supports 20 MHz operation only; or
- The channel-list is equal to either {primary} or {primary, secondary}, and the HT STA expected to transmit the expected response supports both 20 MHz and 40 MHz operation (see 10.15.2).

If the beginning of such reception does not occur during the first slot time following a SIFS, then the originator may perform error recovery by retransmitting a BlockAckReq frame PIFS after the previous BlockAckReq frame when both of the following conditions are met:

- The carrier sense mechanism (see 9.3.2.2) indicates that the medium is idle at the TxPIFS slot boundary (defined in 9.3.7) after the expected start of a BlockAck, and
- The remaining duration of the GCR TXOP is longer than the total time required to retransmit the GCR BlockAckReq plus one slot time.

NOTE—If an originator fails to receive a BlockAck frame in response to a BlockAckReq frame and there is insufficient time to transmit a recovery frame, the AP retransmits the BlockAckReq frame in a new TXOP.

9.26 PSMP Operation

9.26.1 Frame transmission mechanism during PSMP

9.26.1.1 PSMP frame transmission (PSMP-DTT and PSMP-UTT)

Change the second paragraph of 9.26.1.1 as follows:

A PSMP sequence may be used to transmit non-GCR-SP group addressed frames along with individually addressed frames. Individually addressed frames shall be scheduled after group addressed frames.

10. MLME

10.2 Power management

10.2.1 Power management in an infrastructure network

10.2.1.1 General

Change the third paragraph of 10.2.1.1 as follows:

If any STA in its BSS is in PS mode, the AP shall buffer all non-GCR-SP group addressed BUs and deliver them to all STAs immediately following the next Beacon frame containing a DTIM transmission.

10.2.1.2 STA Power Management modes

Change Table 10-1 as follows:

Table 10-1—Power Management modes

<u>Mode</u>	<u>Description</u>
Active mode or AM	STA may receive frames at any time. In Active mode, a STA shall be in the Awake state. A STA on the polling list of a PCF shall be in Active mode for the duration of the CFP.
PS	<p>STA listens to selected Beacon frames (based upon the ListenInterval parameter of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive) and sends PS-Poll frames to the AP if the TIM element in the most recent Beacon frame indicates an individually addressed BU is buffered for that STA.</p> <p>The AP shall transmit buffered individually addressed BUs to a PS STA only in response to a PS-Poll from that STA, during the CFP in the case of a CF-Pollable PS STA, or during a scheduled or unscheduled APSD service period for the STA, <u>or during the SP of a scheduled GCR-SP</u>. In PS mode, a STA shall be in the Doze state and shall enter the Awake state to receive selected Beacon frames, to receive group addressed transmissions following certain received Beacon frames, <u>to receive transmissions during the SP of a scheduled GCR-SP</u>, to transmit, and to await responses to transmitted PS-Poll frames or (for CF-Pollable STAs) to receive CF transmissions of buffered BUs.</p>

10.2.1.3 AP TIM transmissions

Change 10.2.1.3 as follows:

The TIM shall identify the STAs for which traffic is pending and buffered in the AP. This information is coded in a *partial virtual bitmap*, as described in 8.4.2.7. In addition, the TIM contains an indication whether group addressed traffic is pending. Every STA is assigned an AID by the AP as part of the association process. AID 0 (zero) is reserved to indicate the presence of buffered non-GCR-SP group addressed BUs. The AP shall identify those STAs for which it is prepared to deliver buffered BUs by setting bits in the TIM’s partial virtual bitmap that correspond to the appropriate AIDs.

10.2.1.4 TIM types

Change the first paragraph of 10.2.1.4 as follows:

Two different TIM types are distinguished: TIM and DTIM. After a DTIM, the AP shall transmit buffered non-GCR-SP group addressed BUs, before transmitting any individually addressed frames.

Change the fourth paragraph of 10.2.1.4 as follows:

The third and fourth lines in Figure 10-4 depict the activity of two STAs operating with different power management requirements. Both STAs power on their receivers when they need to listen for a TIM. This is indicated as a ramp-up of the receiver power prior to the TBTT. The first STA, for example, powers up its receiver and receives a TIM in the first Beacon frame; that TIM indicates the presence of a buffered BU for the receiving STA. The receiving STA then generates a PS-Poll frame, which elicits the transmission of the buffered BU from the AP. Non-GCR-SP group addressed BUs are sent by the AP subsequent to the transmission of a Beacon frame containing a DTIM. The DTIM is indicated by the DTIM count field of the TIM element having a value of 0.

10.2.1.5 Power management with APSD

10.2.1.5.1 Power management with APSD procedures

Change the fourth paragraph of 10.2.1.5.1 as follows:

If there is no unscheduled SP in progress, the unscheduled SP begins when the AP receives a trigger frame from a STA, which is a QoS data or QoS Null frame using an AC the STA has configured to be trigger-enabled. An A-MPDU that contains one or more trigger frames acts as a trigger frame. An unscheduled SP ends after the AP has attempted to transmit at least one BU using a delivery-enabled AC and destined for the STA, but no more than the number indicated in the Max SP Length field of the QoS Capability element of the STA's (Re)Association Request frame if the field has a nonzero value. By setting the EOSP field to 1 in the last frame sent during the SP, an unscheduled SP may be terminated before the maximum number of BUs in the SP has been reached.

Change paragraphs 8 to 11 of 10.2.1.5.1 as follows:

A scheduled SP starts at fixed intervals of time specified in the Service Interval field. If the scheduled Service Interval field equals 0 (for example, with the GCR-A delivery method), the scheduled SP starts from the service start time without a fixed delivery interval. In order to use a scheduled SP for a TS when the access policy is controlled channel access, a STA shall send an ADDTS Request frame to the AP with the APSD subfield of the TS Info field in the TSPEC element set to 1. To use a scheduled SP for a TS for a AC when the access policy is contention-based channel access, a STA shall send an ADDTS Request frame to the AP with the APSD and Schedule subfields of the TS Info field in the TSPEC element both set to 1. If the APSD mechanism is supported by the AP and the AP accepts the corresponding ADDTS Request frame from the STA, the AP shall respond to the ADDTS Request frame with a response containing the Schedule element indicating that the requested service can be accommodated by the AP. When the access policy is contention-based channel access for a GCR group addressed stream, a scheduled SP is set up according to 10.23.15.3.3. The first scheduled SP starts when the lower order 4 octets of the TSF timer equal the value specified in the Service Start Time field. If the SI is nonzero, the STA using scheduled SP shall first wake up at the service start time to receive downlink individually addressed and/or GCR-SP group addressed BUs buffered and/or to receive polls from the AP/HC. If the SI is nonzero, the STA shall wake up subsequently at a fixed time interval equal to the SI. The AP may modify the non-GCR service start time by indicating so in the Schedule element in a successful ADDTS Response frame (which is sent in response to an ADDTS Request frame) and in Schedule frames (which are sent at other times). The AP may modify the GCR service start time by indicating so in the Schedule element in the GCR Response subelements (see 8.4.2.91 and 10.23.15.3.4). In both non-GCR and GCR cases, the service start time shall be updated (using the previously described service start time modification procedures) whenever the upper 4 octets of the TSF timer change.

A scheduled SP begins at the scheduled wakeup time that corresponds to the SI and the service start time indicated in the Schedule element sent in response to a TSPEC or GCR Request. If the SI is nonzero, the STA shall wake up at a subsequent time when

$$(TSF - \text{service start time}) \bmod \text{minimum SI} = 0.$$

If the SI is nonzero, a scheduled SP for a GCR group ends after the AP has attempted to transmit at least one BU associated with the GCR group but no more than the number indicated in the Max SP Length field of the QoS Capability element of the STA's (Re)Association Request frame. The last frame of the GCR SP shall have the EOSP field set to 1.

If a scheduled SP overlaps the period during which the AP is required to transmit non-GCR-SP group addressed frames and frames individually addressed to STAs in PS mode that follow a DTIM beacon that

has at least 1 bit set to 1 in the partial virtual bitmap of its TIM, the scheduled SP shall be deferred until the AP has transmitted all such buffered frames.

When the GCR-A delivery method is used, the scheduled Service Interval field is 0. If a STA has a GCR agreement with an AP for a group address using the GCR-A delivery method, there is no defined end of the scheduled SP. The STA in PS mode shall enter the Awake state and shall remain awake in order to receive the buffered group addressed BUs until the AP changes the delivery method of the stream to a method other than GCR-A or until the GCR agreement is cancelled.

If scheduled ~~services periods~~ SPs are supported in a BSS, a STA may use both unscheduled and scheduled APSD on different ACs at the same time. The GCR-SP delivery method may be used on any AC, irrespective of the non-GCR unscheduled or scheduled APSD flows. When a STA establishes scheduled delivery for an AC, the AP shall not transmit BUs using that AC during an SP that is initiated by a trigger frame, and it shall not treat BUs using the AC that are received from the STA as trigger frames. The AP shall decline any ADDTS Request frame that indicates the use of both scheduled and unscheduled APSD to be used on non-GCR-SP frames of the same AC at the same time.

APSD shall be used only to deliver individually addressed BUs and GCR-SP BUs to a STA. Non-GCR and non-GCR-SP ~~g~~Group addressed BU delivery shall follow the frame delivery rules defined for group addressed BUs as defined in 10.2.1.7.

10.2.1.6 AP operation during the CP

Change list items d), e), and f) of the second paragraph in 10.2.1.6 as follows:

- d) If a STA has set up a scheduled SP, it shall automatically wake up at each SP. Therefore, the APSD-capable AP shall transmit frames associated with admitted traffic with the APSD subfield equal to 1 in the TSPECs buffered for the STA during a scheduled SP. If the STA has set up to use unscheduled SPs, the AP shall buffer BUs using delivery-enabled ACs until it has received a trigger frame using a trigger-enabled AC from the non-AP STA, which indicates the start of an unscheduled SP. A trigger frame received by the AP from a STA that already has an unscheduled SP underway shall not trigger the start of a new unscheduled SP. The AP transmits BUs destined for the STA and using delivery-enabled ACs during an unscheduled SP. The bit for AID 0 (zero) in the bitmap control field of the TIM element shall be set to 1 when non-GCR-SP group addressed traffic is buffered, according to 8.4.2.7.
- e) If any associated STAs are in PS mode, all non-GCR-SP group addressed BUs except those with a service class of StrictlyOrdered shall be buffered.
- f) When dot11MgmtOptionFMSActivated is false, the AP shall transmit all buffered non-GCR-SP group addressed BUs immediately after every DTIM.

When dot11MgmtOptionFMSActivated is true and the AP has established an FMS delivery interval for a multicast stream, the AP shall transmit all non-GCR-SP group addressed BUs belonging to a particular FMS stream immediately after the DTIM that has the Current Count field value of the FMS Counter field set to 0 for that particular FMS stream.

The More Data field of each group addressed frame shall be set to indicate the presence of further buffered non-GCR-SP group addressed BUs. If the AP is unable to transmit all of the buffered non-GCR-SP group addressed BUs before the primary or secondary TBTT following the DTIM, the AP shall set the bit for AID 0 (zero) in the TIM element to 1 for a single BSSID or set the corresponding Group Address bit to 1 for multiple BSSIDs, as defined in 8.4.2.7, and when dot11MgmtOptionFMSActivated is true, shall set the appropriate bits in the FMS Descriptor element as described in 8.4.2.77 to indicate for which non-GCR-SP group addresses there are still buffered BUs, until all buffered non-GCR-SP group addressed BUs have been transmitted.

When the AP transmits an STBC DTIM or TIM Beacon frame, the AP shall retransmit all non-GCR-SP group addressed BUs that were transmitted following the non-STBC DTIM or TIM Beacon frame except that they are transmitted using the basic STBC MCS. It may be the case that a complete set of buffered non-GCR-SP group addressed BUs is sent over a period of time during which non-STBC and STBC transmissions are interleaved, but the transition from non-STBC group addressed transmissions to STBC group addressed transmissions shall be preceded by the transmission of an STBC Beacon frame, and the transition from STBC group addressed transmissions to non-STBC group addressed transmissions shall be preceded by the transmission of a non-STBC Beacon frame.

10.2.1.7 AP operation during the CFP

Change list items d), e), and f) of the second paragraph in 10.2.1.7 as follows:

- d) All non-GCR-SP group addressed MSDUs except those with a service class of StrictlyOrdered shall be buffered if any associated STAs are in the PS mode, regardless of whether those STAs are CF-Pollable.
- e) When dot11MgmtOptionFMSActivated is false, the AP shall transmit all buffered non-GCR-SP group addressed BUs immediately after every DTIM (Beacon frame with DTIM Count field of the TIM element equal to 0).

When dot11MgmtOptionFMSActivated is true and the AP has set up an FMS delivery interval for a multicast stream, the AP shall send all non-GCR-SP group addressed BUs belonging to a particular FMS stream immediately after the DTIM with the Current Count field value of the FMS Counter field set to 0 for that particular FMS stream.

The More Data field shall be set to 1 in the headers of all but the final frame containing one of these buffered non-GCR-SP group addressed BUs to indicate the presence of further buffered group addressed BUs. If the AP is unable to transmit all of the buffered non-GCR-SP group addressed BUs before the non-STBC or STBC TBTT following the DTIM, the AP shall set the bit for AID 0 (zero) in the TIM element to 1 for a single BSSID or set the corresponding group addressed bit to 1 for multiple BSSIDs, as defined in 8.4.2.7, and when dot11MgmtOptionFMSActivated is true, shall set the appropriate bits in the FMS Descriptor element as described in 8.4.2.77 to indicate for which non-GCR-SP group addresses there are still buffered BUs, until all buffered non-GCR-SP group addressed BUs have been transmitted.

When the AP transmits an STBC DTIM or TIM Beacon frame, the AP shall retransmit all non-GCR-SP group addressed BUs that were transmitted following the non-STBC DTIM or TIM Beacon frame except that they are transmitted using the basic STBC MCS. It may be the case that a complete set of buffered non-GCR-SP group addressed BUs is sent over a period of time during which non-STBC and STBC transmissions are interleaved, but the transition from non-STBC group addressed transmissions to STBC group addressed transmissions shall be preceded by the transmission of a STBC Beacon frame, and the transition from STBC group addressed transmissions to non-STBC group addressed transmissions shall be preceded by the transmission of a non-STBC Beacon frame.

- f) Buffered BUs for STAs in the PS mode shall be forwarded to the CF-Pollable STAs under control of the PC. Transmission of these buffered BUs as well as CF-Polls to STAs in the PS mode that were indicated in the DTIM in accordance with paragraph c) of this subclause shall begin immediately after transmission of buffered non-GCR-SP group addressed frames (if any), and shall occur in order by increasing AID of CF-Pollable STAs. A CF-Pollable STA for which the TIM element of the most recent Beacon frame indicated buffered BUs shall be in the Awake state at least until the receipt of an individually addressed frame from the AP in which the Frame Control field does not indicate the existence of more buffered BUs. After acknowledging the last of the buffered BUs, the CF-Pollable STA operating in the PS mode may enter the Doze state until the next DTIM is expected.

10.4 TS operation

10.4.1 Introduction

Change the second paragraph of 10.4.1 as follows.

A TS may have one or more TCLAS (within the discretion of the STA that sets up the stream) associated with it. The AP uses the parameters in the TCLAS elements to filter the MSDUs belonging to this TS for delivery as part of the TS. An Intra-Access Category Priority element may be associated with a TS by the inclusion of an Intra-Access Category Priority element in an ADDTS Request frame. The User Priority subfield of the Intra-Access Category Priority element shall be set to the same UP as specified in the User Priority subfield of the TS Info field. If dot11AlternateEDCAActivated is true, the Alternate Queue subfield is used to select the appropriate EDCA transmit queue when the Access Policy subfield of the TS Info field in the TSPEC is EDCA or HEMM. When an Intra-Access Category Priority element is associated with a TS, the Drop Eligibility subfield is used to indicate the drop eligibility of the MSDUs of this TS.

Change the fourth paragraphs of 10.4.1 as follows.

TSPEC, optional TCLAS, ~~and~~ optional EBR, and optional Intra-Access Category Priority elements are transported on the air by the ADDTS Request frame and the ADDTS Response frame, and across the MLME SAP by the MLME-ADDTS primitives. In addition, a TS could be created if a STA sends a resource request to an AP prior to initiating a transition to that AP or in the Reassociation Request frame to that AP.

10.4.4 TS setup

Change 10.4.4 as follows:

10.4.4.1 General

A TS setup may be initiated by a non-AP STA or an AP.

10.4.4.2 Non-AP-STA-initiated TS setup

Figure 10-8 shows the sequence of messages occurring at a TS setup initiated by a non-AP STA. This message sequence in this figure and in the subsequent figures does not show the acknowledgment.

Figure 10-8 remains unchanged.

10.4.4.3 AP-initiated TS setup

Figure 10-8a shows the sequence of messages occurring at a TS setup initiated by the AP. This message sequence in this figure and in the subsequent figures does not show the acknowledgments.

TS setup may be initiated by an AP in response to a request originating from higher layer protocols. An AP in which dot11RobustAVStreamingImplemented is true shall not send ADDTS Reserve Request action frames to an associated STA that has set the RobustAVStreaming bit in the Extended Capabilities element in its (Re)Association Request frame to 0.

The higher layer stream ID is defined by the higher layer. The Higher Layer Stream ID element shall be included in the ADDTS Reserve Request action frame sent by the AP to the non-AP STA. This Higher Layer Stream ID is used in the TS setup procedure between the AP and the non-AP STA.

