IEEE STANDARDS ASSOCIATION

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 1: Prioritization of Management Frames

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

6 April 2012

IEEE Std 802.11ae™-2012
(Amendment to
IEEE Std 802.11™-2012)

IEEE Std 802.11ae™-2012
(Amendment to
IEEE Std 802.11™-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 1: Prioritization of Management Frames

Sponsor

LAN/MAN Standards Committee

of the

IEEE Computer Society

Approved 29 March 2012

IEEE-SA Standards Board

Abstract: A mechanism for prioritization of management frames is provided and a protocol to communicate management frame prioritization policy is specified in this amendment.

Keywords: IEEE 802.11, IEEE 802.11ae, management, QMF, QoS, quality-of-service management frame

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

PDF: ISBN 978-0-7381-7241-5 STD97228
Print: ISBN 978-0-7381-7255-2 STDPD97228

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 documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata.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

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/findstds/interps/index.html.

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. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website <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 non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this amendment was submitted to the IEEE-SA for approval, the IEEE 802.11 Working Group had the following membership:

Bruce Kraemer, *Chair*
Jon Rosdahl, *Vice-chair and Treasurer*
Adrian P. Stephens, *Vice-chair, Technical Editor, and Assigned Number Authority*
Stephen McCann, *Secretary*
Peter Ecclesine, *Technical Editor*

At the time this amendment was submitted to sponsor ballot, Task Group ae had the following officers:

Michael Mentemurro, *Chair*
Henry Ptasinski, *Technical Editor*
Matthew Fischer, *Secretary*

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

Osama S. AboulMagd
Santosh P. Abraham
Roberto Aiello
Carlos H. Aldana
David C. Andrus
Sirikiat L. Ariyavisitakul
Lee R. Armstrong
Yusuke Asai
Alex Ashley
Kwok Shum Au
Geert A. Awater
David Bagby
Michael Bahr
Gabor Bajko
Raja Banerjea
Kaberi Banerjee
John R. Barr
Tuncer Baykas
Ted Booth
Daniel Borges
Andre Bourdoux
Gregory Breit
John Buffington
G. Bumiller
Necati Canpolat
Laurent Cariou
William Carney
Philippe Chambelin
Kapseok Chang
Clint F. Chaplin
Minho Cheong
Meng W. Chia
Woong Cho
Chang-Soon Choi
Inhwan Choi
In-Kyeong Choi
Jee-Yon Choi
Liwen Chu
John Coffey
Charles Cook
Carlos Cordeiro
Xavier P. Costa
Subir Das
Rolf J. de Vegt
Yohannes Demessie
Theodorus Denteneer
Thomas Derham
Susan Dickey
John Dorsey
Offie Drennan
Roger P. Durand
Peter Ecclesine
Marc Emmelmann
Vinko Erceg
Leonardo Estevez
Matthew Fischer
Wayne K. Fisher
George Flammer
Colin Frank
Wen Gao
Matthew Gast
Mohamed Ghamri-Doudane
Amir Ghasemi
James P. Gilb
Jeffrey Gilbert
Claude Giraud
Ronald Glibbery
Reinhard Gloger
Michelle Gong
David Goodall
Elad Gottlib
Sudheer A. Grandhi
Michael Grigat
Mark Grodzinsky
David Halasz
Mark Hamilton
Christopher J. Hansen
Dan N. Harkins
Brian D. Hart
Chris Hartman
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
Haeyoung Jun
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
Thet Khine
Alexey Khoryaev
Bonghoe Kim

Eun S. Kim
Eung S. Kim
Joonsuk Kim
Kyeongpyo Kim
Yongsun Kim
Youhan Kim
Youngsoo Kim
Yunjoo Kim
Shoichi Kitazawa
Jarkko Kneckt
Mark M. Kobayashi
Fumihide Kojima
Tom Kolze
Bruce P. Kraemer
Riichi Kudo
Thomas M. Kurihara
Joseph Kwak
Hyoungjin Kwon
Ui K. Kwon
Ismail Lakkis
Paul Lambert
Zhou Lan
Leonardo Lanante
Jeremy A. Landt
Joseph P. Lauer
Daewon Lee
Hoosung Lee
Il-Gu Lee
Jae S. Lee
Wookbong Lee
Wooyong Lee
Yuro Lee
Paul Lin
Hang Liu
Pei Liu
Yong Liu
Peter Loc
Artyom Lomayev
Bradley Lynch
Michael Lynch
Alastair Malarky
Jouni K. Malinen
Alexander Maltsev
Hiroshi Mano
Bill Marshall
Kenichi Maruhashi
Stephen McCann
Justin P. McNew
Simone Merlin
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
Mohammad H. Nasrabadi
Chiu Ngo
Paul Nikolich
Yujin Noh
Knut Odman
Jong-Ee Oh
Kazuyasu Okada
Satoshi Oyama
Santosh G. Pandey
Thomas Pare
Hyungu Park
Jaewoo Park
Minyoung Park
Bemini H. Peiris
Xiaoming Peng
Eldad Perahia
James E. Petranovich
Albert Petrick
John Petro
Riku Pirhonen
Vishakan Ponnampalam
James D. Portaro
Henry Ptasinski
Rene Purnadi
Ivan Pustogarov
Emily H. Qi
Huyu Qu
Jim E. Raab
Harish Ramamurthy
Ivan Reede
Alex Reznik
Sandrine Roblot
Jon Rosdahl
Ali Sadri
Kazuyuki Sakoda
Hemanth Sampath
Hirokazu Sawada
Jean Schwoerer
Yongho Seok
Huairong Shao
Nir Shapira
Stephen J. Shellhammer
Bazhong Shen
Ian Sherlock
Nobuhiko Shibagaki
Ashish Shukla
Michael Sim
Francois Simon
Shubhranshu Singh
Dwight Smith
Graham K. Smith
Jae-Hyung Song
Sudhir Srinivasa
Robert Stacey
Dorothy Stanley
Adrian P. Stephens
David S. Stephenson
John Stine
Guenael T. Strutt
Chin-Sean Sum
Mineo Takai
Yasushi Takatori
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
Ganesh Venkatesan
Sameer Vermani
George A. Vlantis
Sanjay Wadhwa
Chao-Chun Wang
Haiguang Wang
James J. Wang
Junyi Wang
Qi Wang
Fujio Watanabe
Menzo M. Wentink
Pyo C. Woo
James Worsham
Harry R. Worstell
Ye Wu
Liuyang Yang
James Yee
Jung Yee
Peter Yee
Su K. Yong
Christopher Young
Artur Zaks
Hongyuan Zhang
Ning Zhang
Meiyuan Zhao