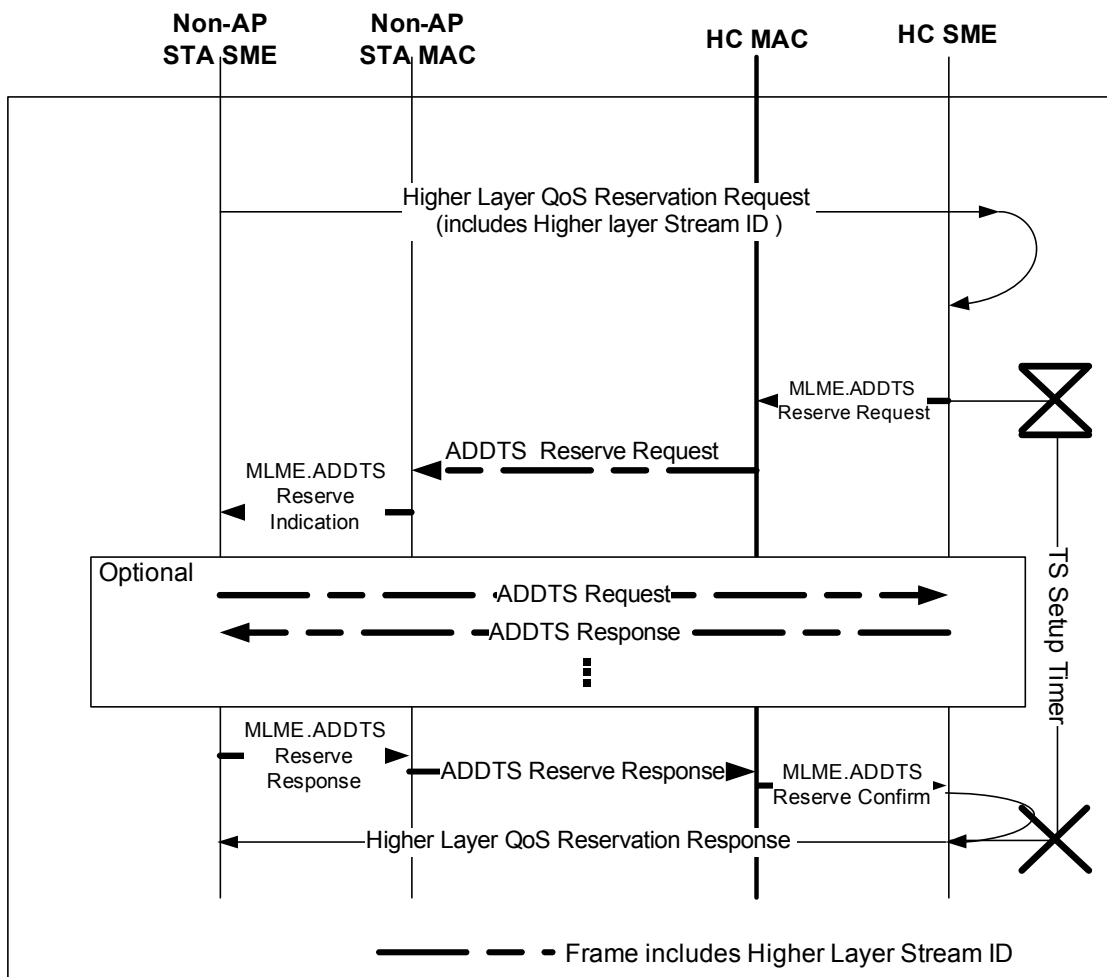


Figure 10-8a—TS setup when initiated by the AP

The AP initiates the TS setup by sending an ADDTS Reserve Request action frame that includes the Higher Layer Stream ID element to the non-AP STA. On receipt of the ADDTS Reserve Request action frame from the AP, the non-AP STA shall perform one of the following:

- a) Complete the AP-initiated TS setup procedure by sending an ADDTS Reserve Response action frame that includes the Higher Layer Stream ID corresponding to the AP-initiated TS setup procedure and with the status code set to “SUCCESS.”
- b) Send an ADDTS Reserve Response action frame with a nonzero status code and abort the AP-initiated TS setup. The Higher Layer Stream ID field in this ADDTS Reserve Response action frame shall be set to the Higher Layer Stream ID corresponding to the AP-initiated TS setup procedure.
- c) Send an ADDTS Request action frame to the AP. There might be multiple ADDTS Request/ADDTS Response exchanges between the non-AP STA and the AP, as described in 10.4.4.4, to negotiate the TSPEC parameters. The Higher Layer Stream ID shall be included in all frames corresponding to the AP-initiated TS setup procedure that are exchanged between the non-AP STA and the AP. The AP-initiated TS setup procedure is completed by sending an ADDTS Reserve Response action frame that includes the Higher Layer Stream ID corresponding to the AP-initiated TS setup procedure and with the status code set to indicate the result of the TSPEC negotiation.

NOTE 1—Stream Reservation Protocol (SRP) as described in clause 35 of IEEE Std 802.1Q-2011 is an example of a higher layer protocol. The IEEE 802.11 subsystem at a non-AP STA does not interpret the SRP reservation request but simply sends it to the AP with which it is associated. A higher layer agent called Designated Multiple Stream Registration Protocol (MSRP) Node (DMN) is co-located with the AP in the device that supports SRP. All incoming SRP reservation requests are forwarded to the MSRP DMN. The MSRP DMN interprets the SRP reservation request and invokes appropriate IEEE 802.11 primitives in order for the AP to invoke the MLME-ADDTSRESERVE.request primitive. The MSRP DMN responds to the originator of the SRP Reservation request with the outcome of the AP-initiated TS setup procedure. The procedures performed by the MSRP DMN are described in C.3 of IEEE Std 802.1Q-2011.

NOTE 2—If the higher layer SRP Reservation Request is lost within the IEEE 802.11 subsystem, the corresponding retry/recovery procedure is the responsibility of the SRP protocol. These procedures are described in Clause 35 of IEEE Std 802.1Q-2011.

10.4.4.4 TS setup procedures for both AP and non-AP STA initiation

The non-AP STA's SME decides that a TS needs to be created. How it does this, and how it selects the TSPEC parameters, is beyond the scope of this standard. The SME generates an MLME-ADDTS.request primitive containing a TSPEC. A TSPEC may also be generated autonomously by the MAC without any initiation by the SME. However, if a TSPEC is generated subsequently by the SME, the TSPEC containing the same TSID generated autonomously by the MAC shall be overridden. If one or more TSPECs are initiated by the SME, the autonomous TSPEC shall be terminated.

The remaining text formerly in 10.4.4 through the last paragraph (“When a STA requests service ... described in Annex N.”) is unchanged.

10.4.8 Data transfer

Insert the following paragraphs at the end of 10.4.8:

If dot11AlternateEDCAActivated is true, if an Intra-Access Category Priority element was provided when the TS was created, and if the Access Policy subfield of the TS Info field in the TSPEC is EDCA or HEMM, the value from the Alternate Queue subfield is used to select the appropriate EDCA transmit queue.

If an Intra-Access Priority element was provided when the TS was created, the Drop Eligibility subfield is used to determine the drop eligibility of the MSDU.

10.5 Block Ack operation

10.5.2 Setup and modification of the Block Ack parameters

10.5.2.2 Procedure at the originator

Change item b) of the first paragraph in 10.5.2.2 as indicated:

- b) Check whether the intended peer STA is capable of participating in the Block Ack mechanism by discovering and examining its “Delayed Block Ack” and “Immediate Block Ack” capability bits. If the recipient is capable of participating, the originator sends an ADDBA frame indicating the TID and the buffer size. If the recipient is capable of participating and the GCRGroupAddress parameter of the MLME-ADDBA.request primitive is present, the originator sends an ADDBA Request frame that includes a GCR Group Address element.

10.5.2.4 Procedure common to both originator and recipient

Insert the following row at the end of Table 10-2 (note that the entire table is not shown here):

Table 10-2—Types of Block Ack agreement based on capabilities and ADDBA conditions

Capabilities condition	ADDBA condition	Type of Block Ack agreement
Both STAs are robust AV streaming STAs, and the agreement was established using ADDBA Request/Response frames that included GCR Group Address elements.	Block Ack Policy subfield equal to 1; ADDBA GCR Group Address Present subfield equal to 1	GCR Block Ack

10.5.4 Error recovery upon a peer failure

Change the first sentence of the first paragraph in 10.5.4 as indicated:

Every STA shall maintain an inactivity timer for every negotiated Block Ack setup, unless the Block Ack is set up for a GCR group address.

Insert the following note at the end of 10.5.4:

NOTE—A Block Ack associated with a GCR group address does not use an inactivity timer because the GCR originator might switch between the DMS delivery method, the GCR unsolicited retry retransmission policy, and the GCR Block Ack retransmission policy during the lifetime of a GCR agreement.

10.18 RSNA A-MSDU procedures

Change the end of 10.18 as follows:

~~NOTE—The subclause does not describe the operation of group addressed A-MSDUs because the use of group addressed A-MSDUs is not permitted, as defined in 9.11.~~

An AP may transmit SPP A-MSDU for a GCR group address if it has successfully negotiated RSNA (re)associations with all associated STAs that have an active GCR agreement for this group address.

10.23 Wireless network management procedures

Change the title and text of 10.23.15 as follows (including creating two new subclauses, 10.23.15.1 and 10.23.15.2):

10.23.15 Group addressed transmission service ~~DMS procedures~~

10.23.15.1 General

The group addressed transmission service provides delivery of group addressed frames and comprises the two services, DMS and GCR.

10.23.15.2 DMS procedures

The directed multicast service (DMS) is a service that may be provided by an AP to its associated non-AP STAs that support DMS, where the AP transmits group addressed MSDUs as individually addressed A-MSDUs.

Implementation of DMS is optional for a WNM STA and mandatory for a robust AV streaming STA (as defined in 10.26.1). A STA that implements DMS has dot11MgmtOptionDMSImplemented set to true. When dot11MgmtOptionDMSImplemented is true, at least one of dot11WirelessManagementImplemented and dot11RobustAVStreamingImplemented shall be true, and dot11HighThroughputOptionImplemented shall be true. A STA that has a value of true for dot11MgmtOptionDMSActivated is defined as a STA that supports Directed Multicast. A STA for which dot11MgmtOptionDMSActivated is true shall set the DMS field of the Extended Capabilities element to 1.

The remaining text formerly in 10.23.15, ending with the last paragraph (“If the AP supports both DMS and TFS, the AP shall first apply TFS to the frame and then apply DMS.”), is unchanged.

Insert the following subclauses, 10.23.15.3 to 10.23.15.3.8 (including Table 10-9a and Table 10-9b), after 10.23.15.2:

10.23.15.3 GCR procedures

10.23.15.3.1 Overview

Groupcast with retries (GCR) is a flexible service to improve the delivery of group addressed frames while optimizing for a range of criteria. GCR service may be provided by the AP to associated STAs in an infrastructure BSS or by a mesh STA to its peer mesh STAs in a mesh BSS. GCR uses the setup, modification, and termination procedures defined 10.23.15.2. The differences between GCR procedures and DMS procedures are as follows:

- a) A GCR agreement applies to a single group address and, if a TCLAS Processing element is present, it has the Processing subfield value set to 0, whereas a DMS flow is not restricted to a single group address.
- b) DMS offers multicast-to-unicast conversion only, whereas GCR includes several retransmission policies and delivery methods.

A STA with dot11RobustAVStreamingImplemented true shall implement the GCR procedures defined in 10.23.15.3.2 to 10.23.15.3.6. When dot11RobustAVStreamingImplemented is true, dot11MgmtOptionDMSImplemented and dot11HighThroughputOptionImplemented shall be true. A STA that implements advanced GCR supports GCR Block Ack (10.23.15.3.7) and GCR-SP (10.23.15.3.8) and has dot11AdvancedGCRImplemented set to true. When dot11AdvancedGCRImplemented is true, dot11RobustAVStreamingImplemented shall be true. In a mesh BSS, a STA that implements GCR has dot11MeshGCRImplemented set to true. When dot11MeshGCRImplemented is true, dot11HighThroughputOptionImplemented shall be true.

DMS allows the transmission of group addressed MSDUs as individually addressed A-MSDUs and is particularly suited to small numbers of group members. It provides a high level of reliability but has low scalability as the efficiency decreases and delay increases proportionally to the number of group members.

GCR employs the DMS Request and DMS Response elements with the addition of GCR Request and Response subelements, respectively, for administering the announcement, setup, modification, and teardown of GCR services between an AP and non-AP STAs or between peer mesh STAs. The DMS procedures and state machine of 10.23.15.2 shall apply to GCR with the extensions and constraints specific to GCR described below in 10.23.15.3.3 to 10.23.15.3.8.

Along with the No-Ack/No-Retry or non-GCR (defined in 9.3.6) and the DMS (defined in 10.23.15.2) retransmission mechanisms, GCR defines two additional retransmission policies for group addressed frames:

- GCR unsolicited retry
- GCR Block Ack

When using the GCR unsolicited retry retransmission policy for a group address, the STA providing GCR service retransmits an MSDU one or more times (subject to applicable MSDU lifetime and retry limits) to increase the probability of correct reception at STAs that are listening to this group address. The decision to retransmit these MSDUs is implementation dependent. GCR unsolicited retry is particularly suited to use with large numbers of group members as it has moderate delay, efficiency, and reliability, but high scalability.

The GCR Block Ack retransmission policy extends the block acknowledgment mechanism to group addressed frames. The STA providing the GCR service initiates Block Ack agreements with each STA receiving GCR frames that supports GCR Block Ack for a particular group address. Once this Block Ack agreement is in place, the STA providing GCR service regularly sends BlockAckReq frames to the STAs receiving the frames to ascertain the reception status of MSDUs related to this group address, as described in 9.21.10. This allows the STA providing GCR service to discover MSDUs that have not been received and to schedule their retransmission. GCR Block Ack is particularly suited to use with moderate numbers of group members as it has moderate delay, high efficiency, and moderate scalability and reliability.

The GCR service has two delivery methods for group addressed frames:

- Non-GCR-SP
- GCR-SP (see 10.23.15.3.8)

The non-GCR-SP delivery method may be provided using one or more of the following:

- FMS (see 10.2.1.16)
- Transmit frames within a GCR stream after the DTIM Beacon frame if any STA in the GCR group is in PS mode
- Transmit frames at any time if all STAs in the GCR group are in Active mode in an infrastructure BSS
- In accordance with 13.13 in a mesh BSS

GCR-SP transmits GCR group addressed frames at intervals, where the interval between transmissions might be smaller than the beacon interval. Compared to non-GCR-SP, GCR-SP might provide lower delay and jitter.

10.23.15.3.2 GCR group membership procedures

The procedures described in 10.23.15.3.3 to 10.23.15.3.8 depend upon the AP or mesh STA knowing the membership of the multicast groups of STAs that support GCR.

One method for an AP to discover the multicast groups that its associated STAs are receiving or for a mesh STA to discover the multicast groups that its peer mesh STAs are receiving is to use the Group Membership Request frame (as defined in 8.5.19.4) to request the contents of the dot11GroupAddressesTable of its associated STAs or peer mesh STAs.

Other methods of group membership detection are also possible, using information that is outside the scope of this standard. For example, group membership detection could be achieved by inspecting the protocol messages of IETF RFC 3376.⁴

An AP may transmit a Group Membership Request frame as an individually addressed frame to an associated STA that has indicated that it supports robust AV streaming (as indicated by the Robust AV Streaming bit equal to 1 in the Extended Capabilities element) to request the associated STA's dot11GroupAddressesTable. An AP shall not send a Group Membership Request frame to an associated STA that has the Robust AV Streaming bit equal to 0 in its Extended Capabilities element.

A STA for which dot11GCRActivated or dot11MeshGCRActivated is true shall reply to a Group Membership Request frame by sending a Group Membership Response frame with the Dialog Token field set to the value from the Group Membership Request frame, the Address Count field set to the number of entries in the dot11GroupAddressesTable, and the Group Address List field set to the group MAC addresses in the dot11GroupAddressesTable. A STA for which dot11GCRActivated or dot11MeshGCRActivated is true shall set dot11GCRGroupMembershipAnnouncementActivated to true upon reception of a Group Membership Request frame.

A STA for which dot11GCRGroupMembershipAnnouncementActivated and at least one of dot11MeshGCRActivated and dot11GCRActivated are true shall send an unsolicited Group Membership Response frame with the Dialog Token field set to 0, the Address Count field set to the number of entries in the dot11GroupAddressesTable, and the Group Address List field set to the group MAC addresses in the dot11GroupAddressesTable, every time the contents of the dot11GroupAddressesTable is modified.

If an unsolicited Group Membership Response frame is sent by an associated STA, the frame shall be transmitted as a directed frame to the AP with which it is associated. If an unsolicited Group Membership Response frame is sent by a mesh station in a mesh BSS, the frame shall be transmitted as a broadcast frame.

10.23.15.3.3 GCR setup procedures

An AP with dot11GCRActivated true may transmit to an associated non-AP STA an unsolicited individually addressed DMS Response frame that contains one DMS Status field with a GCR Response subelement per group address, if it detects that the associated non-AP STA meets all of the following conditions:

- Robust AV Streaming was equal to 1 in the Extended Capabilities element in the most recently received (Re)Association Request frame from the non-AP STA.
- The non-AP STA is receiving one or more group addresses for which there is an active GCR service.
- The non-AP STA does not have a GCR agreement for one or more of these group addresses.

A mesh STA with dot11MeshGCRActivated true may transmit to a peer mesh STA an unsolicited individually addressed DMS Response frame that contains one DMS Status field with a GCR Response subelement per group address, if it detects that the peer mesh STA meets all of the following conditions:

- Mesh GCR was equal to 1 in the Extended Capabilities element in the most recently received mesh beacon from the peer mesh STA.
- The peer mesh STA is receiving one or more group addresses for which there is an active GCR service.
- The peer mesh STA does not have a GCR agreement for one or more of these group addresses.

Each DMS Status field includes a TCLAS element to identify the GCR group address, the DMSID corresponding to this GCR traffic flow, and other associated parameters. The Status subfield of this DMS Status field shall be set to "GCR Advertise." The associated STA may ignore the DMS Response frame or initiate a GCR agreement for one or more of the group addresses.

A STA requests use of the GCR service for a group address by sending a DMS Descriptor (as described in 10.23.15.2) with the following modifications:

⁴ IETF RFC 3376, Internet Group Management Protocol (IGMP).

- The DMS Descriptor shall contain one TCLAS element with the frame classifier type equal to 0 (Ethernet parameters), one TSPEC element, and one GCR Request subelement.
- The DMS Descriptor may contain other TCLAS elements in addition to the mandatory TCLAS element.
- When there are multiple TCLAS elements, a TCLAS Processing element shall be present, and the Processing subfield in the TCLAS Processing element shall be set to 0. Otherwise, no TCLAS Processing elements shall be present in the DMS Descriptor.
- The TSID subfield within the TS Info field of the TSPEC element shall be reserved. Since the AP might choose a delivery method of GCR-SP, the non-AP STA should set the Minimum Service Interval, Maximum Service Interval, and Service Start Time fields in the TSPEC element to indicate the STA's preferred wakeup schedule. In a mesh BSS, the Delivery Method field shall not be set to "GCR-SP."
- The GCR Request subelement specifies the retransmission policy and delivery method requested by the non-AP STA for the group addressed stream.

A STA shall not request transmission of a group address via the GCR service while it has an active DMS for this group address. A STA shall not request transmission of a group address via DMS while it has an active GCR service for this group address.

An AP or mesh STA accepts a GCR request by sending a DMS Response Action frame with a DMS Response element that contains a DMS Status field with the Response Type field set to "Accept" (as described in 10.23.15.2) with the following modifications:

- The DMS Status field shall include a GCR Response subelement indicating the retransmission policy, delivery method, and GCR concealment address for the group addressed stream. The Retransmission Policy field shall not be set to "No Preference." The Delivery Method field shall not be set to "No Preference." The GCR Concealment Address field of the GCR Response subelement shall be set to dot11GCRConcealmentAddress. In a mesh BSS, the Delivery Method field shall not be set to "GCR-SP."
- If the GCR group addressed stream is subject to the GCR-SP delivery method, then the AP shall also include a Schedule element in the DMS Status field indicating the wakeup schedule for the group addressed stream.
- If a TSPEC Element is included, the TSID subfield shall be set to 0.

For each GCR Request subelement, the AP or mesh STA may

- Adopt the requested retransmission policy and delivery method, or
- Maintain its existing retransmission policy and delivery method, or
- Select an alternate retransmission policy and delivery method, or
- Deny GCR service for the group addressed stream.

In an infrastructure BSS, the retransmission policy shall not be GCR Block Ack for a GCR group address while the AP has a GCR agreement for the group address with a non-AP STA that had the Advanced GCR field equal to 0 in the Extended Capabilities element in the (Re)Association Request frame most recently received by the AP.

In a mesh BSS, the retransmission policy shall not be GCR Block Ack for a GCR group address while the mesh STA has a GCR agreement for the group address with a peer mesh STA that had the Mesh GCR field equal to 0 in the Extended Capabilities element.