Major contributions were received from the following individuals:

Matthew Fischer
Jouni Malinen
Stephen McCann
Michael Montemurro
Santosh G. Pandey
Henry Ptasinski
Dorothy Stanley
Dave Stephenson
Allan Thomson

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

Tomoko Adachi
Iwan Adhicandra
Thomas Alexander
Mark Anderson
Butch Anton
Lee R. Armstrong
Alex Ashley
Arthur Astrin
Kwok Shum Au
Michael Bahr
Harry Bims
Nancy Bravin
John Buffington
William Byrd
William Carney
Clint F. Chaplin
Keith Chow
Charles Cook
Wael Diab
Patrick Diamond
Thomas Dineen
Sourav Dutta
Peter Ecclesine
Richard Eckard
Richard Edgar
Dennis Edwards
Matthew Fischer
Andre Fournier
Matthew Gast
John Geiger
Pieter-Paul Giesberts
Gregory Gillooly
Reinhard Gloger
David Goodall
Sudheer A. Grandhi
Randall Groves
Michael Gundlach
C. Guy
Rainer Hach
Mark Hamilton
Christopher J. Hansen
Hiroshi Harada
Robert F. Heile
Rodney Hemminger
Jerome Henry
Marco Hernandez
David Hunter
Tetsushi Ikegami
Noriyuki Ikeuchi
Yasuhiko Inoue
Sergiu Iordanescu
Paul Isaacs
Akio Iso
Atsushi Ito
Raj Jain
Junghoon Jee
Tal Kaitz
Shinkyo Kaku
Piotr Karocki
Richard H. Kennedy
John Kenney
Stuart J. Kerry
Yongbum Kim
Youhan Kim
Bruce Kraemer
Thomas M. Kurihara
Geoff Ladwig
Richard Lancaster
Jeremy A. Landt
Jan-Ray Liao
Arthur Light
Lu Liru
William Lumpkins
Greg Luri
Elvis Maculuba
Jouni K. Malinen
W. Kyle Maus
Stephen McCann
Michael Mcinnis
Gary Michel
Apurva Mody
Michael Montemurro
Rick Murphy
Peter Murray
Andrew Myles
Michael S. Newman
Paul Nikolich
Kevin Noll
John Notor
Satoshi Obara
Robert O'hara
Chris Osterloh
Satoshi Oyama
Stephen Palm
Brian Phelps
Shmulik Pisanty
Clinton Powell
Venkatesha Prasad
Michael Probasco
Henry Ptasinski
Emily H. Qi
Mohammad Azizur Rahman
Jayaram Ramasastry
Ivan Reede
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jon Rosdahl
Randall Safier
Shigenobu Sasaki
Bartien Sayogo
Shusaku Shimada
John Short
Gil Shultz
Graham K. Smith
Kapil Sood
Amjad Soomro
Robert Stacey
Dorothy Stanley
Thomas Starai
Adrian P. Stephens
Walter Struppler
Mark Sturza
Bo Sun
Joseph Tardo
Michael Johas Teener
Ichihiko Toyoda
Mark-Rene Uchida
Anna Urra
Dmitri Varsanofiev
Prabodh Varshney
Ganesh Venkatesan
John Vergis
Bhupender Virk
George A. Vlantis
Khurram Waheed
Lei Wang
Stanley Wang
Stephen Webb
Hung-Yu Wei
Menzo M. Wentink
James Worsham
Tan Pek Yew
Joseph Yob
Oren Yuen

When the IEEE-SA Standards Board approved this standard 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 Kyun 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

Catherine Berger
IEEE Standards Senior Program Manager, Document Development

Kathryn Bennett
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of 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 Medium Access Control (MAC) and physical layer (PHY) Specifications—Amendment 1: Prioritization of Management Frames.

This document provides amendments to the IEEE 802.11 PHY/MAC layers related to QoS for Management Frames.

Contents

3. Definitions, acronyms, and abbreviations 2

3.2 Definitions specific to IEEE 802.11 2
3.3 Abbreviations and acronyms 2

4. General description 3

4.5 Overview of the services 3
4.5.6 Traffic differentiation and QoS support 3

5. MAC service definition 3

5.1 Overview of MAC services 3
5.1.1 Data service 3

6. Layer management 4

6.3 MLME SAP interface 4
6.3.3 Scan 4
6.3.7 Associate 4
6.3.8 Reassociate 6
6.3.11 Start 8
6.3.83 QMF policy 9

8. Frame formats 14

8.2 MAC frame formats 14
8.2.4 Frame fields 14
8.3 Format of individual frame types 16
8.3.3 Management frames 16
8.4 Management frame body components 18
8.4.2 Information elements 18
8.5 Action frame format details 20
8.5.8 Public Action details 20
8.5.11 Protected Dual of Public Action frames 22

9. MAC sublayer functional description 22

9.2 MAC architecture 22
9.2.4 Hybrid coordination function (HCF) 22
9.3 DCF 22
9.3.2 Procedures common to the DCF and EDCAF 22

10. MLME 24

10.23 Wireless network management procedures 24
10.23.14 Channel usage procedures 24
10.25 Quality-of-service management frame (QMF) 25
10.25.1 General 25
10.25.2 QMF policy advertisement and configuration procedures 28
10.25.3 Interpreting QMF access categories 31

11. Security 32

11.4 RSNA confidentiality and integrity protocols 32
11.4.3 CTR with CBC-MAC Protocol (CCMP) 32
11.4.4 Broadcast/Multicast Integrity Protocol (BIP) 33

Annex B (normative) Protocol Implementation Conformance Statement (PICS) proforma 35

B.2 Abbreviations and special symbols 35
B.2.2 General abbreviations for Item and Support columns 35
B.4 PICS proforma—IEEE Std 802.11-2012 35
B.4.3 IUT configuration 35
B.4.24 QMF extensions 36

Annex C (normative) ASN.1 encoding of the MAC and PHY MIB 37

C.3 MIB Detail 37

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 1: Prioritization of Management Frames

(This amendment specifies enhancements to IEEE Std 802.11™.)

NOTE—The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.[1]

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

3. Definitions, acronyms, and abbreviations

3.2 Definitions specific to IEEE 802.11

Insert the following new definitions:

group-addressed quality-of-service management frame (GQMF): A group-addressed management frame that is transmitted using the quality-of-service management frame (QMF) service.

individually addressed quality-of-service management frame (IQMF): An individually addressed management frame that is transmitted using the quality-of-service management frame (QMF) service.

non-quality-of-service management frame (non-QMF) access point (AP): An AP that does not implement the quality-of-service management frame (QMF) service.

non-quality-of-service management frame (non-QMF) station (STA): A STA that does not implement the quality-of-service management frame (QMF) service.

quality-of-service management frame (QMF): A management frame that is transmitted using the QMF service.

quality-of-service management frame (QMF) access point (AP): A quality-of-service AP that implements the QMF service.

quality-of-service management frame (QMF) policy: A policy defining the access category of management frames. QMF stations (STAs) transmit their management frames using the access category defined by the policy.

quality-of-service management frame (QMF) service: A service in which the enhanced distributed channel access (EDCA) access category with which a management frame is sent is determined according to a configured policy.

quality-of-service management frame (QMF) station (STA): A quality-of-service STA that implements the QMF service.

3.3 Abbreviations and acronyms

Insert the following new acronyms in alphabetical order:

GQMF	group-addressed quality-of-service management frame
IQMF	individually addressed quality-of-service management frame
QACM	QMF access category mapping
QMF	quality-of-service management frame

4. General description

4.5 Overview of the services

4.5.6 Traffic differentiation and QoS support

Insert the following heading (4.5.6.1) immediately after the heading 4.5.6:

4.5.6.1 General

Insert the following new subclause at the end of 4.5.6:

4.5.6.2 Quality-of-service management frame support

When the quality-of-service management frame (QMF) service is enabled, some management frames might be transmitted using an access category other than the access category assigned to voice traffic (access category AC_VO, see 8.4.2.31) in order to improve the quality of service of other traffic streams. This is achievable by the use of a QMF policy. A QMF policy defines the access categories of different management frames. Only QoS STAs are able to implement QMF policy. A non-AP QMF STA uses the default QMF policy or the QMF policy accepted from a peer QMF STA to transmit management frames to that peer QMF STA. A QMF AP sets its own QMF policy for the transmission of QMFs to its associated STAs. A QMF STA uses access category AC_VO to transmit management frames to STAs that do not support the QMF service.