An AP or mesh STA denies a GCR request by sending a DMS Response Action frame with a DMS Response element that contains a DMS Status field with

- The Response Type field set to "Deny" (as described in 10.23.15.2) and

- An empty GCR Response subelement.

If an AP or mesh STA denies a GCR request, it may suggest an alternative TCLAS-based classifier by including one or more TCLAS elements and an optional TCLAS Processing element (as described in 8.4.2.35). One TCLAS element shall be included in the DMS Descriptor with the frame classifier type equal to 0 (Ethernet parameters). Other TCLAS elements may be included in the DMS Descriptor, but, if present, a TCLAS Processing element with the Processing subfield equal to 0 shall also be included.

If a STA requesting GCR service determines that one or more GCR Response subelements are unacceptable, then the STA shall discard any received ADDBA Request frames for the unacceptable GCR streams and shall send a new DMS Request frame containing a DMS Request element with one DMS Descriptor for each unacceptable GCR stream. The DMSID fields shall be set to the DMSIDs of the unacceptable streams, and the Request Type field shall be set to “Remove.”

In an infrastructure BSS, if the non-AP STA accepts the response to its GCR request, the non-AP STA shall set dot11GCRConcealmentAddress to the value contained in the GCR Concealment Address field of the GCR Response subelement.

In a mesh BSS, if a STA requesting GCR service accepts the response to its GCR request, it shall add to dot11GroupAddressesTable the value contained in the GCR Concealment Address field of the GCR Response subelement.

In a mesh BSS, a GCR agreement instance is identified by a GCR agreement instance identifier. The mesh GCR agreement instance consists of the DMSID, localMAC, peerMAC, and concealment address.

For each group addressed stream requested by the non-AP STA and accepted by the AP, the AP shall immediately initiate a Block Ack negotiation if both of the following conditions are true:

- The AP advertised an Advanced GCR field equal to 1 in its Extended Capabilities element.
- The non-AP STA advertised an Advanced GCR field equal to 1 in the Extended Capabilities element in the (Re)Association Request frame most recently received by the AP.

For each group addressed stream requested by a mesh STA, the peer mesh STA shall immediately initiate a Block Ack negotiation if both the mesh STAs advertised a Mesh GCR field equal to 1 in their Extended Capabilities element in their most recently received mesh Beacon frame.

If all the above conditions are true, the AP or mesh STA shall immediately initiate a Block Ack negotiation by sending an ADDBA Request frame to the STA that originated the GCR request. The Block Ack Policy subfield in the Block Ack Parameter Set field within the ADDBA frames shall not be set to 0. The TID subfield in the Block Ack Parameter Set field within the ADDBA frames shall be set to 0. The A-MSDU Supported subfield within the ADDBA frames shall be set to 1 (A-MSDU permitted). The Starting Sequence Number field within the ADDBA Request frames shall be greater than (modulo 4096) the last sequence number of the last group address frame transmitted before the ADDBA Request frame. STAs shall maintain this Block Ack agreement for the duration of their GCR agreement, irrespective of whether GCR Block Ack is the current retransmission policy. While the retransmission policy of the GCR group addressed stream is DMS, the STA receiving GCR frames shall suspend its Block Ack processing for the group addressed stream.

NOTE—Having a Block Ack agreement with all members of a GCR group address allows the AP or mesh STA to change the GCR retransmission policy dynamically.

For each GCR agreement, there shall be only one retransmission policy and delivery method active at any time. A GCR agreement between a non-AP STA and an AP or between peer mesh STAs shall begin when the STA providing GCR service successfully transmits an individually addressed DMS Response frame with

a DMS Response element containing a DMS Status field that has the Status field set to “Accept” (as described in 10.23.15.2) with the DMS Status field including a GCR Response subelement.

10.23.15.3.4 GCR frame exchange procedures

In an infrastructure BSS, a GCR Block Ack agreement exists between a non-AP STA and an AP for a group addressed stream from when the non-AP STA successfully transmits an ADDBA Response frame until one of the following situations occurs:

- The AP or non-AP STA successfully transmits a DELBA frame to the other party.
- The GCR agreement no longer exists.

In a mesh BSS, a GCR Block Ack agreement exists between a mesh STA and its peer mesh STA for a group addressed stream from the time when the mesh STA successfully transmits an ADDBA Response frame to the peer mesh STA until one of the following situations occurs:

- The mesh STA or the peer mesh STA successfully transmits a DELBA frame to the other party.
- This GCR Block Ack agreement expires (see 9.10.5).
- The GCR agreement is terminated.

An AP or a mesh STA may transmit a group addressed stream via the No-Ack/No-Retry (non-GCR; see 9.3.6) service and GCR service simultaneously. Each frame shall be transmitted via the No-Ack/No-Retry retransmission policy before it is transmitted via the GCR service, except when using the GCR-SP delivery method. The AP may transmit each frame via the No-Ack/No-Retry retransmission policy before or after it transmits the frame via the GCR service when using the GCR-SP delivery method. A STA providing GCR service may switch between the DMS, GCR Block Ack, or GCR unsolicited retry retransmission policies, but only one delivery mode may be active at any given time for each GCR group address.

An AP or mesh STA shall transmit a frame belonging to a group address via the GCR service if any associated STA or peer mesh STA has a GCR agreement for the group address and, otherwise, does not transmit the frame via the GCR service.

In an infrastructure BSS, an AP shall transmit a frame belonging to a group address via the No-Ack/No-Retry service if one or more of the following situations occur:

- The group address is the broadcast address.
- The group address is not the broadcast address, and at least one associated STA has the Robust AV Streaming bit equal to 0 in the Extended Capabilities element of the STA’s most recent (Re)Association Request frame and has been determined by the AP to be a member of the group address (how this determination is made is out of the scope of this standard).
- The group address is not the broadcast address, at least one non-AP STA has a Block Ack agreement for the group address, and the frame precedes the start of the Block Ack agreement (the sequence number of the frame is less than the starting sequence number of the block Ack agreement, as described in 9.21.2).

In a mesh BSS, a mesh STA providing GCR service shall transmit a frame belonging to a group address via the No-Ack/No-Retry service if one or more of the following situations occur:

- The group address is the broadcast address.
- The group address is not the broadcast address, and at least one peer mesh STA has the Mesh GCR bit equal to 0 in the Extended Capabilities element of the STA’s most recent mesh Beacon frame and has been determined to be a member of the group address (how this determination is made is out of the scope of this standard).
- The group address is not the broadcast address, at least one peer mesh STA has a Block Ack agreement for the group address, and the frame precedes the start of the Block Ack agreement (the

sequence number of the frame is less than the starting sequence number of the Block Ack agreement, as described in 9.10.2).

When the AP updates the retransmission policy, the AP shall set the Last Sequence Control field in the GCR Response subelement to the sequence number of the MPDU corresponding to the GCR traffic flow that is being updated that was delivered prior to the change in retransmission policy.

To avoid undetected retries being passed up at a receiver's MAC_SAP, duplicate detection and removal for group addressed frames is required in STAs with dot11RobustAVStreamingImplemented true or dot11MeshGCRImplemented true (see 9.3.2.10).

GCR frames shall be QoS data frames (with QoS subfield of the Subtype field set to 1).

If the Block Ack agreement is successfully established for the group addressed stream and the delivery method for the group addressed stream is GCR-SP, then the non-AP STA ensures it is awake for subsequent SPs (see 10.23.15.3.8).

A STA may request a change of GCR service for a group addressed stream by sending a DMS Descriptor with the DMSID identifying the group address and the Request Type field set to "Change" (as described in 10.23.15.2) with the following modifications:

- The DMS Descriptor shall contain zero TCLAS elements, zero TCLAS Processing elements, one TSPEC element, and one GCR Request subelement.
- The TSPEC element and GCR Request subelement of this DMS Descriptor shall together contain at least one field that is different from the original TSPEC element and GCR Request subelement identified by the DMSID.

An AP or mesh STA may update the retransmission policy, delivery method, and schedule for any reason, such as the size of the group changes, the capabilities of the members of the group change, GCR Request subelements for the group are received, or multicast diagnostics are needed. The AP or mesh STA advertises the current settings upon a change and periodically by either of the following methods:

- Transmitting an unsolicited DMS Response frame with the current settings addressed to the GCR concealment address. This DMS Response frame shall be scheduled for delivery at the appropriate DTIM interval or SP in which all STAs within the group are awake to receive the frame. One TCLAS element shall be included with the frame classifier type equal to 0 (Ethernet parameters). Other TCLAS elements may be present, but if present, a TCLAS Processing element with the Processing subfield equal to 0 shall also be included. One TSPEC element and one GCR Subelement shall be included per DMS Descriptor in the DMS Response element of the DMS Response frame to identify each GCR stream. The DMSID that identifies the GCR stream shall be included in the DMS Descriptor. Each Status field in the DMS Status fields included in the frame shall be set to "GCR Advertise."
- Transmitting unsolicited DMS Response frames with the current settings individually addressed to each GCR group member. Each GCR stream is identified by the DMSID in a DMS Status field in the DMS Response element of the DMS Response frame. These DMS Status fields shall not include a TCLAS element, TSPEC element, or GCR subelement. Each Status field in the DMS Status fields included in the frame shall be set to "GCR Advertise."

STAs receiving GCR frames shall recover from missing group addressed DMS Response frames containing GCR Response subelements that advertise a changed retransmission policy or delivery method according to Table 10-9a or Table 10-9b, respectively.

Table 10-9a—STA recovery procedures for a changed retransmission policy

Current retransmission policy state at STA receiving GCR frames	Actual retransmission policy being used by the AP or mesh STA providing GCR service	Recovery procedure
GCR unsolicited retry or GCR Block Ack	No-Ack/No-Retry	A STA receiving GCR frames shall cancel the GCR service for the group address by sending a DMS Response frame that contains a DMS Descriptor with the Request Type set to “Remove” when no frames for the group address are received via the GCR service after a period of dot11GCRPolicyChangeTimeout.
DMS	GCR unsolicited retry or GCR Block Ack	A STA receiving GCR frames shall update its current retransmission policy of the GCR stream to GCR unsolicited retry upon receiving an A-MSDU for the DMS group address concealed via the GCR concealment address.
GCR unsolicited retry or GCR Block Ack	DMS	A STA receiving GCR frames shall update its current retransmission policy of the GCR stream to DMS upon receiving an A-MSDU with the RA field equal to the non-AP STA’s individual address and the DA field of the A-MSDU subframe equal to the GCR group address.
GCR unsolicited retry	GCR Block Ack	A STA receiving GCR frames shall update its current retransmission policy of the GCR stream to GCR Block Ack upon receiving a BlockAckReq frame with a GCR Group Address subfield equal to the GCR group address.
GCR Block Ack	GCR unsolicited retry	A STA receiving GCR frames shall update its current retransmission policy of the GCR stream to GCR unsolicited retry if MSDUs for the GCR group address concealed via the GCR concealment address are being received yet no BlockAckReq frames for the GCR group address are received after a period of dot11GCRPolicyChangeTimeout.

A GCR agreement between a non-AP STA and an AP or between peer mesh STAs shall end (as described in 10.23.15.2) when one of the following situations occurs:

- In an infrastructure BSS, the AP deauthenticates or disassociates the non-AP STA, or
- In a mesh BSS, the mesh STA providing GCR service tears down the peer link to the mesh STA receiving GCR frames, or
- The non-AP STA or mesh STA receiving GCR frames successfully transmits a DMS Request frame to the AP or mesh STA providing GCR service containing a DMS Request element that has a DMS Descriptor with the DMSID identifying the group addressed stream and the Request Type field set to “Remove,” or
- The AP or a mesh STA providing GCR service successfully transmits an individually addressed DMS Response frame with a DMS Response element containing a DMS Status field with the DMSID identifying the group addressed stream that has the Status field set to “Terminate.”

Table 10-9b—Non-AP STA recovery procedures for a changed delivery method

Current delivery method state at non-AP STA	Actual delivery method being used by the AP	Recovery procedure
Non-GCR-SP	GCR-SP	<p>A non-AP STA shall update the current delivery method state of the GCR stream to GCR-SP if</p> <ul style="list-style-type: none"> a) No frames with the More Data field in the Frame Control field equal to 1 for the GCR stream are received for a period of <code>dot11GCRPolicyChangeTimeout</code>, and b) At least one frame for the GCR stream with the More Data field in the Frame Control field equal to 0 is received. <p>Note that upon detecting condition a), the STA should enter the Awake state in order to assist with detecting condition b).</p>
GCR-SP	Non-GCR-SP	<p>A non-AP STA shall update the current delivery method of the GCR stream to Non-GCR-SP if no frames with the More Data field in the Frame Control field equal to 0 for the GCR stream are received for a period of <code>dot11GCRPolicyChangeTimeout</code> and at least one frame for the GCR stream with the More Data field in the Frame Control field equal to 1 is received.</p>

A GCR agreement between a non-AP STA and an AP or between peer mesh STAs shall end (as described in 10.23.15.2) with the following modifications:

- The DMS Status field shall include a GCR Response subelement.
- The DMS response frame may be transmitted by an AP to the GCR concealment address or as an individually addressed frame to each STA that has an active GCR agreement for this GCR group address. The DMS response frame shall be transmitted by a non-AP STA or mesh STA as an individually addressed frame to the STA that it has an active GCR agreement for this GCR group address.

A cancellation of a GCR agreement shall also cause the Block Ack agreement to be cancelled for the GCR stream.

10.23.15.3.5 Concealment of GCR transmissions

Concealment prevents group addressed frames transmitted via the GCR unsolicited retry or GCR Block Ack retransmission policies from being passed up through the MAC_SAPs of GCR-incapable STAs.

GCR group addressed MSDUs shall be sent in an A-MSDU when

- Retransmitted via the GCR unsolicited retry or GCR Block Ack retransmission policies or
- Transmitted via the GCR-SP delivery method.

The MPDU containing this A-MSDU shall have the Address 1 field set to `dot11GCRConcealmentAddress` and the Retry bit of the Frame Control field set to 1. The DA field in the A-MSDU subframe shall contain the GCR group address that is being concealed (i.e., the same value as the DA field for non-GCR group addressed delivery). One A-MSDU subframe shall be contained within one A-MSDU frame. GCR group addressed MSDUs retransmitted via the GCR unsolicited retry or GCR Block Ack retransmission policies shall set the Sequence Control field of the MPDU containing this A-MSDU to the same value as the Sequence Control field of the frame that contained the corresponding MSDU that was transmitted with the Retry bit equal to 0. The first transmission attempt of a GCR group addressed MSDU transmitted via the

GCR-SP delivery method shall set the Sequence Control field of the MPDU containing this A-MSDU according to the procedures defined in 9.3.2.10.

A STA with `dot11RobustAVStreamingImplemented` true or `dot11MeshGCRImplemented` true shall not use its GCR concealment address for any purpose other than the transmission of GCR streams.

A STA with `dot11RobustAVStreamingImplemented` true or `dot11MeshGCRImplemented` true and with a GCR agreement shall add the GCR concealment address from the GCR Response subelement to the STA's `dot11GroupAddressesTable`.

An AP with `dot11RobustAVStreamingImplemented` true shall not send an MSDU to the DS that has the DA field set to the GCR concealment address.

The Individual/Group Address bit (LSB of octet 0) of `dot11GCRConcealmentAddress` shall be set to 0.

10.23.15.3.6 GCR unsolicited retry

A STA supports the GCR unsolicited retry retransmission policy if `dot11RobustAVStreamingImplemented` or `dot11MeshGCRImplemented` is true; otherwise, the STA does not support the GCR service with retransmission policy equal to GCR unsolicited retry.

An AP or a mesh STA adopting the GCR unsolicited retry retransmission policy for a GCR group address chooses a lifetime limit for the group address. The AP or a mesh STA may vary the lifetime limit for the group address at any time and may use different lifetime limits for different GCR group addresses. An AP adopting the GCR unsolicited retry retransmission policy for a GCR group address shall transmit each MSDU according to 10.23.15.3.5, subject to the lifetime and retry limits. Transmission uses the backoff procedure described in 9.19.2.6.2.

If a Block Ack agreement has successfully been established for a group addressed stream that is delivered using the GCR unsolicited retry retransmission policy, the STA shall follow the duplicate detection procedures defined in 9.3.2.10 and 9.20.4.

If a Block Ack agreement has successfully been established for all STAs receiving a GCR group address, for a group delivered using the GCR unsolicited retry retransmission policy, the AP may retransmit any of the last m A-MSDUs that have the DA field in the A-MSDU subfield set to the GCR group address, where m is GCR buffer size (as defined in 10.23.15.3.7), subject to the lifetime limits.

If there is a STA with an active GCR agreement for a group address that does not have an active Block Ack agreement, the AP shall not retransmit a preceding A-MSDU for that group address. A preceding A-MSDU is defined as an A-MSDU with a sequence number value that precedes, using the modulo 2^{12} rules defined in 9.21.1, the sequence number value of the last transmitted A-MSDU for the GCR group address.

10.23.15.3.7 GCR Block Ack

A STA supports the GCR Block Ack retransmission policy if `dot11AdvancedGCRImplemented` is true or `dot11MeshGCRImplemented` is true; otherwise, the STA does not support the GCR service with retransmission policy equal to GCR Block Ack.

The AP shall maintain a set of the most recently received values of the Buffer Size subfield from the Block Ack Parameter Set field in the ADDBA Response frame received from each member of a specific group address. The minimum of that set of values is defined to be the *GCR buffer size* for that group address (see 9.21.10).

10.23.15.3.8 GCR-SP

The GCR-SP delivery method transmits GCR group addressed frames at intervals that might be smaller than the beacon interval.

A STA supports the GCR-SP delivery method if `dot11AdvancedGCRImplemented` is true; otherwise, the STA does not support the GCR service with the delivery method equal to GCR-SP.

NOTE—Group addressed traffic transmitted at the end of a DTIM beacon might be an impediment to providing QoS for uplink transmissions and in OBSSs. Therefore, APs in an overlapped environment are advised to make use of GCR-SP for group addressed traffic that consumes appreciable medium time.

Group addressed MSDUs shall not be transmitted via the GCR-SP delivery method policy if a non-GCR-SP delivery method is active for that group address.

All MSDUs transmitted via the GCR-SP delivery method shall be concealed using the procedures described in 10.23.15.3.5. A STA receiving group addressed MSDUs transmitted via the GCR-SP delivery method shall discard all nonconcealed MSDUs for this group address.

An AP advertises that a group addressed stream is subject to GCR-SP within a GCR Response subelement. The subelement indicates the start of each SP. See 10.2.1.5. When the Service Interval field in the Schedule element of the DMS Response frame is greater than 0, at every scheduled SP, the AP schedules for transmission buffered GCR-SP group addressed frames assigned to that particular group address.

An AP shall not establish both a GCR-SP and an FMS agreement for a group addressed stream with a single non-AP STA.

An AP may use the GCR-SP delivery method for an accepted GCR service when all the non-AP STA that requested the GCR service for the group address have the Robust AV Streaming bit in the Extended Capabilities element equal to 1 and the Advanced GCR bit in the Extended Capabilities element equal to 1. Otherwise, the AP shall not use the GCR-SP delivery method for the accepted GCR service.