5. MAC service definition

5.1 Overview of MAC services

5.1.1 Data service

5.1.1.1 General

Change the first paragraph as follows:

This service provides peer LLC entities with the ability to exchange MSDUs. To support this service, the local MAC uses the underlying PHY-level services to transport an MSDU to a peer MAC entity, where it is delivered to the peer LLC. Such asynchronous MSDU transport is performed on a connectionless basis. By default, MSDU transport is on a best-effort basis. However, the QoS facility uses a traffic identifier (TID) to specify differentiated services on a per-MSDU basis. The QoS facility also permits more synchronous behavior to be supported on a connection-oriented basis using TSPECs. There are no guarantees that the submitted MSDU will be delivered successfully. Group addressed transport is part of the data service provided by the MAC. Due to the characteristics of the WM, group addressed MSDUs may experience a lower QoS, compared to that of individually addressed MSDUs. All STAs support the data service, but only QoS STAs in a QoS BSS differentiate their MSDU delivery according to the designated traffic category or traffic stream (TS) of individual MSDUs. QoS STAs that support the QMF service differentiate their MMPDU delivery according to the MMPDU's access category. The access category of each MMPDU is designated by the transmitter's current QMF policy.

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 new row at the end of the BSSDescription parameter table:

Name	Type	Valid range	Description	IBSS adoption
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	The values from the QMF Policy element if such an element was present in the Probe Response or Beacon frame, else null.	Do not adopt

6.3.7 Associate

6.3.7.3 MLME-ASSOCIATE.confirm

6.3.7.3.2 Semantics of the service primitive

Change the primitive parameter list as follows:

The primitive parameters are as follows:

MLME-ASSOCIATE.confirm(
ResultCode,
CapabilityInformation,
AssociationID,
SupportedRates,
EDCAParameterSet,
RCPI.request,
RSNI.request,
RCPI.response,
RSNI.response,
RMEnabledCapabilities,
Content of FT Authentication elements,
SupportedOperatingClasses,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
TimeoutInterval,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
QosMapSet,
QMFPolicy,

VendorSpecificInfo
)

Insert the following new row before VendorSpecificInfo in the parameter table:

Name	Type	Valid range	Description
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	The values from the QMF Policy element if such an element was present in the Association Response frame else null.

6.3.7.5 MLME-ASSOCIATE.response

6.3.7.5.2 Semantics of the service primitive

Change the primitive parameter list as follows:

The primitive parameters are as follows:

MLME-ASSOCIATE.response(
PeerSTAAddress,
ResultCode,
CapabilityInformation,
AssociationID,
EDCA Parameter Set,
RCPI,
RSNI,
RMEnabledCapabilities,
Content of FT Authentication Elements,
SupportedOperatingClasses,
DSERegisteredLocation,
HTCapabilities,
Extended Capabilities,
20/40 BSS Coexistence,
TimeoutInterval,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
QoSMapSet,
QMFPolicy,
VendorSpecificInfo
)

Insert the following new row before VendorSpecificInfo in the parameter table:

Name	Type	Valid range	Description
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	Describes the QMF policy of the AP. This parameter is present when dot11QMFActivated is true, and is not present otherwise.

6.3.8 Reassociate

6.3.8.3 MLME-REASSOCIATE.confirm

6.3.8.3.2 Semantics of the service primitive

Change the primitive parameter list as follows:

The primitive parameters are as follows:

MLME-REASSOCIATE.confirm(
ResultCode,
CapabilityInformation,
AssociationID,
SupportedRates,
EDCAParameterSet,
RCPI.request,
RSNI.request,
RCPI.response,
RSNI.response,
RMEnabledCapabilities,
Content of FT Authentication Elements,
SupportedOperatingClasses,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
TimeoutInterval,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
FMSResponse,
DMSResponse,
QoSMapSet,
QMFPolicy,
VendorSpecificInfo
)

Insert the following new row before VendorSpecificInfo in the parameter table:

Name	Type	Valid range	Description
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	The values from the QMF Policy element if such an element was present in the Reassociation Response frame, else null.

6.3.8.5 MLME-REASSOCIATE.response

6.3.8.5.2 Semantics of the service primitive

Change the primitive parameter list as follows:

The primitive parameters are as follows:

MLME-REASSOCIATE.response(
PeerSTAAddress,
ResultCode,
CapabilityInformation,
AssociationID,
EDCAParameterSet,
RCPI,
RSNI,
RMEnabledCapabilities,
Content of FT Authentication elements,
SupportedOperatingClasses,
DSERegisteredLocation,
HT Capabilities,
Extended Capabilities,
20/40 BSS Coexistence,
TimeoutInterval,
BSSMaxIdlePeriod,
TIMBroadcastResponse,
FMSResponse,
DMSResponse,
QoSMapSet,
<u>QMFPolicy,</u>
VendorSpecificInfo
)

Insert the following new row before VendorSpecificInfo in the parameter table:

Name	Type	Valid range	Description
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	Describes the QMF policy of the AP. This parameter is present when dot11QMFActivated is true, and is not present otherwise.

6.3.11 Start

6.3.11.2 MLME-START.request

6.3.11.2.2 Semantics of the service primitive

Change the primitive parameter list as follows:

The primitive parameters are as follows:

MLME-START.request(
SSID,
SSIDEncoding,
BSSType,
BeaconPeriod,
DTIMPeriod,
CF parameter set,
PHY parameter set,
IBSS parameter set,
ProbeDelay,
CapabilityInformation,
BSSBasicRateSet,
OperationalRateSet,
Country,
IBSS DFS Recovery Interval,
EDCAParameterSet,
DSERegisteredLocation,
HT Capabilities,
HT Operation,
BSSMembershipSelectorSet,
BSSBasicMCSSet,
HTOperationalMCSSet,
Extended Capabilities,
20/40 BSS Coexistence,
Overlapping BSS Scan Parameters,
MultipleBSSID,
InterworkingInfo,
AdvertisementProtocolInfo,
RoamingConsortiumInfo,
Mesh ID,
Mesh Configuration,
QMFPolicy,
VendorSpecificInfo
)

Insert the following new row before VendorSpecificInfo in the parameter table:

Name	Type	Valid range	Description
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This element is present when dot11QMFActivated is true and BSSType = INFRASTRUCTURE or MESH, and is not present otherwise, and is provided by the SME to signal to the MLME the QMF policy to be used for this BSS.

Insert the following new subclauses:

6.3.83 QMF policy

6.3.83.1 Introduction

The following MLME primitives support the signaling of QMF policy.

6.3.83.2 MLME-QMFPOLICY.request

6.3.83.2.1 Function

This primitive requests the transmission of an unsolicited QMF Policy frame to a peer entity.

6.3.83.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICY.request (
                        Peer STA Address,
                        QMFPolicy
                        )
```

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC entity to which the QMF policy is sent.
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This parameter describes the QMF policy the peer STA is required to use.

6.3.83.2.3 When generated

This primitive is generated by the SME to request that a QMF Policy frame be sent to a peer entity to communicate QMF policy information.

6.3.83.2.4 Effect of receipt

On receipt of this primitive, the MLME constructs a QMF Policy frame. This frame is then scheduled for transmission.

6.3.83.3 MLME-QMFPOLICY.indication

6.3.83.3.1 Function

This primitive indicates that an unsolicited QMF Policy frame has been received from a peer entity.

6.3.83.3.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICY.indication (
                                    Peer STA Address,
                                    QMFPolicy
                                    )
```

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC from which the QMF policy was received.
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This parameter describes the QMF policy the peer STA is requiring to be used.

6.3.83.3.3 When generated

This primitive is generated by the MLME when a valid QMF Policy frame with dialog token equal to 0 is received from a peer entity.

6.3.83.3.4 Effect of receipt

The SME is notified of the receipt of a QMF policy.

6.3.83.4 MLME-QMFPOLICYCHANGE.request

6.3.83.4.1 Function

This primitive supports the change of QMF Policy between peer STAs. The SME requests the transmission of a QMF Policy Change frame in order to request a change in the QMF policy the STA uses to transmit to the peer STA.

6.3.83.4.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICYCHANGE.request (
                                    Peer STA Address,
```


Dialog Token,
QMFPolicy
)

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC entity to which the QMF policy change request is sent.
Dialog Token	Integer	1–255	The dialog token to identify the QMF policy change transaction.
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This parameters describes the QMF policy the STA is requesting to use.

6.3.83.4.3 When generated

This primitive is generated by the SME when a STA wishes to request a change of the QMF policy it uses to transmit management frames to a peer entity.

6.3.83.4.4 Effect of receipt

On receipt of this primitive, the MLME constructs a QMF Policy Change frame containing the set of QMF policy parameters. This frame is then scheduled for transmission.

6.3.83.5 MLME-QMFPOLICYCHANGE.confirm

6.3.83.5.1 Function

This primitive reports the results of a policy change attempt with a peer QMF STA.

6.3.83.5.2 Semantics of the service primitive

The primitive parameters are as follows:

MLME-QMFPOLICYCHANGE.confirm (
Peer STA Address,
Dialog Token,
Result Code
)

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC entity from which the QMF policy was received.
Dialog Token	Integer	1–255	The dialog token to identify the QMF policy change transaction.
Result Code	Enumeration	SUCCESS, REJECT, TIMEOUT	Reports the receipt of a QMF Policy frame and the result of the QMF policy change at the peer SME or if no matching response is received within dot11QMFPolicyChangeTimeout TU.

6.3.83.5.3 When generated

This primitive is generated by the MLME as a result of receipt of a QMF Policy frame with a dialog token that matches the dialog token from the MLME-QMFPOLICYCHANGE.request.

6.3.83.5.4 Effect of receipt

The SME is notified of the results of the QMF policy change procedure.

6.3.83.6 MLME-QMFPOLICYCHANGE.indication

6.3.83.6.1 Function

This primitive indicates that a QMF Policy Change frame has been received from a peer entity.

6.3.83.6.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICYCHANGE.indication (
                                    Peer STA Address,
                                    Dialog Token,
                                    QMFPolicy
                                    )
```

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC entity from which the QMF policy change request was received.
Dialog Token	Integer	1–255	The dialog token to identify the QMF policy change transaction.
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This parameter describes the QMF policy the peer STA is requesting to use.

6.3.83.6.3 When generated

This primitive is generated by the MLME when a valid QMF Policy Change frame is received from a peer entity.

6.3.83.6.4 Effect of receipt

On receipt of this primitive, the parameters of the QMF Policy Change frame are provided to the SME to be processed.