When the Service Interval field in the Schedule element of the DMS Response frame is 0, the AP may transmit group addressed frames that are subject to this GCR agreement at any time without regard to the power state of non-AP STAs in the group. This delivery method is called GCR-A, where all members of the group need to stay in the Awake state to receive these group addressed frames.

10.25 Quality-of-service management frame (QMF)

10.25.2 QMF policy advertisement and configuration procedures

10.25.2.2 QMF policy change in an infrastructure BSS or in an MBSS

Insert the following paragraph at the end of 10.25.2.2:

An AP for which `dot11AlternateEDCAActivated` is true shall not use the alternate video (A_VI) nor alternate voice (A_VO) transmit queues in its QMF policy.

Insert the following subclauses, 10.26 to 10.27.4.3 (including Table 10-14), after 10.25.3:

10.26 Robust AV streaming

10.26.1 Robust AV streaming dependencies

When dot11RobustAVStreamingImplemented is true, the STA is a robust AV streaming STA. The attribute dot11QosOptionImplemented shall be true in a robust AV streaming STA.

10.26.2 SCS procedures

The stream classification service (SCS) is a service that may be provided by an AP to its associated STAs that support SCS. In SCS, the AP classifies incoming unicast MSDUs based upon parameters provided by the non-AP STA.

The classification allows the UP, drop eligibility, and EDCA transmit queue to be selected for all MSDUs matching the classification.

Implementation of SCS is optional for a STA. A STA that implements SCS has dot11SCSImplemented set to true. A STA that has a value of true for dot11SCSActivated is defined as a STA that supports stream classification. When dot11SCSActivated is true, dot11SCSImplemented shall be true. A STA for which dot11SCSActivated is true shall set the SCS field of the Extended Capabilities element to 1.

A non-AP STA that supports SCS may request use of SCS by sending an SCS Request frame that includes an SCS Descriptor element with the Request Type field set to “Add” or “Change.” The SCS Descriptor List field in the SCS Descriptor element identifies how MSDUs are classified and the priority to assign to MSDUs that match this classification. If the TCLAS Processing element is present in an SCS Descriptor element, the Processing subfield shall have a value of 0 or 1. An AP shall decline any SCS Request frame where a TCLAS Processing element is present and the Processing subfield does not have a value of 0 or 1.

Each SCS stream is identified by an SCSID. This SCSID is used by a non-AP STA to request creation, modification, or deletion of an SCS stream. The SCSID is used by an AP to identify an SCS stream in SCS responses.

Upon receipt of an SCS Request frame from an associated non-AP STA, the AP shall respond with a corresponding SCS Response frame. A value of “SUCCESS” shall be set in the corresponding Status field of the SCS Status duple in the SCS Response frame when the AP accepts the SCS request for the requested SCSID. A value of “REQUEST_DECLINED,” “REQUESTED_TCLAS_NOT_SUPPORTED_BY_AP,” or “INSUFFICIENT_TCLAS_PROCESSING_RESOURCES” shall be set in the corresponding SCS Status field of the SCS Status duple in the SCS Response frame when the AP denies the SCS request for the requested SCSID.

If the AP declines a request to change a previously accepted SCSID, the previously accepted classification for this SCSID continues to operate.

If the requested SCS is accepted by the AP, the AP shall process subsequent incoming unicast MSDUs from the DS or WM that match the TCLAS elements and optional TCLAS Processing element classifier specified in the SCS Descriptor element.

A match of the classifier is defined as follows:

- When the Processing subfield of the TCLAS Processing element is 0, the classifier matches all the parameters in the TCLAS elements in the SCS Descriptor element.

- When the Processing subfield of the TCLAS Processing element is 1 or the TCLAS Processing element is not present, the classifier matches if the parameters match at least one of the TCLAS elements in the SCS Descriptor element.

The processing of matching MSDUs depends upon the access policy assigned to the MSDU:

- For matching MSDUs that are not part of a TS (as described in 10.4), the User Priority subfield of the Intra-Access Category Priority element is used as the UP of these MSDUs.
- For matching MSDUs that are part of a TS (as described in 10.4), the TID and UP classification of these MSDUs shall follow the rules specified in 10.4.8.
- If dot11AlternateEDCAActivated is true, for matching MSDUs that are not part of a TS (as described in 10.4) or for MSDUs that are part of a TS that uses EDCA or HEMM as the access policy, the Alternate Queue subfield of the Intra-Access Category Priority element is used to select whether the primary EDCA transmit queue or alternate EDCA transmit queue is used for these MSDUs.
- All matching MSDUs have their DEI set using the value from the Drop Eligibility subfield of the Intra-Access Category Priority element in the DEI subfield of the HT Control field, as defined in 8.2.4.6.

A non-AP STA may request the termination of an accepted SCS stream by sending an SCS Request frame with the Request Type field set to “Remove” and the requested SCSIDs in the SCS Descriptor element. The Length field of the SCS Descriptor element is set to 0; and no Intra-Access Priority, TCLAS, or TCLAS Processing elements shall be included in the SCS Descriptor element.

Upon reception of a request to terminate a previously accepted SCS stream, the AP shall cease to apply the classifier related to this SCSID. The AP shall send an SCS Response frame to confirm the termination of the SCS stream identified by the SCSID, by including the SCSID and a value of “Terminate” in the Status field of an SCS Status duple in an SCS Response frame and the dialog token in the SCS Response frame set to the value from the SCS Request frame that requested termination.

The AP may send an unsolicited SCS Response frame at any time to cancel a granted SCS stream identified by the SCSID, by including the SCSID and a value of “Terminate” in the Status field of an SCS Status duple in an SCS Response frame and the dialog token in the SCS Response frame set to 0.

10.27 Procedures to manage OBSS

10.27.1 General

QLoad Report elements, HCCA TXOP Update Count elements, HCCA TXOP Advertisement action frames, and HCCA TXOP Response action frames are designed to mitigate the effects of OBSSs and provide the means to

- Advertise QoS load information for channel selection
- Extend the admission control and scheduled mechanisms to a distributed environment
- Enable the coordination of scheduled HCCA TXOPs between HCs operating with OBSSs

OBSS APs are APs that are using the same primary channel and that are able to receive or obtain frames from each other, including Beacon frames. These frames are received directly or via associated STAs that support the Beacon Request capability (as indicated by the Beacon Passive Measurement capability enabled bit or the Beacon Active Measurement capability enabled bit being set in the RM Enabled Capabilities element in the (Re)Association frame). An AP might scan other channels as part of its channel selection process or might request associated STAs that have the Beacon Request capability enabled to perform an off-channel Beacon Request measurement, and these procedures might provide QLoad Report elements

received from APs operating on other channels. Subclause X.3 provides an example of using QLoad Reports from adjacent channels.

NOTE 1—These OBSS procedures might use unauthenticated Beacon frames and public action frames. Implementations might choose to use additional heuristics (e.g., a history of collaboration and traffic monitoring) to determine the authenticity of this information.

NOTE 2—These OBSS procedures are intended for stationary and portable APs (see 4.2.4).

10.27.2 QLoad Report element

10.27.2.1 Introduction

The QLoad Report element is contained in QLoad Report frames or Protected QLoad Report frames that are provided by an AP and, optionally, periodically in the Beacon frame. The QLoad Report frame is transmitted, upon the receipt of a QLoad Request frame by an AP for which `dot11QLoadReportActivated` is true, to the STA that sent the QLoad Request frame. An AP shall not send a QLoad Request frame or Protected QLoad Request frame to another AP that has QLoad Report field set to 0 in its Extended Capability element. The Protected QLoad Report frame is transmitted, upon the receipt of a Protected QLoad Request frame when `dot11ProtectedQLoadActivated` is true, to the STA that sent the Protected QLoad Request frame. An AP for which `dot11ProtectedQLoadReportActivated` is false shall discard any received Protected QLoad Request or Protected QLoad Report frames.

Whenever there is a change in the contents of the QLoad Report element and there is no pending delay period for an unsolicited QLoad Report frame, an unsolicited QLoad Report frame should be transmitted with the RA field set to the broadcast address, after a randomly selected delay between 1 and `dot11QLoadReportDelay` seconds. After this delay, the AP shall transmit an unsolicited QLoad Report frame that contains the most recently available QLoad information. When `dot11QLoadReportActivated` is true, the QLoad Report element shall be included in the Beacon frame every `dot11QLoadReportIntervalDTIM` DTIMs. When `dot11QLoadReportActivated` is false, the QLoad Report element shall not be included in Beacon frames.

10.27.2.2 Calculating field values

The value of the Potential Traffic Self field represents the potential QoS traffic of this BSS; therefore, the value in the Mean subfield shall always be equal to or greater than the value of the Mean subfield in the Allocated Traffic Self field.

The AP shall include in the Allocated Traffic Self field all accepted and not deleted TSPECs as they are sent by non-AP STAs. At the deletion of each such TSPEC, the AP shall remove the TSPEC from its Allocated Traffic Self field.

The number of active AC_VI and AC_VO streams shall be provided in the Allocated Traffic Self field. For each admitted admission control TSPEC, the AP calculates a medium time, as described in L.2.2. This medium time, however, does not include the medium access overhead that, in turn, is related to the number of streams. This access overhead is further discussed in X.2.7, and a recommendation is given for its value.

An example of a method of calculating the values for the Mean and Standard Deviation subfields in the Potential Traffic Self field is given in X.2.3.

The Sharing Policy field is used to indicate the currently active policy for sharing the medium with OBSSs. Setting the Sharing Policy field to “Static” indicates that the share of the total available medium time of an AP does not change when the value of the Allocated Traffic Shared field changes. Setting the Sharing Policy field to “Dynamic” indicates that the share of the total available medium time of an AP might change when

the value of the Allocated Traffic Shared field changes. If the Sharing Policy field has the value “Vendor Specific,” then the QLoad Report element shall contain a Vendor Specific subelement.

If the value of the Overlap field changes, the share of the total available medium time of an AP might change for both static and dynamic sharing policies.

The value of the Potential Traffic Self field represents the potential QoS traffic of this AP and, therefore, shall always be equal to or greater than the values represented by the Allocated Traffic Self field.

The Allocated Traffic Self field contains the mean and standard deviation values of the total EDCA admission control and HCCA traffic that the AP has allocated at any one time and contains the number of AC_VI and AC_VO EDCA admission control streams. As each stream is added or deleted, the AP shall calculate the new value of the Allocated Traffic Self field. A recommended method for calculating the Allocated Traffic Self field mean and standard deviation values is given in X.2.4.

The Allocated Traffic Shared field is calculated from the Allocated Traffic Self field values for all APs that overlap with the AP performing the calculation, including the Allocated Traffic Self field value of the AP performing the calculation. A recommended method for summing the Allocated Traffic Self field values is given in X.2.4.

The EDCA Access Factor is the total traffic bandwidth requirement for all the OBSSs expressed as a fraction that may be greater than 1. An implementation might calculate the EDCA Access Factor from the summation of the Potential Traffic Self field values of all the APs that are overlapping, as follows:

- a) Sum all the Potential Traffic Self field values for all OBSSs, including self, in order to calculate the peak traffic requirement in multiples of 32 μ s per second. As the Potential Traffic Self field value is expressed in terms of mean and standard deviations, it is possible to sum the Potential Traffic Self field values as a composite stream. A suggested method for this summation is given in X.2.3.
- b) Sum all the HCCA Peak field values from all OBSSs, including self, in order to calculate the peak HCCA traffic requirement, in multiples of 32 μ s per second.
- c) Subtract the value derived in step b) from the value derived in step a). This value is the EDCA traffic.
- d) Sum the AC_VO and AC_VI streams reported in its own QLoad report and all the QLoad reports of OBSSs. Based upon the number of EDCA streams, an EDCA Overhead Factor can be estimated to account for the medium access time requirements. EDCA Overhead Factor is further discussed in X.2.3, and a recommendation is given for its value.
- e) Multiply together the EDCA traffic from step c) and the EDCA Overhead Factor to obtain a value that represents the total peak bandwidth requirement for the OBSSs. This value is in multiples of 32 μ s per second.
- f) Convert the total peak bandwidth requirement to a fraction that is rounded down to a multiple of 1/64 (8 bits). This value is the EDCA Access Factor. An example for this conversion is given in X.2.6.

The HCCA Peak field value is the sum of the all the medium times of active TS that use the HCCA or HEMM access policy over a 1 s period for all the HCCA TSPECs included in the QLoad field. The TXOP time, scheduled by the HC, multiplied by the reciprocal of its SI, is termed the *HCCA medium time*. The HCCA Peak field value is the summation of the HCCA medium times that the HC has scheduled, in multiples of 32 μ s.

The HCCA Access Factor is the total HCCA TXOP medium time requirement for all the OBSSs expressed as a fraction that may be greater than 1. An implementation might calculate the HCCA Access Factor from the summation of the HCCA Peak field values of all the APs that in an OBSS, by summation of all the

HCCA Peak field values for all APs in OBSSs and converting this summation to a fraction that is rounded down to 1/64 (8 bits). An example for this conversion is given in X.2.8.

10.27.2.3 Requesting QLoad Reports using radio measurement requests

If an AP has associated STAs that support passive or active beacon measurement (as indicated by the Beacon Passive Measurement capability enabled bit or the Beacon Active Measurement capability enabled bit being set in the RM Enabled Capabilities element), it may use the neighbor report capability of these associated STAs to attempt to retrieve QLoad Report elements from APs with which the AP is unable to exchange frames directly.

The AP sends a Radio Measurement Request frame that contains a Measurement Request element to an associated STA that supports neighbor reporting and beacon reporting. This Measurement Request element has the Measurement Type field set to “Beacon Request” (as defined in Table 8-59), and the BSSID field of the Measurement Request field of the Beacon Request frame (as defined in Figure 8-113) is set to the wildcard BSSID. There shall be a Request subelement in the Measurement Request field of the Beacon Request frame that contains the Element ID of the QLoad Report element (as defined in Table 8-54) and may contain other element IDs. The SSID subelement shall not be included in the Request subelement of the Measurement Request field of the Beacon Request frame.

Depending upon the signaled enabled radio measurement capabilities of the associated STA, the AP may use either the passive or active measurement mode. The Channel Number field should be set to the primary channel number that is currently being used by the AP, but may be set to other values if off-channel beacon measurement is supported by the STA to which the measurement request is to be sent.

If the measurement request is accepted, the requested STA performs the measurement request (as described in 10.11). The subsequent Radio Measurement Report frame contains beacon reports for successful measurements. These beacon reports might contain QLoad Report elements inside a Reported Frame Body subelement, if the reporting STA received QLoad Report elements from the Beacon or Probe Response frames that it received from neighboring APs. The contents of these QLoad Report elements can then be used in calculating Allocated Traffic Shared, EDCA Access Factor, and HCCA Access Factor field values as described in 10.27.2.2.

10.27.3 HCCA TXOP negotiation

The procedures described in this subclause allow HCCA APs to cooperatively create new HCCA schedules that do not collide.

When sharing with at least one other HCCA AP, each sharing AP for which `dot11RobustAVStreamingImplemented` is true shall set its `dot11HCCWmax` to a value of at least 3.

HCCA APs that are able to directly exchange frames without the use of a third-party STA and signal support for unprotected or protected TXOP negotiation (as indicated by the Unprotected TXOP Negotiation or Protected TXOP Negotiation field equal to 1 in the Extended Capabilities element in Beacon frames) coordinate their TXOP schedules using HCCA TXOP Advertisement and HCCA TXOP Response frames. In this subclause, an HCCA AP in an OBSS that is able to directly exchange frames without the use of a third-party STA is referred to as a *collaboration candidate*.

The HCCA TXOP Update Count element is included in the Beacon frame to indicate that an HCCA TXOP schedule has changed. The Update Count field of the HCCA TXOP Update Count element is incremented (modulo 256) each time a TS with an access policy of HCCA or HEMM is created or deleted. An HCCA AP for which `dot11PublicHCCATXOPNegotiationActivated` is true or `dot11ProtectedHCCATXOPNegotiationActivated` is true shall advertise the Duration, Service Interval, and

Start Time subfields for each HCCA TXOP reservation in a TXOP Reservation field as described in 8.4.1.43.

An HCCA AP for which `dot11PublicTXOPNegotiationImplemented` is true or `dot11ProtectedTXOPNegotiationImplemented` is true shall be able to maintain one or more `dot11APCEntry(s)` for each collaboration candidate in the `dot11APCTable`. These fields indicate the schedules that the AP should try to avoid using when creating schedules for new TS requests.

Before accepting a TSPEC request that has the Access Policy subfield of the TSPEC element equal to “HCCA” or “HEMM,” an HC for which `dot11PublicTXOPNegotiationImplemented` is true or `dot11ProtectedTXOPNegotiationImplemented` is true should examine all `dot11APCEntry(s)` that are present in the `dot11APCTable`.

When an AP with `dot11PublicHCCATXOPNegotiationActivated` true or with `dot11ProtectedHCCATXOPNegotiationActivated` true receives a TSPEC request that has the Access Policy subfield of the TSPEC element equal to “HCCA” or “HEMM,” it shall send an HCCA TXOP advertisement to each collaboration candidate. These HCCA TXOP advertisements shall have the TXOP Reservation field set to the TXOP that the AP is attempting to schedule.

An AP with `dot11ProtectedTXOPNegotiationActivated` true shall send the HCCA TXOP advertisement using a Protected HCCA TXOP Advertisement frame to each collaboration candidate that indicates support for protected HCCA TXOP negotiation (as indicated by the Protected TXOP Negotiation field equal to 1 in the Extended Capabilities element in Beacon frames from the collaboration candidate).

An AP with `dot11PublicTXOPNegotiationActivated` true shall send the HCCA TXOP advertisement using a HCCA TXOP Advertisement frame to each collaboration candidate that indicates support for unprotected HCCA TXOP negotiation (as indicated by the Unprotected TXOP Negotiation field equal to 1 in the Extended Capabilities element in Beacon frames from the collaboration candidate) unless the HCCA TXOP advertisement has already been transmitted to this collaboration candidate using a Protected HCCA TXOP Advertisement frame.

NOTE—When peer APs have both unprotected and protected TXOP negotiation activated, protected TXOP negotiation is used.

The AP shall not send an ADDTS Response frame to the requesting STA until one of the following conditions occurs:

- a) The AP has received an HCCA TXOP Response frame, with the Status field equal to “SUCCESS,” from all the APs to which HCCA TXOP advertisements were sent.
- b) At least two Beacon frames have been received from all the APs to which HCCA TXOP advertisements were sent.
- c) A Beacon frame containing the HCCA TXOP Update Count element is received from all the APs to which HCCA TXOP advertisements were sent.
- d) A period of three `dot11BeaconPeriod` TU has elapsed.

If an AP receives another TSPEC request while waiting for one of the above conditions to occur, it shall delay processing this additional TSPEC request until one of the above conditions occurs.

An AP with `dot11PublicTXOPNegotiationActivated` false shall discard any received HCCA TXOP Advertisement frames. An AP with `dot11ProtectedTXOPNegotiationActivated` true shall discard any received HCCA TXOP Advertisement frames from a peer AP with which it has an active security association.

Upon reception of an unprotected HCCA TXOP Advertisement frame, an AP with `dot11PublicTXOPNegotiationActivated` true shall discard all `dot11APCEntry(s)` from the `dot11APCTable`

that have dot11APEntryMACAddress equal to the MAC address of the AP that sent the HCCA TXOP Advertisement frame and shall prepare a response using the procedures below.

An AP with dot11ProtectedTXOPNegotiationActivated false shall discard any received Protected HCCA TXOP Advertisement frames.

An AP with dot11ProtectedTXOPNegotiationActivated true that does not have an active security association with a peer AP that indicates support for protected HCCA TXOP negotiation shall use the AP PeerKey protocol (as defined in 11.10) and authenticated mesh peering exchange (AMPE) (as defined in 13.5) to negotiate security parameters and create a new SMKSA and STKSA to secure the Protected HCCA TXOP Advertisement frames. The use of AMPE proves possession of the PMK (generated using the procedures described in 11.10) and implicitly the private key that corresponds to the peer's public key.

Upon reception of a valid Protected HCCA TXOP Advertisement frame, an AP with dot11ProtectedTXOPNegotiationActivated true shall discard all dot11APEntry(s) from the dot11APCTable that have dot11APEntryMACAddress equal to the MAC address of the AP that sent the Protected HCCA TXOP Advertisement frame and shall prepare a response using the procedures below.

If the (Protected) HCCA TXOP Advertisement frame has not been discarded due to the procedures above, the AP shall create a dot11APEntry in the dot11APCTable for each TXOP reservation in the Active TXOP Reservations field of the (Protected) HCCA TXOP Advertisement frame.

If the (Protected) HCCA TXOP Advertisement frame has not been discarded due to the procedures above, the AP shall inspect its HCCA schedule to check whether the TXOP reservations number given in the Pending TXOP Reservations field of the HCCA TXOP Advertisement frame is in conflict with an existing accepted HCCA TXOP, allocated by itself. If there is no conflict, the AP shall send an HCCA TXOP Response frame with the Status field set to "SUCCESS" and create a dot11APEntry for each TXOP reservation in the Pending TXOP Reservations field in the HCCA TXOP Advertisement frame.

If the HCCA advertisement was sent using an unprotected Public Action frame, the HCCA TXOP response shall be sent using an unprotected Public Action frame.

If the HCCA advertisement was sent using a Protected HCCA TXOP Advertisement frame, the HCCA TXOP response shall be sent using a Protected HCCA TXOP Response frame.

If the AP detects that the TXOP given in the (Protected) HCCA TXOP Advertisement frame is in conflict with an existing accepted HCCA TXOP and this AP is not itself currently processing an ADDTS request, it shall send a (Protected) HCCA TXOP Response frame with the Status field set to "TS_SCHEDULE_CONFLICT," the Alternate Schedule field set to a period of time that does not conflict with any currently accepted HCCA TXOPs, and the Avoidance Request field absent. The Duration subfield of the Alternate Schedule field should be greater than or equal to the Duration subfield of the Schedule field in the (Protected) HCCA TXOP Advertisement frame. The Duration subfield of the Alternate Schedule field may be less than the Duration subfield of the Schedule field in the (Protected) HCCA TXOP Advertisement frame when there is an insufficient period of time that does not conflict with currently accepted HCCA TXOPs.

If the AP detects that the TXOP given in the (Protected) HCCA TXOP Advertisement frame is in conflict with an in-progress ADDTS request for a HCCA TXOP for which HCCA TXOP Response frames have not been received, it shall send a (Protected) HCCA TXOP Response frame with the Status field set to "TS_SCHEDULE_CONFLICT" and the Alternate Schedule and Avoidance Request fields set according to the following rules:

- If $MIX(MAC_i) < MIX(MAC_j)$, the Alternate Schedule field is set to a value that does not conflict with any accepted HCCA TXOPs and also does not conflict with the TXOP of the in-progress

ADDTS request. The Avoidance Request field is set to the TXOP of the in-progress ADDTS request.

- If $MIX(MAC_r) > MIX(MAC_i)$, the Alternate Schedule field is set to the value from the TXOP Reservation field from the HCCA TXOP Advertisement frame. The Avoidance Request field is set to a time period that does not conflict with any accepted HCCA TXOPs nor the TXOP in the Alternate Schedule field and has sufficient duration and service interval to meet the requirements of the in-progress ADDTS request.

where

- MAC_r is the MAC address of the AP that received the HCCA TXOP Advertisement frame
- MAC_i is the MAC address of the AP that sent the HCCA TXOP Advertisement frame

The MIX function takes the 6 octets of a MAC address and computes a new 6 octet value:

$$MIX(MAC) = MAC[4] \parallel MAC[5] \parallel MAC[0] \parallel MAC[1] \parallel MAC[2] \parallel MAC[3]$$

Table 10-14 provides a summary of the values used in a HCCA TXOP Response frame.

Table 10-14—Contents of HCCA TXOP Response frame

Case	Status code	Alternate Schedule field	Avoidance Request field
No conflict with existing or in-progress schedules	SUCCESS	Not present	Not Present
Conflicts with existing schedule; no ADDTS request in progress	TS_SCHEDULE_CONFLICT	Period of time that does not conflict with any currently accepted HCCA TXOPs	Not Present
Conflict with in-progress schedules, $MIX(MAC_r) < MIX(MAC_i)$	TS_SCHEDULE_CONFLICT	Period of time that does not conflict with any currently accepted HCCA TXOPs nor the in-progress ADDTS request	Schedule of in-progress ADDTS request
Conflict with in-progress schedules, $MIX(MAC_r) > MIX(MAC_i)$	TS_SCHEDULE_CONFLICT	Same schedule that was in the HCCA TXOP Advertisement frame	Period of time that does not conflict with any currently accepted HCCA TXOPs nor the period given in the Alternate Schedule field

The AP shall keep a record of the TXOP proposed in the Alternate Schedule field in a TXOP avoidance record and should avoid scheduling any new HCCA TXOPs in this proposed period until any of the following conditions occurs:

- A period of $dot11HCCATXOPBeaconTimeout$ multiplied by $dot11BeaconPeriod$ TUs has elapsed.
- The AP with $dot11PublicTXOPNegotiationActivated$ true receives an unprotected HCCA TXOP Advertisement frame from the AP to which the unprotected HCCA TXOP Response frame was sent.
- The AP with $dot11ProtectedTXOPNegotiationActivated$ true receives a Protected HCCA TXOP Advertisement frame from the AP to which the Protected HCCA TXOP Response frame was sent.

If an AP with `dot11PublicTXOPNegotiationActivated` true receives an unprotected HCCA TXOP Response frame with the Status field equal to “TS_SCHEDULE_CONFLICT,” the AP should create a new schedule for the TSPEC request using the suggestion provided in the HCCA TXOP Response frame. If an AP with `dot11ProtectedTXOPNegotiationActivated` true receives a Protected HCCA TXOP Response frame with the Status field equal to “TS_SCHEDULE_CONFLICT,” the AP should create a new schedule for the TSPEC request using the suggestion provided in the Protected HCCA TXOP Response frame.

If an AP creates a new schedule in response to a (Protected) HCCA TXOP Response frame, it shall send a new HCCA TXOP advertisement to each collaboration candidate, using the procedures previously defined in this subclause.

After one or more HCCA TXOP Advertisement frame transmissions that cause the reception of an HCCA TXOP Response frame with the Status field equal to “TS_SCHEDULE_CONFLICT,” the AP may terminate the HCCA TXOP advertisement procedure and respond to the ADDTS Request frame with a nonzero status code (decline the ADDTS Request) or a zero status code (accept the ADDTS Request regardless of potential HCCA TXOP conflicts).

10.27.4 HCCA AP timing synchronization for HCCA TXOP advertisement

10.27.4.1 General

HCCA APs in OBSSs for which `dot11RobustAVStreamingImplemented` is true and `dot11PublicHCCATXOPNegotiationActivated` is true synchronize their TSF timing so that the HCCA TXOP advertisement scheme does not suffer from time differences between the clocks of the overlapping APs.

In order to use HCCA TXOP advertisement, the AP maintains synchronization with its APs in OBSSs. HCCA APs that use HCCA TXOP advertisement shall use a DTIM interval with a duration of $2^n \times 100$ TU where n a non-negative integer less than or equal to 5.

NOTE—The DTIM interval of the form $2^n \times 100$ TU has been chosen to facilitate the verification that HCCA TXOP reservations do not overlap. The restriction that n be less than or equal to 5 has been chosen so that the range of the HCCA TXOP start time in the reservation (see 8.4.1.43) is compatible with the maximal DTIM interval length.

10.27.4.2 Timing offset

An HCCA AP with `dot11PublicHCCATXOPNegotiationImplemented` true or `dot11ProtectedHCCATXOPNegotiationImplemented` true shall update the timing offset value based on time stamps from the received Beacon frames from HCCA APs that have an entry in the `dot11APCTable`. The timing offset value is calculated using Equation (10-4).

$$T_{offset} = T_T - T_R \quad (10-4)$$

where

T_{offset} is the timing offset value

T_T is the value in the Timestamp field in the received Beacon frame from the overlapping HCCA AP

T_R is the Beacon frame reception time measured using the HCCA AP’s TSF timer

The offset value is represented as twos complement. The unit of the offset value is microseconds. The HCCA AP shall keep the T_{offset} value calculated from the latest Beacon frame received from each AP in an OBSS.

10.27.4.3 Clock drift adjustment

When `dot11RobustAVStreamingImplemented` is true and `dot11PublicHCCATXOPNegotiationActivated` is true, the HCCA AP shall examine the reception time of the Beacon frames from overlapping HCCA APs with which it maintains synchronization and adjust its TSF timer to compensate the relative timing error among overlapping HCCA APs caused by the clock drift. The HCCA AP adjusts its TSF so that its TSF counting frequency is aligned to the AP with the lowest TSF counting frequency.

The HCCA AP shall operate the following clock drift compensation procedure:

- a) If the HCCA AP does not have a valid T_{offset} value obtained from the previous Beacon frame reception from a particular overlapping HCCA AP, it shall not operate the clock drift compensation for that AP.
- b) When the HCCA AP receives a Beacon frame from one of the overlapping HCCA APs with which it maintains synchronization, the HCCA AP shall calculate the clock drift amount $T_{ClockDrift}$ by comparing the T_{offset} obtained previously for this overlapping HCCA AP and the T_{offset} obtained from the Beacon frame reception. See Equation (10-5).

$$T_{ClockDrift} = T_{offset,1} - T_{offset,0} \quad (10-5)$$

where

- $T_{ClockDrift}$ is the clock drift amount represented as twos complement, in microseconds
- $T_{offset,1}$ is the T_{offset} obtained from the previous reception
- $T_{offset,0}$ is the T_{offset} obtained from the current frame reception

- c) The HCCA AP shall calculate the $T_{ClockDrift}$ value for all overlapping HCCA APs with which it maintains synchronization and select the largest $T_{ClockDrift}$ value. If the largest $T_{ClockDrift}$ is greater than zero, it shall suspend its TSF timer for the duration of the largest $T_{ClockDrift}$. The HCCA AP shall suspend its TSF timer frequently enough so that the delay amount within a single beacon period does not exceed 0.08% of its beacon interval.

NOTE—This clock drift compensation procedure is not intended to maintain a strict synchronization. It aims to stop TBTT drifting away among overlapping HCCA Aps to allow some jitter of TSF timer.

11. Security

11.8 Per-frame pseudo-code

11.8.2 RSNA frame pseudo-code

11.8.2.8 Per-MSDU/Per-A-MSDU Rx pseudo-code

Change the pseudo code in 11.8.2.8 as indicated:

```

if dot11RSNAActivated = TRUE then
  if the frame was not protected then
    Receive the MSDU or A-MSDU unprotected
    Make MSDU(s) available to higher layers
  else if address1 has an individual RA then // Have a protected MSDU or A-MSDU
    if Pairwise key is an AES-CCM key then
      Accept the MSDU or A-MSDU if its MPDUs had sequential PNs (or if it consists of
        only one MPDU), otherwise discard the MSDU or A-MSDU as a replay attack and
        increment dot11RSNAStatsCCMPReplays

```

```

        Make MSDU(s) available to higher layers
    else if Pairwise key is a TKIP key then
        Compute the MIC using the Michael algorithm
        Compare the received MIC to the computed MIC
        discard the frame if the MIC fails increment
        dot11RSNAStatsTKIPLocalMICFailures and invoke countermeasures if
        appropriate
        compare TSC to replay counter, if replay check fails increment
        dot11RSNAStatsTKIPReplays
        otherwise accept the MSDU
        Make MSDU available to higher layers
    else if dot11WEPKeyMappings has a WEP key then
        Accept the MSDU since the decryption took place at the MPDU
        Make MSDU available to higher layers
    endif
else // Have a group addressed MSDU or A-MSDU
    if GTK for the Key ID does not exist then
        discard the frame body and increment dot11WEPUndecryptableCount
    else if GTK for the Key ID is null then
        discard the frame body and increment dot11WEPUndecryptableCount
    else if GTK for the Key ID is a CCM key then
        Accept the MSDU or A-MSDU if its MPDUs had sequential PNs (or if it consists of
        only one MPDU), otherwise discard the MSDU or A-MSDU as a replay attack and
        increment dot11RSNAStatsCCMPReplays
        Make MSDU(s) available to higher layers
    else if GTK for the Key ID is a TKIP key then
        Compute the MIC using the Michael algorithm
        Compare the received MIC to the computed MIC
        discard the frame if the MIC fails increment
        dot11RSNAStatsTKIPLocalMICFailures and invoke countermeasures if
        appropriate
        compare TSC to replay counter, if replay check fails increment
        dot11RSNAStatsTKIPReplays
        otherwise accept the MSDU
        Make MSDU available to higher layers
    else if GTK for the Key ID is a WEP key then
        Accept the MSDU since the decryption took place at the MPDU
        Make MSDU available to higher layers
    endif
endif
endif

```

Insert the following subclauses, 11.10 to 11.10.2, after 11.9:

11.10 AP PeerKey support

11.10.1 AP PeerKey overview

The AP PeerKey protocol provides session identification and data confidentiality for an AP-to-AP connection. An AP PeerKey association is composed of an SMKSA and an STKSA.

AP PeerKey uses various functions and data to accomplish its task and assumes certain properties about each function as follows:

- H is an “extractor” function (see IETF RFC 5869) that concentrates potentially dispersed entropy from an input to create an output that is a cryptographically strong, pseudorandom key. This function takes as input a non-secret “salt” and a secret input and produces a fixed-length output.
- A finite cyclic group is negotiated for which solving the discrete logarithm problem is computationally infeasible.

When used with AKM 10 from Table 8-101 to indicate AP PeerKey, H shall be instantiated as HMAC-SHA256:

$$H(\text{salt}, \text{ikm}) = \text{HMAC-SHA256}(\text{salt}, \text{ikm})$$

Other instantiations of function H require creation of a new AKM identifier.

11.10.2 AP PeerKey protocol

AP PeerKey uses the same discrete logarithm cryptography as SAE (as described in 11.3) to achieve key agreement. Each party to the exchange has a public and private key with respect to a particular set of domain parameters that define a finite cyclic group. Groups may be based on elliptic curve cryptography (ECC) or finite field cryptography (FFC). Each component of a group is referred to as an “element.” Groups are negotiated using an identifying number from a repository maintained by IANA as “Group Description” attributes for IETF RFC 2409 (IKE) [B17]. The repository maps an identifying number to a complete set of domain parameters for the particular group. For the purpose of interoperability, APs that have `dot11ProtectedHCCATXOPNegotiationImplemented` true or `dot11ProtectedQLoadReportImplemented` true shall support group nineteen (19), an ECC group defined over a 256-bit prime order field.

AP PeerKey uses one arithmetic operator that takes one element and one scalar value to produce another element (called the “scalar operation”). The convention used here is to represent group elements in uppercase bold italic and scalar values in lowercase italic. The scalar operation takes an element and a scalar and is denoted $\text{scalar-op}(x, Y)$.

The private key d shall be chosen randomly so that $1 < d < r$, where r is the order of the group. The public key Q shall be produced using Equation 11-1.

$$Q = \text{scalar-op}(d, G) \tag{11-1}$$

where

G is the generator (also known as the base point) of the group

An AP for which `dot11ProtectedTXOPNegotiationActivated` is true or `dot11ProtectedQLoadReportActivated` is true shall support at least one public key from cyclic group nineteen. An AP for which `dot11ProtectedTXOPNegotiationActivated` is true or `dot11ProtectedQLoadReportActivated` is true may support multiple public keys from multiple cyclic groups. An AP that supports the Multiple BSSID capability and has `dot11ProtectedTXOPNegotiationActivated` true or `dot11ProtectedQLoadReportActivated` true may use one public key across multiple BSSIDs, or it may choose to generate a public key for each supported BSSID.

An AP requests the public key of a peer AP by sending a Public Key frame with the Request Type field set to “Request.” This frame contains the public key of the initiating AP.

An AP for which `dot11ProtectedTXOPNegotiationActivated` is true or `dot11ProtectedQLoadReportActivated` is true shall reply to a Public Key frame for which the Request Type field is “Request” with a Public Key frame with the Request Type field set to “Response.” If the Group field in the public key request is a group that is supported by the responding AP, the AP replies with a public key

of the same group as the request by generating such a key pair if required. The response may be of a different group to the request if the Group field in the public key request specifies a group that is not supported by the responding AP, or it is not able to generate a key in this group.

Regardless of the value of the Request Type field, the Public Key field shall contain the public key of the AP transmitting the Public Key frame. The Group field shall contain the group identifier of the domain parameters used to construct the public key in the Public Key field.

An AP that has a private key from the same finite cyclic group as the public key from a peer AP can compute the Diffie-Hellman shared secret for an AP-to-AP peer link using scalar-op() and function F from 11.3.4:

$$k = F(\text{scalar-op}(d, Q_p)) \quad (11-2)$$

where

d is the private key of the AP that is calculating k
 Q_p is the public key of the peer AP

Entropy of the shared secret shall then be extracted using function H to produce *keyseed* using Equation (11-3).

$$\textit{keyseed} = H(\langle 0 \rangle_{32}, k) \quad (11-3)$$

The PMK shall be derived using the key derivation function (KDF) from 11.5.1.7.2 using Equation (11-4).

$$\text{PMK} = \text{KDF-256}(\textit{keyseed}, \text{“AP Peerkey Protocol”}, 0x00 \parallel \text{Max}(\text{LOCAL-MAC}, \text{PEER-MAC}) \parallel \text{Min}(\text{LOCAL-MAC}, \text{PEER-MAC})) \quad (11-4)$$

where

0x00 is a single octet with a value of zero
 LOCAL-MAC is the AP’s BSSID
 PEER-MAC is the peer AP’s BSSID

Keyseed shall be irretrievably destroyed after the PMK is generated.

To enable the use of Protected HCCA TXOP Advertisement frames, Protected HCCA TXOP Response frames, Protected QLoad Request frames, and Protected QLoad Report frames, AMPE (as defined in 13.5) is used to enable security capability selection, enable key management, and prove possession of the PMK (and implicitly the private key that corresponds to the peer’s public key). If the AMPE procedure completes successfully, Protected HCCA TXOP Advertisement frames and Protected HCCA TXOP Response frames may be used in the HCCA TXOP negotiation procedures, as defined in 10.27.3. If the AMPE procedure completes successfully, Protected QLoad Request frames and Protected QLoad Report frames may be used in the QLoad report procedures, as defined in 10.27.2.