6.3.83.7 MLME-QMFPOLICYCHANGE.response

6.3.83.7.1 Function

This primitive requests the transmission of a QMF Policy frame with no QMF Policy field to a peer entity, in response to a received QMF Policy Change frame.

6.3.83.7.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICYCHANGE.response (
                                    Peer STA Address,
                                    Dialog Token,
                                    Result Code
                                    )
```

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC Address	The address of the peer MAC entity to which the QMF Policy frame is sent in response to a QMF policy change request.
Dialog Token	Integer	1–255	The dialog token identifying the QMF policy change transaction.
Result Code	Enumeration	SUCCESS, REJECT	Reports the outcome of the transaction.

6.3.83.7.3 When generated

This primitive is generated by the SME to request that a QMF Policy frame be transmitted to a peer entity to convey the results of the QMF policy change procedure.

6.3.83.7.4 Effect of receipt

On receipt of this primitive, the MLME constructs a QMF Policy frame containing the set of QMF Policy elements specified. This frame is then scheduled for transmission.

6.3.83.8 MLME-QMFPOLICYSET.request

6.3.83.8.1 Function

This primitive directs the setting of a specific QMF policy in the local MLM.

6.3.83.8.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-QMFPOLICYSET.request (
                                    Peer STA address,
                                    QMFPolicy
                                    )
```

6.3.83.8.3 When generated

This primitive is generated by the SME to set the MLME's QMF policy for a peer STA.

Name	Type	Valid range	Description
Peer STA Address	MAC Address	Any valid individual MAC address	The address of the peer STA for which the QMF policy is to be used. If this parameter is null, the QMF policy applies to all transmissions.
QMFPolicy	QMF Policy element	As defined in 8.4.2.122	This parameter describes the QMF policy the MLME is directed to use for all QMFs transmitted to the Peer STA Address.

6.3.83.8.4 Effect of receipt

On receipt of this primitive, the MLME uses the supplied set of QMF policy parameters in future transmissions to the peer.

8. Frame formats

8.2 MAC frame formats

8.2.4 Frame fields

8.2.4.1 Frame Control field

8.2.4.1.4 To DS and From DS fields

Change the clause as follows:

The meaning of the combinations of values for the To DS and From DS fields <u>in data frames</u> are shown in Table 8-2.

Table 8-2—To/From DS combinations in data frames

To DS and From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, a data frame direct from one non-AP STA to another non-AP STA within the same BSS, or a data frame outside the context of a BSS~~, as well as all management and control frames~~.
To DS = 1 From DS = 0	A data frame destined for the DS or being sent by a STA associated with an AP to the Port Access Entity in that AP.
To DS = 0 From DS = 1	A data frame exiting the DS or being sent by the Port Access Entity in an AP, or a group addressed Mesh Data frame with Mesh Control field present using the three-address MAC header format.
To DS = 1 From DS = 1	A data frame using the four-address MAC header format. This standard defines procedures for using this combination of field values only in a mesh BSS.

Insert the following new text at the end of the clause:

The meanings of the combinations of values of the management frame To DS and From DS fields are shown in Table 8-2a.

Table 8-2a—To/From DS combinations in management frames

To DS and From DS values	Meaning
To DS = 0 From DS = 0	All non-QMF management frames.
To DS = 1 From DS = 0	All QMF management frames.
To DS = 0 From DS = 1	This combination is reserved.
To DS = 1 From DS = 1	This combination is reserved.

In all control frames, To DS and From DS are both zero.

8.2.4.4 Sequence Control field

8.2.4.4.2 Sequence Number field

Change the clause as follows:

Each MSDU, A-MSDU, or MMPDU transmitted by a STA is assigned a sequence number. See 9.3.2.10 (Duplicate detection and recovery). Sequence numbers are not assigned to control frames, as the Sequence Control field is not present in those frames.

The Sequence Number field in data frames is a 12-bit field indicating the sequence number of ~~an~~the MSDU~~,~~ or A-MSDU.~~, or MMPDU. Each MSDU, A-MSDU or MMPDU transmitted by a STA is assigned a sequence number. Sequence numbers are not assigned to control frames, as the Sequence Control field is not present.~~

The Sequence Number field in QMFs comprises the QMF Sequence Number subfield and the AC Index (ACI) subfield. The QMF Sequence Number subfield is a 10-bit subfield indicating the sequence number of the frame. The ACI subfield is a 2-bit subfield indicating the ACI of the frame. The format of the Sequence Number field in QMFs is shown in Figure 8-3a.

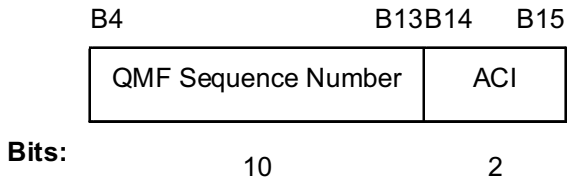

Figure 8-3a—Sequence Number field in QMFs

The value of the ACI subfield represents the ACI of the frame as defined in 8.4.2.31.

The Sequence Number field in management frames that are not QMFs is a 12-bit field indicating the sequence number of the frame.

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.