NOTE—The PMK, as well as any key derived from it, is not authenticated in any way nor is it bound to any identity. This protocol protects an AP that cooperates in scheduling its HCCA TXOPs using Protected HCCA TXOP Advertisement frames because no other entity knows its private key and cannot forge Protected HCCA TXOP Advertisement frames. An AP that receives a Protected HCCA TXOP Advertisement frame is assured it was sent by the holder of a particular private key, and no one else, and can, therefore, establish which APs are cooperating in their HCCA TXOP scheduling. An AP that receives a Protected QLoad Report frame is assured it was sent by the holder of a particular private key, and no other STA, and can, therefore, establish which APs are correctly reporting their QoS load.

Annex B

(normative)

Protocol Implementation Conformance Statement (PICS) proforma

B.2 Abbreviations and special symbols

B.2.2 General abbreviations for Item and Support columns

Insert the following abbreviation into B.2.2 in alphabetic order:

AVT audio video transport

B.4 PICS proforma—IEEE Std 802.11-2012

B.4.3 IUT configuration

Insert item CF23 at the end of the IUT configuration table:

Item	IUT configuration	References	Status	Support
*CF23	Is RobustAVT supported?	4.3.16	(CF12):O	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>

Insert the following subclause, B.4.25, after B.4.24:

B.4.25 RobustAVT extensions

Item	Protocol capability	References	Status	Support
AVT1	Extended Capabilities element	8.4.2.29	CF23:M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
AVT2	Groupcast with Retries (GCR)	10.23.15.3.2, 10.23.15.3.3, 10.23.15.3.4, 10.23.15.3.5, 10.23.15.3.6	(CF16 and CF23 and WNM19): M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
AVT2.1	Advanced GCR	8.4.2.29, 10.23.15.3.7, 10.23.15.3.8, 9.2.1.10	(CF1 and CF23 and WNM19 and HTM4.4):M (CF23 and QB5): O	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
AVT3	Alternate EDCA transmit queues	9.2.4.2	CF23:O	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>

Item	Protocol capability	References	Status	Support
AVT4 AVT4.1 AVT4.2 AVT4.3	Stream Classification Service (SCS) SCS Request frame SCS Response frame Drop eligibility indicator (DEI)	10.26.2 8.5.19.2 8.5.19.3 10.26.2	CF23:O AVT4:M AVT4:M (CF16 and AVT4):M	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
ATV5 ATV5.1 ATV5.2 AVT5.2.1 AVT5.2.2 AVT5.2.3 AVT5.2.4 AVT5.3 AVT5.3.1 AVT5.3.2	Overlapping Basic Service Set (OBSS) Management AP Peer Key QLoad Report QLoad Report element QLoad Request frame QLoad Report frame Protected QLoad Report HCCA TXOP Update Count element HCCA TXOP Negotiation Protected HCCA TXOP Negotiation	10.27, 8.4.2.29 11.10 10.27.2 8.4.2.125 8.5.8.20 8.5.8.21 8.5.8.21 8.4.2.126 10.27.3 10.27.3	(CF1 and (QP2 or QD6) and CF23):M AVT5:O AVT5:M AVT5.2:M AVT5.2:M AVT5.2:M (AVT5.2 and AVT5.1):O (AVT5 and QP2):O AVT5.3:O (AVT5.3 and ATV5.1):O	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
AVT6	GCR for Mesh	8.4.2.29, 9.21.10, 10.23.15.3.7, 10.23.15.36	(WNM19 and HTM4.4 and CF16 and CF23 and CF2a):O	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>

Annex C

(normative)

ASN.1 encoding of the MAC and PHY MIB

Change the end of the “Dot11STAStatisticsReportEntry” of the “dot11STAStatisticsReport TABLE” in Annex C as follows:

<u>dot11STAStatisticsnonSTBCCTSFailureCount</u>	<u>Counter32,</u>
<u>dot11STAStatisticsAverageMSDUSizeVideo</u>	<u>Unsigned32,</u>
<u>dot11STAStatisticsAverageMSDUSizeVoice</u>	<u>Unsigned32,</u>
<u>dot11STAStatisticsAverageBitrateVideo</u>	<u>Unsigned32,</u>
<u>dot11STAStatisticsAverageBitrateVoice</u>	<u>Unsigned32 }</u>

Insert the following elements at the end of the “dot11STAStatisticsReport TABLE” element definitions in Annex C:

```
dot11STAStatisticsAverageMSDUSizeVideo OBJECT-TYPE
    SYNTAX Unsigned32 (0..7935)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a status variable.
        It is written by the SME when a measurement report is completed or
        by an external management entity.
        Changes from an external management entity take effect as soon as practical
        in the implementation.

        If dot11STAStatisticsMeasurementDuration is zero, this attribute indicates
        the value of the Average MSDU size for the Video Access Category returned
        from the STA in this STA Statistics Report. If
        dot11STAStatisticsMeasurementDuration indicates a nonzero value, this
        attribute indicates the difference in the referenced size over the indicated
        duration. Changes by an external management entity are ignored when
        dot11STAStatisticsMeasurementDuration is nonzero."
    DEFVAL { 1401 }
    ::= { dot11STAStatisticsReportEntry 89 }
```

```
dot11STAStatisticsAverageMSDUSizeVoice OBJECT-TYPE
    SYNTAX Unsigned32 (0.. 7935)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a status variable.
        It is written by the SME when a measurement report is completed or
        by an external management entity. Changes from an external management
        entity take effect as soon as practical in the implementation.

        If dot11STAStatisticsMeasurementDuration is zero, this attribute indicates
        the value of the Average MSDU size for the Voice Access Category returned
        from the STA in this STA Statistics Report. If
        dot11STAStatisticsMeasurementDuration indicates a nonzero value, this
        attribute indicates the difference in the referenced size over the indicated
        duration. Changes by an external management entity are ignored when
        dot11STAStatisticsMeasurementDuration is nonzero."
    DEFVAL { 365 }
    ::= { dot11STAStatisticsReportEntry 90 }
```

```
dot11STAStatisticsAverageBitrateVideo OBJECT-TYPE
    SYNTAX Unsigned32 (0..4294967295)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a status variable.
        It is written by the SME when a measurement report is completed or
```

by an external management entity.
Changes from an external management entity take effect as soon as practical in the implementation.

If dot11STAStatisticsMeasurementDuration is zero, this attribute indicates the value of the Average PHY bit rate of MPDUs transmitted and received using the Video Access Category returned from the STA in this STA Statistics Report. If dot11STAStatisticsMeasurementDuration indicates a nonzero value, this attribute indicates the difference in the referenced size over the indicated duration. Changes by an external management entity are ignored when dot11STAStatisticsMeasurementDuration is nonzero."

```
::= { dot11STAStatisticsReportEntry 91 }
```

```
dot11STAStatisticsAverageBitrateVoice OBJECT-TYPE
SYNTAX Unsigned32 (0..4294967295)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
```

"This is a status variable.
It is written by the SME when a measurement report is completed or by an external management entity.
Changes from an external management entity take effect as soon as practical in the implementation.

If dot11STAStatisticsMeasurementDuration is zero, this attribute indicates the value of the Average PHY bit rate of MPDUs transmitted and received using the Voice Access Category returned from the STA in this STA Statistics Report. If dot11STAStatisticsMeasurementDuration indicates a nonzero value, this attribute indicates the difference in the referenced size over the indicated duration. Changes by an external management entity are ignored when dot11STAStatisticsMeasurementDuration is nonzero."

```
::= { dot11STAStatisticsReportEntry 92 }
```

Change the end of the “Station Management (SMT) Attributes” in the “Major sections” part of Annex C as follows:

```
-- dot11RSMNConfigDLGroupTable ::= { dot11smt 26 }
-- dot11AVOptionsTable ::= { dot11smt 28 }
-- dot11AVConfigTable ::= { dot11smt 29 }
-- dot11APCTable ::= { dot11smt 30 }
```

Change the end of the “Dot11StationConfigEntry” of the “dot11StationConfig TABLE” in Annex C as follows:

```
dot11QMFPolicyChangeTimeout Unsigned32,
dot11RobustAVStreamingImplemented TruthValue
}
```

Insert the following element at the end of the “dot11StationConfig TABLE” element definitions in Annex C:

```
dot11RobustAVStreamingImplemented 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 the station
    implementation supports robust AV streaming."
DEFVAL { false }
::= { dot11StationConfigEntry 140 }
```

Insert the following tables (“dot11AVOptions TABLE,” “dot11AVConfig TABLE,” and “dot11APC TABLE”) after the “dot11RSNAConfigDLGroup TABLE” in Annex C:

```
-- *****
-- * dot11AVOptions TABLE
-- *****

dot11AVOptionsTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Dot11AVOptionsEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "AV streaming attributes. In tabular form to allow for multiple instances on
        an agent. This table applies to the interface only if
        dot11RobustAVStreamingImplemented is true in the dot11StationConfigTable.
        Otherwise this table should be ignored."
    ::= { dot11smt 28 }

dot11AVOptionsEntry OBJECT-TYPE
    SYNTAX Dot11AVOptionsEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry in the dot11AVOptionsTable. For all AV Streaming features, an
        Activated MIB variable is used to activate/enable or deactivate/disable the
        corresponding feature. An Implemented MIB variable is used for an optional
        feature to indicate whether the feature is implemented. A mandatory feature
        does not have a corresponding Implemented MIB variable. It is possible for
        there to be multiple IEEE 802.11 interfaces on one agent, each with its
        unique MAC address. The relationship between an IEEE 802.11 interface and an
        interface in the context of the Internet-standard MIB is one-to-one. As
        such, the value of an ifIndex object instance can be directly used to
        identify corresponding instances of the objects defined herein.

        ifIndex - Each IEEE 802.11 interface is represented by an ifEntry. Interface
        tables in this MIB module are indexed by ifIndex."
    INDEX { ifIndex }
    ::= { dot11AVOptionsTable 1 }

Dot11AVOptionsEntry ::=
    SEQUENCE {
        dot11GCRActivated TruthValue,
        dot11AdvancedGCRImplemented TruthValue,
        dot11AdvancedGCRActivated TruthValue,
        dot11SCSImplemented TruthValue,
        dot11SCSActivated TruthValue,
        dot11QLoadReportActivated TruthValue,
        dot11AlternateEDCAActivated TruthValue,
        dot11GCRGroupMembershipAnnouncementActivated TruthValue,
        dot11PublicHCCATXOPNegotiationImplemented TruthValue,
        dot11PublicHCCATXOPNegotiationActivated TruthValue,
        dot11ProtectedHCCATXOPNegotiationImplemented TruthValue,
        dot11ProtectedHCCATXOPNegotiationActivated TruthValue,
        dot11ProtectedQLoadReportImplemented TruthValue,
        dot11ProtectedQLoadReportActivated TruthValue,
        dot11MeshGCRImplemented TruthValue,
        dot11MeshGCRActivated TruthValue }

dot11GCRActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive
        or MLME-JOIN.request primitive.

        This attribute, when true, indicates that the station
        implementation supports the GCR procedures as defined in 10.23.15.3 and that
        this has been activated."
```

```
DEFVAL { false }
 ::= { dot11AVOptionsEntry 1 }

dot11AdvancedGCRImplemented 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 the station implementation
    supports the Advanced GCR features."
DEFVAL { false }
 ::= { dot11AVOptionsEntry 2 }

dot11AdvancedGCRActivated OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by the SME or external management entity.
    Changes take effect for the next MLME-START.request primitive
    or MLME-JOIN.request primitive.

    This attribute, when true, indicates that the station implementation
    supports the GCR procedures as defined in 10.23.15.3 and that this has been
    activated."
DEFVAL { false }
 ::= { dot11AVOptionsEntry 3 }

dot11SCSImplemented 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 the station implementation
    supports the stream classification service."

DEFVAL { false }
 ::= { dot11AVOptionsEntry 4 }

dot11SCSActivated OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by the SME or external management entity.
    Changes take effect for the next MLME-START.request primitive
    or MLME-JOIN.request primitive.

    This attribute, when true, indicates that the station implementation
    supports the stream classification service and that this has been
    activated."
DEFVAL { false }
 ::= { dot11AVOptionsEntry 5 }

dot11QLoadReportActivated OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by the SME or external management entity.
    Changes take effect for the next MLME-START.request primitive.
```

```

        This attribute, when true, indicates that the AP performs the QLoad report
        procedures described in 10.27.2."
    DEFVAL { false }
    ::= { dot11AVOptionsEntry 6 }

dot11AlternateEDCAActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive.

        This attribute, when true, indicates that the station can additionally use
        the Alternate EDCA transmit queues."
    DEFVAL { false }
    ::= { dot11AVOptionsEntry 7 }

dot11GCRCGroupMembershipAnnouncementActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect as soon as practical in the implementation.

        This attribute, when true, indicates that the STA sends unsolicited Group
        Membership Response frames when its dot11GroupAddressesTable changes."
    DEFVAL { false }
    ::= { dot11AVOptionsEntry 8 }

dot11PublicHCCATXOPNegotiationImplemented 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 the station implementation
        supports the negotiation of HCCA TXOPs using public action frames."
    DEFVAL { true }
    ::= { dot11AVOptionsEntry 9 }

dot11PublicHCCATXOPNegotiationActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive.

        This attribute, when true, indicates that the AP can negotiate HCCA TXOPs
        using public action frames."
    DEFVAL { true }
    ::= { dot11AVOptionsEntry 10 }

dot11ProtectedHCCATXOPNegotiationImplemented 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 the station implementation
        supports the negotiation of HCCA TXOPs using protected dual of public action
        frames."
    DEFVAL { true }

```

```
 ::= { dot11AVOptionsEntry 11 }

dot11ProtectedHCCATXOPNegotiationActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive.

        This attribute, when true, indicates that the AP can negotiate HCCA TXOPs
        using protected dual of public action frames."
    DEFVAL { true }
    ::= { dot11AVOptionsEntry 12 }

dot11ProtectedQLoadReportImplemented 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 the station implementation
        supports the reporting of QLoad using protected dual of public action
        frames."
    DEFVAL { true }
    ::= { dot11AVOptionsEntry 13 }

dot11ProtectedQLoadReportActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive.

        This attribute, when true, indicates that the AP can report QLoad using
        protected dual of public action frames."
    DEFVAL { true }
    ::= { dot11AVOptionsEntry 14 }

dot11MeshGCRImplemented 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 the mesh station
        implementation supports the Advanced GCR features."
    DEFVAL { false }
    ::= { dot11AVOptionsEntry 15 }

dot11MeshGCRActivated OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive
        or MLME-JOIN.request primitive.

        This attribute, when true, indicates that the mesh station
        implementation supports the GCR procedures as defined in 10.23.15.3 and
        that this has been activated."
    DEFVAL { false }
    ::= { dot11AVOptionsEntry 16 }
```



```

-- *****
-- * End of dot11AVOptions TABLE
-- *****

-- *****
-- * dot11AVConfig TABLE
-- *****

dot11AVConfigTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Dot11AVConfigEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "AV streaming attributes. In tabular form to allow for multiple instances on
        an agent. This table only applies to the interface if
        dot11RobustAVStreamingImplemented is true in the dot11StationConfigTable.
        Otherwise this table should be ignored."
    ::= { dot11smt 29 }

dot11AVConfigEntry OBJECT-TYPE
    SYNTAX Dot11AVConfigEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry in the dot11AVConfigTable. It is possible for there to be multiple
        IEEE 802.11 interfaces on one agent, each with its unique MAC address. The
        relationship between an IEEE 802.11 interface and an interface in the
        context of the Internet-standard MIB is one-to-one. As such, the value of an
        ifIndex object instance can be directly used to identify corresponding
        instances of the objects defined herein.

        ifIndex - Each IEEE 802.11 interface is represented by an ifEntry. Interface
        tables in this MIB module are indexed by ifIndex."
    INDEX { ifIndex }
    ::= { dot11AVConfigTable 1 }

Dot11AVConfigEntry ::=
SEQUENCE {
    dot11GCRPolicyChangeTimeout                Unsigned32,
    dot11QLoadReportIntervalDTIM              Unsigned32,
    dot11HCCATXOPBeaconTimeout                Unsigned32,
    dot11GCRConcealmentAddress                MacAddress,
    dot11QLoadReportDelay                     Unsigned32,
    dot11ShortDEIRetryLimit                   Unsigned32,
    dot11LongDEIRetryLimit                    Unsigned32,
    dot11UnsolicitedRetryLimit                Unsigned32,
    dot11DefaultSurplusBandwidthAllowance     Unsigned32 }

dot11GCRPolicyChangeTimeout OBJECT-TYPE
    SYNTAX Unsigned32(5..18000)
    UNITS "100 TUs"
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by the SME or external management entity.
        Changes take effect for the next MLME-START.request primitive or
        MLME-JOIN.request primitive.

        This attribute indicates the interval after which a STA updates its
        GCR delivery mode or retransmission policy state using the procedures
        defined in 10.23.15.3.4."
    DEFVAL { 100 }
    ::= { dot11AVConfigEntry 1 }

dot11QLoadReportIntervalDTIM OBJECT-TYPE
    SYNTAX Unsigned32 (1..255)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.

```

It is written by an external management entity.
Changes take effect at the next MLMESTART.request primitive.

This attribute describes the number of DTIM intervals between transmissions of Beacon frames containing a Qload Report element."
 ::= { dot11AVConfigEntry 2 }

dot11HCCATXOPBeaconTimeout OBJECT-TYPE

SYNTAX Unsigned32 (1..100)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the MAC or external management entity.

Changes take effect for the next MLME-START.request primitive.

This attribute specifies the number of beacon periods an AP defers scheduling new potentially conflicting HCCA TXOPs while performing the HCCA TXOP procedures defined in 10.27.3."

DEFVAL { 3 }

::= { dot11AVConfigEntry 3 }

dot11GCRCConcealmentAddress OBJECT-TYPE

SYNTAX MacAddress

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME or external management entity.

In a non-AP STA or mesh STA receiving GCR service, it is written by the MAC when it receives a DMS Response that contains a DMS Status field with a GCR Response subelement and a Response Type subfield set to Accept.

In an AP or mesh STA providing GCR service, changes take effect for the next MLME-START.request primitive.

In a non-AP STA or mesh STA receiving GCR service, changes take effect as soon as practical in the implementation.

The purpose of dot11GCRCConcealmentAddress is to define the group address that is used by the GCR procedures (as defined in 10.23.15.3.5) to conceal group addressed frames from STAs that do not support GCR."

DEFVAL {'010FAC474352'H}

::= { dot11AVConfigEntry 4 }

dot11QLoadReportDelay OBJECT-TYPE

SYNTAX Unsigned32 (1..60)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect at the next MLMESTART.request primitive.

This attribute describes the maximum number of seconds an AP delays sending an unsolicited QLoad Report action frame."

DEFVAL { 10 }

::= { dot11AVConfigEntry 5 }

dot11ShortDEIRetryLimit OBJECT-TYPE

SYNTAX Unsigned32 (1..255)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

For frames where the DEI subfield has the value of one and length less than or equal to dot11RTSThreshold, this attribute indicates the maximum number of transmission attempts that are made before a failure condition is indicated. The default value of this attribute is 5."