8.3 Format of individual frame types

8.3.3 Management frames

8.3.3.1 Format of management frames

Insert the following text before the last two paragraphs in 8.3.3.1:

A management frame is an IQMF when both

— The RA of the management frame corresponds to an individual MAC address; and

— The To DS subfield is set to 1 and the From DS subfield of the Frame Control field is set to 0.

A management frame is a GQMF when both

— The RA of the management frame corresponds to a group MAC address; and

— The To DS subfield is set to 1 and the From DS subfield of the Frame Control field is set to 0.

8.3.3.2 Beacon frame format

Insert the following row in Table 8-20 before the "Vendor Specific" element:

Table 8-20—Beacon frame body

Order	Information	Notes
56	QMF Policy	Indicates the QMF policy parameters of the transmitting STA. The QMF Policy element is present when dot11QMFActivated is true, and is not present otherwise. The QMF Policy element is never present in Beacon frames in an IBSS.

8.3.3.6 Association Response frame format

Insert the following row in Table 8-23 before the "Vendor Specific" element:

Table 8-23—Association Response frame body

Order	Information	Notes
22	QMF Policy	The QMF Policy element is present if dot11QMFActivated is true and the QMFActivated subfield is 1 in the Extended Capabilities element in the Association Request that elicited this Association Response frame.

8.3.3.8 Reassociation Response frame format

Insert the following row in Table 8-25 before the "Vendor Specific" element:

Table 8-25—Reassociation Response frame body

Order	Information	Notes
26	QMF Policy	The QMF Policy element is present if dot11QMFActivated is true and the QMFActivated subfield is 1 in the Extended Capabilities element in the Reassociation Request that elicited this Reassociation Response frame.

8.3.3.10 Probe Response frame format

Insert the following row in Table 8-27 before the "Vendor Specific" element

Table 8-27—Probe Response frame body

Order	Information	Notes
55	QMF Policy	The QMF Policy element is present if dot11QMFActivated is true and the QMFActivated subfield is 1 in the Extended Capabilities element in the Probe Request that elicited this Probe Response frame.

8.4 Management frame body components

8.4.2 Information elements

8.4.2.1 General

Insert a new item in Table 8-54, and update the Reserved items as appropriate:

Table 8-54—Element IDs

Element	Element ID	Length of indicated element (in octets)	Extensible
QMF Policy (see 8.4.2.122)	181	3 to 257	

8.4.2.29 Extended Capabilities element

Insert two new items in Table 8-103, and update the reserved values as appropriate:

Table 8-103—Capabilities field

Bit	Information	Notes
49	QMFActivated	This subfield is set to 1 if dot11QMFActivated is true. Otherwise, it is set to 0. See 10.25.
50	QMFReconfigurationActivated	This subfield is set to 1 if dot11QMFReconfigurationActivated is true. Otherwise, it is set to 0. See 10.25.

Insert the following new subclause at the end of 8.4.2:

8.4.2.122 Quality-of-Service Management Frame Policy element

The Quality-of-Service Management Frame (QMF) Policy element defines a QMF access category mapping (QACM) of management frames and is used to advertise and exchange QMF policy between STAs. The use of the QMF Policy element is given in 10.25. See Figure 8-401a.

	Element ID	Length	QACM #1	...	QACM #N
Octets:	1	1	variable		variable

Figure 8-401a—QMF Policy element format

The value of the Element ID field is equal to the QMF Policy value in Table 8-54.

The Length field is a 1-octet field whose value is dependent on the number and size of the QACM fields present in the element. The value of the Length field is between 1 and 255.

The QACM field specifies a group of management frames and their associated access categories. See Figure 8-401b and see 10.25.3.

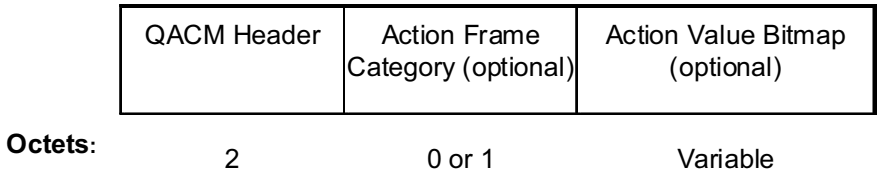

Figure 8-401b—QACM field format

The format of the QACM Header subfield of the QACM field is defined in Figure 8-401c.

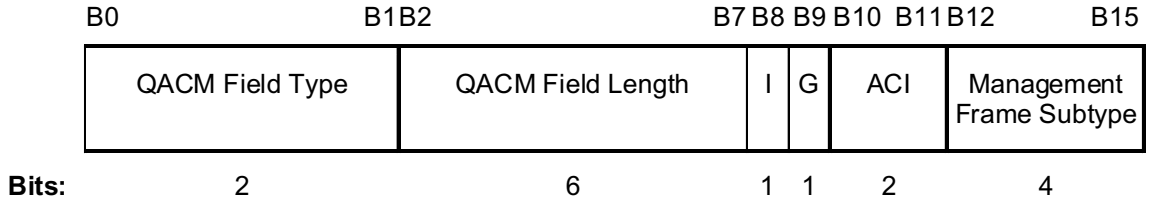

Figure 8-401c—QACM Header subfield

The QACM Field Type subfield is 2 bits in length and defines the structure of the QACM field. Its value is 0. Values 1, 2, and 3 are reserved.