DEFVAL { 5 }

::= { dot11AVConfigEntry 6 }

```

dot11LongDEIRetryLimit OBJECT-TYPE
    SYNTAX Unsigned32 (1..255)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        " This is a control variable.
        It is written by an external management entity.
        Changes take effect as soon as practical in the implementation.

        For frames where the DEI subfield has the value of one and length greater
        than dot11RTSThreshold, this attribute indicates the maximum number of
        transmission attempts that are made before a failure condition is indicated.
        The default value of this attribute is 3."
    DEFVAL { 3 }
    ::= { dot11AVConfigEntry 7 }

dot11UnsolicitedRetryLimit OBJECT-TYPE
    SYNTAX Unsigned32 (1..255)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by an external management entity.
        Changes take effect as soon as practical in the implementation.

        This attribute indicates the maximum number of transmission attempts of a
        frame delivered using the GCR unsolicited retry retransmission policy."
    DEFVAL { 7 }
    ::= { dot11AVConfigEntry 8 }

dot11DefaultSurplusBandwidthAllowance OBJECT-TYPE
    SYNTAX Unsigned32 (100..255)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        " This is a control variable.
        It is written by an external management entity.
        Changes take effect as soon as practical in the implementation.

        This object specifies the default percentage surplus bandwidth allowance
        when calculating medium time.
        "
    DEFVAL { 110 }
    ::= { dot11AVConfigEntry 9 }

-- *****
-- * End of dot11AVConfig TABLE
-- *****

-- *****
-- * dot11APC TABLE
-- *****

dot11APCTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Dot11APCEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Group contains conceptual table of attributes for MIB-based HCCA TXOP
        negotiation."
    ::= { dot11smt 30 }

dot11APCTableEntry OBJECT-TYPE
    SYNTAX Dot11APCEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry in the dot11APCTable, Indexed by dot11APCIndex."
    INDEX { dot11APCIndex }
    ::= { dot11APCTable 1 }

```

```
Dot11APCEnter ::=
SEQUENCE {
    dot11APCIndex                               Unsigned32,
    dot11APCEnterAvoidanceDuration             Unsigned32,
    dot11APCEnterAvoidanceServiceInterval     Unsigned32,
    dot11APCEnterAvoidanceOffset             Unsigned32,
    dot11APCEnterMACAddress                   MacAddress }

dot11APCIndex OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "The auxiliary variable used to identify instances of the columnar objects
    in the HCCA TXOP Table."
 ::= { dot11APCTableEntry 1 }

dot11APCEnterAvoidanceDuration OBJECT-TYPE
SYNTAX Unsigned32 (0..131071)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME.
    Changes take effect as soon as practical in the implementation.

    This attribute contains the duration, in increments of 32 us, of a TXOP
    reservation that the AP attempts to avoid when scheduling new HCCA TXOPs."
 ::= { dot11APCTableEntry 2 }

dot11APCEnterAvoidanceServiceInterval OBJECT-TYPE
SYNTAX Unsigned32 (0..255)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME.
    Changes take effect as soon as practical in the implementation.

    This attribute contains the duration, in ms, of the period between
    successive HCCA TXOPs. When zero, no period has been reserved."
 ::= { dot11APCTableEntry 3 }

dot11APCEnterAvoidanceOffset OBJECT-TYPE
SYNTAX Unsigned32 (0..131071)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME.
    Changes take effect as soon as practical in the implementation.

    This attribute contains the offset, in TUs, from the scheduled start of the
    Beacon transmission until the start of the time period for a TXOP
    reservation that the AP attempts to avoid when scheduling new HCCA TXOPs."
 ::= { dot11APCTableEntry 4 }

dot11APCEnterMACAddress OBJECT-TYPE
SYNTAX MacAddress
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "This is a control variable.
    It is written by an external management entity or the SME.
    Changes take effect as soon as practical in the implementation.

    This attribute contains the MAC address of the peer AP that has scheduled an
    HCCA TXOP in the time period defined by dot11APCEnterAvoidanceDuration,
    dot11APCEnterAvoidanceServiceInterval, and dot11APCEnterAvoidanceOffset."
 ::= { dot11APCTableEntry 5 }

-- *****
```

```
-- * End of dot11APC TABLE
-- *****
```

Insert the following elements (“dot11AVSBase” and “dot11AVSAPCGroup”) into the “Groups - units of conformance” section after “dot11PasswordAuthComplianceGroup” (dot11Groups 62) in Annex C:

```
-- *****
-- * Groups - units of conformance - AVS
-- *****
```

```
dot11AVSBase OBJECT-GROUP
  OBJECTS {
    dot11RobustAVStreamingImplemented,
    dot11GCRActivated,
    dot11AdvancedGCRImplemented,
    dot11AdvancedGCRActivated,
    dot11SCSImplemented,
    dot11SCSActivated,
    dot11QLoadReportActivated,
    dot11AlternateEDCAActivated,
    dot11PublicHCCATXOPNegotiationActivated,
    dot11GCRGroupMembershipAnnouncementActivated,
    dot11MeshGCRImplemented,
    dot11MeshGCRActivated,
    dot11PublicHCCATXOPNegotiationImplemented,
    dot11PublicHCCATXOPNegotiationActivated,
    dot11ProtectedHCCATXOPNegotiationImplemented,
    dot11ProtectedHCCATXOPNegotiationActivated,
    dot11ProtectedQLoadReportImplemented,
    dot11ProtectedQLoadReportActivated,
    dot11QLoadReportIntervalDTIM,
    dot11HCCATXOPBeaconTimeout,
    dot11GCRConcealmentAddress,
    dot11GCRPolicyChangeTimeout,
    dot11QLoadReportDelay,
    dot11DefaultSurplusBandwidthAllowance,
    dot11ShortDEIRetryLimit,
    dot11LongDEIRetryLimit,
    dot11UnsolicitedRetryLimit,
    dot11STAStatisticsAverageMSDUSizeVideo,
    dot11STAStatisticsAverageMSDUSizeVoice,
    dot11STAStatisticsAverageBitrateVideo,
    dot11STAStatisticsAverageBitrateVoice
  }
  STATUS current
  DESCRIPTION
    "The AVSBase package is a set of attributes that are present if the STA
    supports the robust audio video streaming features."
  ::= { dot11Groups 68 }

dot11AVSAPCGroup OBJECT-GROUP
  OBJECTS {
    dot11APCEntryAvoidanceDuration,
    dot11APCEntryAvoidanceServiceInterval,
    dot11APCEntryAvoidanceOffset,
    dot11APCEntryMACAddress
  }
  STATUS current
  DESCRIPTION
    "The AVSAPCGroup package is a set of attributes that are present if the STA
    supports HCCA TXOP negotiation."
  ::= { dot11Groups 69 }
```

Insert the following compliance statement (“Compliance Statements – AVS”) after the “Compliance Statements - WNM” section in Annex C:

```
-- *****
```

```
-- * Compliance Statements - AVS
-- *****

dot11AVSCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
    "The compliance statement for SNMPv2 entities that implement the IEEE
    802.11 Robust Audio/Video Streaming feature.
    Note that additional objects for managing this functionality are located in
    the IEEE 802.11 AVS MIB."
  MODULE -- this module
  GROUP dot11AVSBase
  DESCRIPTION "At least the dot11RobustAVStreamingImplemented object is
    required from dot11StationConfigEntry."
  OBJECT dot11RobustAVStreamingImplemented
  DESCRIPTION "Required object"
  ::= { dot11Compliances 7 }

dot11AVSAPCCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
    "The compliance statement for SNMPv2 entities that implement the IEEE
    802.11 HCCA TXOP Negotiation feature.
    Note that additional objects for managing this
    functionality are located in the IEEE 802.11 AVS MIB."
  MODULE -- this module
  MANDATORY-GROUPS { dot11AVSBase }
  GROUP dot11AVSAPCGroup
  DESCRIPTION "At least the dot11RobustAVStreamingImplemented object is
    required from dot11StationConfigEntry."
  OBJECT dot11RobustAVStreamingImplemented
  DESCRIPTION "Required object"
  ::= { dot11Compliances 8 }
```

Insert the following text, Annex X, after Annex W:

Annex X

(informative)

Overlapping BSS (OBSS) management

X.1 Introduction

When two or more BSSs overlap, the available bandwidth is shared and hence reduced for each BSS. The basic access mechanism, such as DCF, is able to work across OBSSs. Similarly, if EDCA is used, the OBSS might be considered a larger network, and access to the WM is basically shared according to the EDCA access mechanism. Note that for both DCF and EDCA overlapping networks, the sharing is affected by the relative traffic; and if more than two APs are sharing, the problem of “neighbor capture” might occur. The neighbor capture effect might occur when a BSS is in the middle of two other BSSs that are hidden from each other, where it might suffer a disproportionate degradation in throughput, relative to the total traffic in all three BSSs. A particular problem arises when there is some expectation of QoS. If EDCA admission control is in use, then it can be used to regulate the QoS traffic on its own BSS, but it might not take into account the EDCA admitted traffic on an OBSS. The result is that the QoS is compromised if each BSS admits traffic up to its local maximum. Similarly a BSS using HCCA might schedule traffic in its own BSS, to “guarantee” a service, but, if not controlled, this might suppress overlapping EDCA admission control BSS. Furthermore, if two HCCA BSSs overlap and they do not coordinate their scheduled TXOPs, then a degradation of QoS might result. The features described in this annex have been introduced in order to allow a degree of management for OBSSs and for mitigation of the basic problems outlined above.

X.2 QLoad Report element

X.2.1 General

The fields and their uses in the QLoad Report element are as follows:

- Potential Traffic Self field value represents the potential QoS traffic load that this AP is expecting and is provided as an indication to other APs that might be considering selecting the same channel and for sharing when an OBSS situation occurs. The Potential Traffic Self field also includes the peak number of AC_VO and AC_VI EDCA streams.
- Allocated Traffic Self field value represents the total QoS traffic and the numbers of AC_VI and AC_VO streams that are active at that time. This field is provided to enable an on-demand sharing scheme. It might be used by the other APs in OBSSs to determine if the AP has either over-allocated in a proportional sharing scheme or is using an on-demand sharing scheme.
- Allocated Traffic Shared field contains the sum of the Allocated Traffic Self field values for OBSSs and is used to protect an AP from the neighbor capture effect where an AP that has neighbors that are hidden from each other. It indicates to other APs in OBSSs if this AP has either over-allocated in a proportional sharing scheme, or might be using an on-demand sharing scheme.
- EDCA Access Factor field value represents the total QoS traffic bandwidth requirement for all the APs in OBSSs and is used to indicate potential over-allocation. It also enables a proportional sharing scheme. The Potential Traffic Self fields from QLoad Report elements of nearby co-channel APs are used for estimating the overhead bandwidth required due to EDCA contention and is used in the determination of the EDCA Access Factor.

- HCCA Peak field value represents the total peak HCCA TXOP requirement for the BSS and is provided so that other overlapping APs can determine whether the AP has over-allocated.
- HCCA Access Factor field contains the sum of all the HCCA Peak field values in all the QLoad Reports of all the overlapping APs, including its own. This value is used when HCCA APs are sharing as defined in 10.27.2.
- Overlap field value is the number of other APs that are on the same channel and from which Beacon frames are being regularly received. It might be used to aid the channel selection process.

X.2.2 Calculating medium time

This annex uses the function defined in Equation (X-1) for calculating and estimating medium times in both ACM and non-ACM QoS modes:

$$\text{mediumTime}(s,d,m,p) = s \times pps \times \text{MPDUEXchangeTime} \quad (\text{X-1})$$

where

$$pps = \text{ceiling}((d / 8) / m) \quad (\text{X-2})$$

$$\text{MPDUEXchangeTime} = \text{duration}(m,p) + \text{SIFS} + \text{duration}(14,p) \quad (\text{X-3})$$

`duration()` is the PLME-TXTIME primitive that returns the duration of a frame based on its payload size and the PHY data rate employed.

s , d , m and p are parameters that are passed in to the `mediumTime` function

(Also see the definition of `MPDUEXchangeTime` in 9.19.4.2.3.)

X.2.3 Calculation of potential traffic self

The Potential Traffic Self field value represents the sum of all the streams derived from all the potential EDCA admission control and HCCA QoS traffic. The individual TSPEC elements provided by the non-AP STAs are used by the AP to calculate mean, maximum, and minimum values for

- Medium time, in multiples of 32 μs per second, in the case of EDCA admission control
- HCCA medium time, in the case of HCCA; where HCCA medium time is the TXOP time scheduled by the HC converted to multiples of 32 μs over a 1 s period, by dividing the scheduled TXOP time by the SI that the HC has allocated

The AP maintains a $\langle \text{mean, standard deviation, AC_VO, AC_VI} \rangle$ tuple that contains the maximum values from Allocated Traffic Self field. The values of this tuple are calculated using

- a) The mean and standard deviation from the Allocated Traffic Self field that had the largest value of the Mean subfield
- b) The AC_VO Streams subfield from the Allocated Traffic Self field that had the largest value
- c) The AC_VI Streams subfield from the Allocated Traffic Self field that had the largest value

This $\langle \text{mean, standard deviation, AC_VO, AC_VI} \rangle$ tuple is calculated over fixed, consecutive seven-day periods and is reset at the start of each new period. If, at any time, any of the maximum values in the tuple are greater than those in the corresponding subfields of the Potential Traffic Self field, then those fields in the Potential Traffic Self field are set to the value(s) in the tuple. If the AP refuses an ADDTS request due to a perceived over-allocation (for example, step b) 4) in the proportional sharing scheme described in X.4.2.2), then the AP adds the TSPEC values of the rejected request to the tuple.

At the end of each seven-day period, if any of the maximum values in the tuple are less than those in the corresponding subfields of the Potential Traffic Self field, then those subfields in the Potential Traffic Self fields are set to the value(s) in the tuple.

NOTE—It is not required that the start and end of the seven-day periods be synchronized across OBSSs. After the first seven-day period, each AP advertises its correct potential load irrespective of its start time.

TSPECs provide for mean, maximum, and minimum bit rate values, which allow for statistical multiplexing of streams. The result of summing multiple streams is a composite stream, which is recommended to be reported in the Potential Traffic Self field. The summing of streams to produce a composite stream is achieved by using the mean and standard deviation of each stream.

It is recommended that the mean (MEAN), maximum (MAX), and minimum (MIN) values of the medium time or HCCA medium time be calculated using the values provided in the individual TSPECs, as follows:

For a TSPEC for stream, i , the mean value, μ , is:

$$MIN_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Minimum Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-4})$$

$$MEAN_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Mean Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-5})$$

$$MAX_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Peak Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-6})$$

$$\mu_i = MEAN_i \quad (\text{X-7})$$

If the Minimum Data Rate and Peak Data Rate fields were provided in the TSPEC element, σ is:

$$\sigma_i = 0.25(MAX_i - MIN_i) \quad (\text{X-8})$$

Else if the Peak Data Rate field was provided in the TSPEC element, σ is:

$$\sigma_i = \frac{MAX_i - MIN_i}{2} \quad (\text{X-9})$$

Otherwise:

$$\sigma_i = 0 \quad (\text{X-10})$$

When the non-AP STA does not have any active TSPECs, it is recommended that the AP monitor the mean and maximum frame reception and transmission rates for AC_VI and AC_VO (for example, by regular sampling of changes to dot11QosMPDUsReceivedCount and dot11QosTransmittedFrameCount of each AC) to calculate the potential load information as follows:

For a QoS traffic capability, the mean value, μ , is:

$$\mu_0 = \text{mediumTime}(\text{dot11DefaultSurplusBandwidthAllowance}/100, \text{dot11STAStatisticsAverageMSDUSizeVideo}, \text{MAXt[VI]}, \text{dot11STAStatisticsAverageBitrateVideo}) \quad (\text{X-11})$$

$$\mu_I = \text{mediumTime}(\text{dot11DefaultSurplusBandwidthAllowance}/100, \text{dot11STAStatisticsAverageMSDUSizeVoice}, \text{MAXt[VO]}, \text{dot11STAStatisticsAverageBitrateVoice}) \quad (\text{X-12})$$

and the standard deviation, σ , is:

$$\sigma_0 = 0 \quad (\text{X-13})$$

$$\sigma_1 = 0 \quad (\text{X-14})$$

The values reported in the Potential Traffic Self field represent the composite stream of all the individual streams of all associated STAs, and it is recommended that this composite stream be calculated as follows:

Potential traffic self mean is:

$$\mu_{tot} = \sum \mu_i \quad (\text{X-15})$$

Potential traffic self standard deviation:

$$\sigma_{tot} = \sqrt{\sum \sigma_i^2} \quad (\text{X-16})$$

X.2.4 Calculation of allocated traffic self

The Allocated Traffic Self field value represents the total BSS load of all streams that the AP has allocated at any one time and the number of AC_VI and AC_VO streams that make up that total. It is recommended that the AP calculate the mean and standard deviation using the Minimum Data Rate, Mean Data Rate, and Peak Data Rate fields of admitted TSPECs and to recalculate the Allocated Traffic Self field value as each TS is added or deleted. It is recommended that the values of the Mean and Standard Deviation subfields placed in the Allocated Traffic Self field for i allocated streams be calculated using Equation (X-17) to Equation (X-24).

$$MIN_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Minimum Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-17})$$

$$MEAN_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Mean Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-18})$$

$$MAX_i = \text{mediumTime}(\text{Surplus Bandwidth Allowance}, \text{Nominal MSDU Size}, \text{Peak Data Rate}, \text{Minimum PHY Rate}) \quad (\text{X-19})$$

If TSPEC _{i} has the Minimum Data Rate and Peak Data Rate fields populated, σ is:

$$\sigma_i = 0.25(MAX_i - MIN_i) \quad (\text{X-20})$$

Else if TSPEC _{i} has the Mean Data Rate and Peak Data Rate fields populated, σ is:

$$\sigma_i = \frac{MAX_i - MEAN_i}{2} \quad (\text{X-21})$$

Otherwise:

$$\sigma_i = 0 \quad (\text{X-22})$$

$$\text{Mean} = \sum \mu_i \quad (\text{X-23})$$

$$\text{Standard deviation} = \sqrt{\sum \sigma_i^2} \quad (\text{X-24})$$

When admission control is not used, it is recommended that the AP monitor the mean and maximum frame reception and transmission rates for AC_VI and AC_VO (for example, by regular sampling of changes to dot11QosMPDUsReceivedCount and dot11QosTransmittedFrameCount of each AC). The MAX, MEAN, and standard deviation (STDEV) at time t for access category AC are as given in Equation (X-25), Equation (X-26), and Equation (X-27).

$$MEAN_t = o (\text{duration}(s, b) + \text{SIFS} + \text{duration}(14, b)) p_t \quad (\text{X-25})$$

MAX_t is the maximum value of $MEAN_t$ since MLME-START.confirm

$$STDEV_t = \frac{MAX_t - MEAN_t}{2} \quad (\text{X-26})$$

where

$$p_t = \frac{d}{dt} (\text{dot11QosMPDUsReceivedCount}[AC] + \text{dot11QosTransmittedFrameCount}[AC] - \text{dot11QosFrameDuplicateCount}[AC]) \quad (\text{X-27})$$

$o = \text{dot11DefaultSurplusBandwidthAllowance}$

$s = \text{dot11STAStatisticsAverageMSDUSizeVideo}$

$b = \text{dot11STAStatisticsAverageBitrateVideo}$

$\text{duration}()$ is the PLME-TXTIME primitive that returns the duration of a packet based on its payload size and the PHY data rate employed

NOTE—The differentiation above calculates the frames per second for the given AC.

X.2.5 Calculation of allocated traffic shared

The Allocated Traffic Shared field value is the sum of the values expressed in the Allocated Traffic Self fields of all APs in OBSSs, including in its own Allocated Traffic Self field. It is recommended that the values of the mean μ and standard deviation σ , placed in the Allocated Traffic Shared field, for n OBSSs be calculated using Equation (X-28) and Equation (X-29).

$$\mu = \sum \mu_n \quad (\text{X-28})$$

$$\sigma = \sqrt{\sum \sigma_n^2} \quad (\text{X-29})$$

X.2.6 Calculation of EDCA Access Factor

The EDCA Access Factor is the total traffic requirement for all the OBSSs. The value of EDCA Access Factor might be greater than 1. It is recommended that the EDCA Access Factor be calculated from the addition of all the Potential Traffic Self fields of the APs that are overlapping as follows:

First calculate the overlap traffic for all the APs in OBSSs. Each AP notes the reported Potential Traffic Self fields for every OBSS, including the AP's own Potential Traffic Self field, and calculates the maximum traffic of the composite stream, using Equation (X-30), Equation (X-31), and Equation (X-32).

$$\text{Overlap traffic} = \mu_{tot} + 2 \sigma_{tot} \quad (\text{X-30})$$

where, for i Potential Traffic Self fields

$$\mu_{tot} = \sum \mu_i \quad (\text{X-31})$$

$$\sigma_{tot} = \sqrt{\sum \sigma_i^2} \quad (\text{X-32})$$

This overlap traffic value is in multiples of 32 μ s per second.

The following procedure is then recommended to calculate the EDCA Access Factor:

- a) Sum the AC_VI and AC_VO priority streams reported in the Potential Traffic Self fields of its own QLoad report and all the QLoad reports of APs in OBSSs, and determine the EDCA Overhead Factor as recommended in X.2.7.
- b) Multiply the overlap traffic and the resulting EDCA Overhead Factor together. This value represents the total overlap traffic requirement for the OBSSs in multiples of 32 μ s per second.
- c) Convert the total overlap traffic to a fraction (seconds per second) by multiplying by 32×10^{-6} .
- d) Round the resulting fraction value rounded down to a multiple of 1/64.

For example, if the total overlap traffic is 74 268 (32 μ s/s), this is 2.376576 (seconds/second). Now $2.376576 \times 64 = 152.1$ rounded to 152. Hence, the EDCA Access Factor octet, in this case, would be 1001100 (152 in binary, representing the fraction 152/64).

X.2.7 EDCA Overhead Factor

The Potential Traffic Self field also includes the number of AC_VI and AC_VO streams that make up the composite stream. The recommended calculation for medium time for an admitted EDCA is given in L.2.2. This value includes the duration of the packet plus SIFS and ACK times. The medium time, therefore, does not include the access time. For example, for a single stream, between each transmitted packet, there is a time period due to SIFS, AIFSN, and contention window, and for two or more streams, there is also the time when each packet is delayed while another packet is being transmitted. Hence, in order to calculate the total time or bandwidth required to service multiple EDCA streams, an overhead is present.

It is recommended that a fixed value of 1.34 be used for EDCA Overhead Factor. The value of the EDCA Overhead Factor is dependent upon many factors, including

- Number and mix of streams, voice and video
- Mixture of PHY rates and PHYs
- Mixture of streams' data rates
- Use and mix of aggregated MSDUs
- Choice of EDCA parameters including different settings in OBSSs

Based on a range of simulations, the value of EDCA Overhead Factor is normally in the range 1.26 to 1.43. These simulations, however, were not exhaustive and did not include the effects of hidden nodes and non-IEEE-802.11 interference.

X.2.8 Calculation of HCCA Access Factor

It is recommended that the HCCA Access Factor be calculated as follows:

- a) Sum the HCCA Peak field values in all the QLoad reports of all the APs in OBSSs, including its own.
- b) Convert the total peak traffic to a fraction (seconds per second) by multiplying by 32×10^{-6} .
- c) Round the resulting fraction value to the nearest 1/64 and enter the result into the HCCA Access Factor field.

For example, if the total overlap traffic is 74 268 (32 μ s/s), this is 2.376576 (seconds/second). Now $2.376576 \times 64 = 152.1$ rounded to 152. Hence, the HCCA Access Factor octet, in this case, would be 152 (representing the fraction 152/64).

X.3 Channel selection using QLoad report

X.3.1 General

In addition to the channel selection described below, it is advised that other factors such as traffic from IBSSs, energy from non-IEEE-802.11 systems, and device constraints on the AP or STAs anticipated within the BSS be considered, and regulatory constraints need to be complied with.

The most effective mitigation to OBSS is for an AP to operate on channels that are free or that are occupied by another AP that is not fully loaded with QoS traffic. In the absence of a centralized channel assignment algorithm, it is recommended that the Overlap and Potential Traffic Self fields of the QLoad Report element be used by an AP as part of its channel selection procedure. An AP might use the Overlap field and Potential Traffic Self field information when deciding the best channel to select. If there are sufficient channels for an AP to find a channel with no other APs within range, then an AP is advised to select one of them.

It is recommended that when selecting a channel, the AP scan to see whether there is a free channel taking account of BSS channel width and channel spacing. If a free channel is not available, then it is advised to select channels that have the least number of QoS APs present. There might be more than one channel with the same number of QoS APs present. At this point, the AP is advised to select, in turn, the candidate channels and send a QLoad Request frame to each AP on that channel. The AP is advised to examine the Overlap and Potential Traffic Self fields of the QLoad Report element to make its final selection.

X.3.2 AP with admission control mandatory

If no “empty” channels are available, then an AP with the ACM (admission control mandatory) bit in the EDCA Parameter Set element set for AC_VI or AC_VO is recommended to implement a channel selection procedure to share with one or more APs, in the following preference order:

- a) Non-QoS AP where the EDCA Parameter Set element is not present in the Beacon frame
- b) QoS AP with the ACM bit set for AC_VI or AC_VO and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element)
- c) QoS AP with an HC and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element)
- d) QoS AP with an HC and with no indication of support for QLoad reporting
- e) QoS AP with the ACM bit set for AC_VI or AC_VO and with no indication of support for QLoad reporting

- f) QoS AP where the EDCA Parameter Set element is present in the Beacon frame and the ACM bit is not set for AC_VI or AC_VO

X.3.3 AP with an HC

If no “empty” channels are available, then an AP with an HC is recommended to implement a channel selection procedure to share with one or more APs, in the following preference order:

- a) Non-QoS AP where the EDCA Parameter Set element is not present in the Beacon frame
- b) QoS AP where the EDCA Parameter Set element is present in the Beacon frame and the ACM bit is not set for AC_VI or AC_VO
- c) QoS AP with the ACM bit set for AC_VI or AC_VO and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element)
- d) QoS AP with an HC and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element)
- e) QoS AP with the ACM bit set for AC_VI or AC_VO and with no indication of support for QLoad reporting
- f) QoS AP with an HC and with no indication of support for QLoad reporting

X.3.4 Channel selection procedures

The recommended method for channel selection can be implemented by adoption of the following procedures:

- a) Create a list of the available channels. Typically this is the list of channels allowed by regulation in the operating regulatory domain; however, this list might be modified by management policy (e.g., removing overlapping channels, avoiding radar detect channels).
- b) Create an array for each available channel that allows the recording of the QoS AP count, ACM bit count, HC count, overlap count, and potential load for that channel.
- c) Step through the list of available channels, listening for beacons for at least $\text{dot11OBSSScanPassiveTotalPerChannel}$ TUs per channel.
- d) Upon completion of the scan of a channel, process the beacons received on that channel, filtered to the set of unique BSSIDs:
 - 1) Using the capabilities signaled in the beacon, modify the QoS AP count, ACM bit count, HC count, overlap count, and potential load of the channel array for the primary channel indicated in the received beacon.
 - 2) If the AP is using a channel bandwidth that is greater than the channel spacing (e.g., when using the 2.4 GHz band or when the overlapping AP allows 40 MHz HT PPDU in its BSS), also update the channel array for channels that are affected by this OBSS. For example, a beacon received on channel 2 indicating a 20 MHz BSS also affects channels 1, 3, and 4.
- e) Upon completion of scanning all of the channels, the AP has information on the number of APs and the potential load of each channel, including co-channel BSSs.
- f) If the channel array indicates that there are channels with no other APs, it is recommended to randomly choose one of these “empty” channels.
- g) Otherwise, create a list of candidate channels by selecting only the channels with the lowest number of QoS APs. For example, if the channel scan procedure indicated that there were two QoS APs on channel 3, three QoS APs on channel 6, and two QoS APs on channel 11, the list of candidate channels would contain 3 and 11.
 - 1) If this list contains one or more channels with non-QoS APs, then filter the list for the least number of APs.

- 2) If this list contains more than one channel, it is recommended to randomly choose one of these channels.
- h) If this list contains more than one channel and the AP has been configured to set the ACM bit for AC_VI or AC_VO:
 - 1) Filter the list for the minimum count of QoS AP where the EDCA Parameter Set element is present in the Beacon frame and the ACM bit is not set for AC_VI or AC_VO.
 - 2) If this list contains more than one channel, filter the list for the minimum count of QoS AP with the ACM bit set for AC_VI or AC_VO and with no indication of support for QLoad reporting.
 - 3) If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC and with no indication of support for QLoad reporting.
 - 4) If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element).
 - 5) If this list contains more than one channel, filter the list for the minimum count of QoS AP with the ACM bit set for AC_VI or AC_VO and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element).
- i) If this list contains more than one channel and the AP has an HC:
 - 1) Filter the list for the minimum count of QoS AP with an HC and with no indication of support for QLoad reporting.
 - 2) If this list contains more than one channel, filter the list for the minimum count of QoS AP with the ACM bit set for AC_VI or AC_VO and with no indication of support for QLoad reporting.
 - 3) If this list contains more than one channel, filter the list for the minimum count of QoS AP with an HC and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element).
 - 4) If this list contains more than one channel, filter the list for the minimum count of QoS AP with the ACM bit set for AC_VI or AC_VO and with an indication of support for QLoad reporting (i.e., the QLoad Report field equal to 1 in the Extended Capabilities element).
 - 5) If this list contains more than one channel, filter the list for the minimum count of QoS AP where the EDCA Parameter Set element is present in the Beacon frame and the ACM bit is not set for AC_VI or AC_VO.
- j) If this list contains more than one channel, filter the list to the set of channels with the minimum overlap count.
- k) If this list contains more than one channel, filter the list to the set of channels with the minimum potential load.
- l) From the remaining channels in this list, randomly choose one of these channels.

X.4 Sharing in an OBSS situation

X.4.1 General

If the EDCA Access Factor is greater than one, then there is a potential over-allocation of the WM. APs are advised to avoid over-allocation in the channel selection process, but if over-allocation exists, then a sharing scheme is recommended to ensure that each AP has a fair share of the bandwidth, but more importantly, to ensure that any already admitted or scheduled QoS streams are not impaired by the addition of streams from any OBSS. The EDCA Access Factor, HCCA Access Factor, and Potential Traffic Self fields in the QLoad Report element are provided to enable sharing schemes to be used.

The sharing scheme also protects an AP from the neighbor capture effect where it has neighbors that are hidden from each other. A major objective of an OBSS sharing scheme is that if a QoS stream is allocated or

scheduled, then it is not compromised by the addition of further streams from any OBSS that would cause the medium to be over-allocated. This objective is achieved if the APs in OBSSs cooperate.

X.4.2 Sharing schemes

X.4.2.1 General

Two sharing schemes are suggested: proportional sharing and on-demand sharing. In each sharing scheme, the purpose is to keep the total allocated traffic to a value where over-allocation does not occur. The absolute maximum allocation is 1 s/s (100%). In the following descriptions of the two suggested sharing schemes, this value is referred to as the *maximum allocation value* (MAV). It is suggested that in order to provide some protection to non-QoS traffic, each AP select a value for MAV:

$$MAV = (M + 1)/(M + N + 1) \text{ s/s} \quad (\text{X-33})$$

where

- M is the number of overlapping APs that are robust AV streaming STAs
- N is the number of overlapping APs that are not robust AV streaming STAs

There is no requirement that each AP select the same MAV.

X.4.2.2 Proportional sharing scheme

The proportional sharing scheme described in this subclause is an example of a static sharing policy, as described in Table 8-183c and 10.27.2.2.

When using the proportional sharing scheme, the AP examines the sum of the EDCA Access Factors and HCCA Access Factors in the QLoad reports from each OBSS, including its own Qload report, and determines the maximum. This maximum value is termed the *combined access factor*. If the maximum value from the combined access factor is less than or equal to MAV, the AP is advised to allocate only up to its advertised potential traffic self traffic. If the maximum value from the combined access factor is greater than MAV, then the AP is advised to allocate only up to a value of its potential traffic self divided by the combined access factor, multiplied by MAV.

In the proportional sharing scheme, before an AP allocates a new medium time or schedules a new TXOP in response to an ADDTS Request frame, it checks that this addition does not exceed its sharing limit, as follows:

- a) If the EDCA Access Factor is less than or equal to MAV, then the AP allocates up to its advertised potential traffic self, with the composite stream (MAX traffic) calculated as shown in Equation (X-34).

$$\text{MAX traffic} = \mu_{tot} + 2 \sigma_{tot} \quad (\text{X-34})$$

- b) If the EDCA Access Factor is greater than MAV, the AP carries out the following:
 - 1) Calculate the peak traffic value of the potential traffic self using Equation (X-35).

$$\text{Peak} = \mu_{tot} + 2 \sigma_{tot} \quad (\text{X-35})$$

- 2) Divide this value by the combined access factor and multiply by MAV. This value is termed the *maximum allowable potential traffic self traffic*.
- 3) Calculate the resulting value of the allocated traffic self if the new TSPEC is accepted, as explained in X.2.4, and then calculate the resulting peak value using Equation (X-36).

$$Peak = \mu_{tot} + 2 \sigma_{tot} \quad (X-36)$$

- 4) If the resulting peak value, calculated in step 3, is greater than the maximum allowable potential traffic self traffic, then the AP is advised to reject the ADDTS Request frame.
- 5) If the resulting peak value, calculated in step 3, is less than the maximum allowable potential traffic self traffic and the ADDTS Request frame is set for EDCA admission, then the AP is advised to accept the request.
- 6) The AP then checks that it is possible to schedule TXOPs using the HCCA TXOP advertisement as described in 10.27.3.

If the new stream is allocated, then the AP updates the appropriate fields in its QLoad Report element.

X.4.2.3 On-demand sharing scheme

The on-demand sharing scheme described in this subclause is an example of a dynamic sharing policy, as described in Table 8-183c and 10.27.2.2.

The on-demand sharing scheme is as follows:

- a) Before allocating a new stream, the AP examines the Allocated Traffic Shared field values in the QLoad reports from each OBSS, including its own Qload report, and selects the maximum Allocated Traffic Shared field value that has the highest peak value, using Equation (X-37).

$$Peak = \mu_{tot} + 2 \sigma_{tot} \quad (X-37)$$

The AP also notes the number of AC_VI and AC_VO streams in this maximum Allocated Traffic Shared field.

- b) The AP adds the requested new stream (*new*) to the selected maximum Allocated Traffic Shared field value (*max*) determined in step a, using Equation (X-38) and Equation (X-39).

$$\mu = \mu_{new} + Peak \quad (X-38)$$

$$\sigma = \sqrt{\sigma_{new}^2 + \sigma_{max}^2} \quad (X-39)$$

- c) The AP then calculates the peak value for the new composite stream calculated in step b, using Equation (X-40).

$$Peak = \mu + 2\sigma \quad (X-40)$$

- d) Using the values of the AC_VI and AC_VO streams noted in step a, plus the stream represented by the new stream, the AP determines the new EDCA Access Factor and then the combined access factor, as described in X.4.2.2.
- e) Multiply the peak value calculated in step c by the EDCA Access Factor, determined in step d. This value is the new peak traffic requirement.
- f) If this peak traffic requirement value calculated in step e is greater than MAV, then the AP is advised to refuse to allocate the new stream.
- g) If the peak value calculated in step e is less than or equal to MAV and the new allocation is for an EDCA admission ADDTS, then the AP allocates that new traffic.
- h) If the peak value calculated in step d is less than or equal to MAV and the new allocation is for an HCCA ADDTS, the AP checks that it is possible to schedule TXOPs using the HCCA TXOP advertisement as described in 10.27.3.

If the new stream is allocated, then the AP updates the appropriate fields in its QLoad Report element.

The Allocated Traffic Self field in the QLoad Report element of a particular AP can be used by other APs as an indication of whether an AP has over-allocated or is using an on-demand sharing scheme.

If, using either the proportional or on-demand sharing schemes, an AP determines that the acceptance of a TSPEC would exceed the available allocation, or if a non-AP STA has a TSPEC refused, the non-AP STA could always request a new TSPEC that represents a lower medium time or TXOP. This request might be used, for example, where the non-AP STA or AP has the ability to send a more compressed stream.

An AP might choose to use the on-demand sharing scheme until the maximum value of any access factor field in the QLoad Report elements from each OBSS reaches MAV. Once this condition has occurred, the AP could then use the proportional sharing for subsequent ADDTS requests.

X.5 Mitigating consequences of OBSS sharing in presence of noncollaborating devices

The performance of the channel selection and HCAA TXOP negotiation procedures described in this annex and 10.27 might become degraded by the presence of devices that willfully or accidentally behave in an uncooperative manner.

It is suggested that implementations use additional heuristics (e.g., a history of collaboration, traffic monitoring, device configuration, or a combination of such) to assess the accuracy of the information they receive from neighboring APs in order to determine an appropriate collaboration strategy.

An AP that maintains historical information of collaboration results with its neighboring APs could use this information to control its collaboration behavior. For example, an AP might choose to share a channel with an AP that had a history of successful collaboration. In another example, an AP might choose to avoid transmissions only during the HCCA TXOPs of neighboring APs with which it has a history of successful HCCA TXOP negotiation.

When using HCCA TXOP negotiation, it is suggested that an AP perform some monitoring of the channel to assess whether the HCCA AP with which it is collaborating is using its advertised HCCA TXOPs. If the monitoring AP does not detect HCCA traffic during these advertised HCCA TXOPs, such a lack of traffic might indicate that the neighboring AP is willfully or accidentally behaving in an uncooperative manner by advertising HCCA TXOPs that it is not using, possibly as a method to suppress traffic in neighboring BSSs. The monitoring AP might wish to ignore the HCCA TXOP advertisements from APs that do not appear to be collaborating.

Some of the OBSS procedures use unauthenticated Beacon frames and public action frames, which are susceptible to impersonation. If unauthenticated Beacon frames and public action frames are used, an AP might suffer a denial of service attack by another device impersonating the AP. This denial of service attack, due to the actions of the impersonating device, might cause neighboring APs to falsely ascertain the AP is not collaborating.

An AP could enable protected HCCA TXOP negotiation and protected QLoad reporting to provide protection against impersonation. The AP PeerKey protocol is used in the generation of the PMK to prove that an AP has the private key that corresponds to its public key. Impersonation of protected HCCA TXOP negotiation and protected QLoad report management from an AP is prevented while the AP maintains possession of this private key and this private key is not possessed by any other devices.