The QACM Field Length subfield is 6 bits in length and defines the length in octets of the QACM field excluding the QACM Header subfield.

The Individually Addressed subfield (I) is 1 bit in length. When the QACM applies to individually addressed management frames, the value of the Individually Addressed subfield is 1. Otherwise, it is 0.

The Group Addressed subfield (G) is 1 bit in length. When the QACM applies to group addressed management frames, the value of the Group Addressed subfield is 1. Otherwise, it is 0.

The combination of I = 0 and G = 0 is not allowed.

The ACI subfield is 2 bits in length. Each frame of type management that is listed in the QACM Header subfield is transmitted using the access category identified by the accompanying ACI subfield.

The Management Frame Subtype subfield is 4 bits in length. It indicates the subtype of management frames that are sent using the access category indicated in the ACI subfield. The valid values for this subfield are the subtypes in Table 8-1 that correspond to frames of type management.

The Action Frame Category subfield is 1 octet in length and indicates the category of the Action frame, as defined in 8.4.1.11, of Action frames that are sent using the access category indicated in the ACI subfield. The Action Frame Category subfield is included only when the Management Frame Subtype subfield indicates Action or Action No Ack subtype as specified in 10.25.3.

The Action Value Bitmap subfield is included when the QACM Policy is specified for a subset of Action frame types in a Action Frame Category. The Action Value Bitmap subfield is of variable length and indicates the action values, as defined in 8.5, for the corresponding Action frame category that are sent using the access category indicated in the ACI subfield. The Action Value Bitmap subfield is included only when the Management Frame Subtype subfield indicates Action or Action No Ack subtype and the QACM Field Length subfield is greater than or equal to 2. Each bit in the Action Value Bitmap subfield is mapped to the corresponding action value. The Action Value Bitmap subfield is zero padded to complete any incomplete octet. When included, the size in octets of the Action Value Bitmap field is found by subtracting 1 from the value of the QACM Field Length subfield.

8.5 Action frame format details

8.5.8 Public Action details

8.5.8.1 Public Action frames

Insert two new items in Table 8-210 and update the reserved values as appropriate:

Table 8-210—Public Action field values

Public Action field value	Description
18	QMF Policy
19	QMF Policy Change

Insert the following new subclauses at the end of 8.5.8:

8.5.8.18 QMF Policy frame format

The QMF Policy frame uses the Action frame format and is transmitted by a requesting STA to a receiving STA with the included QMF policy. It is either sent unsolicited by the requesting STA or in response to a QMF Policy Change frame from a receiving STA. The format of the Action field of the QMF Policy frame is shown in Figure 8-460a.

	Category	Public Action	Dialog Token	Status Code	QMF Policy element (optional)
Octets:	1	1	1	2	3-257

Figure 8-460a—QMF Policy frame Action field contents

The Category field is set to the value for public action defined in Table 8-38.

The Public Action field is set to indicate a QMF Policy frame, as defined in Table 8-210.

The Dialog Token field is set to the value in the corresponding QMF Policy Change frame. If the QMF Policy frame is not being transmitted in response to a QMF Policy Change frame, then the Dialog Token field is set to zero.

The Status Code field is defined in 8.4.1.9.

The QMF Policy element is set as described in 8.4.2.122. It indicates the new access categories configured for management frame(s). This field is included if the Status Code is 0 (“Successful”) and this frame is not being transmitted in response to a QMF Policy Change frame, and optionally included if the Status Code is 37 (The request has been declined).

8.5.8.19 QMF Policy Change frame format

The QMF Policy Change frame uses the Action frame format and is transmitted by a requesting STA to request a change to the QMF policy it most recently received from the destination STA. The format of the Action field of the QMF Policy Change frame is shown in Figure 8-460b.

	Category	Public Action	Dialog Token	QMF Policy element
Octets:	1	1	1	3-257

Figure 8-460b—QMF Policy Change Action field contents

The Category field is set to the value for public action defined in Table 8-38.

The Public Action field is set to indicate a QMF Policy Change frame, as defined in Table 8-210.

The Dialog Token field is set to a nonzero value chosen by the STA sending the QMF Policy Change frame to identify the transaction.

The QMF Policy element is set as described in 8.4.2.122. It indicates the new access categories requested for management frame(s).

8.5.11 Protected Dual of Public Action frames

Insert two new items at the end of Table 8-228 and update the reserved values as appropriate:

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

Public Action field value	Description	Defined in
18	Protected QMF Policy	8.5.8.18
19	Protected QMF Policy Change	8.5.8.19

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 second-to-last paragraph of 9.2.4.2 as follows:

If dot11QMFActivated is false or not present for a QoS STA, a~~A~~ QoS STA should send individually addressed Management frames that are addressed to a non-QoS STA using the access category AC_BE and shall send all other management frames using the access category AC_VO, whether or not it is associated with a BSS or there is a QoS facility in the BSS. If dot11QMFActivated is false or not present for a QoS STA, a~~A~~ QoS STA that does not send individually addressed Management frames that are addressed to a non-QoS STA using the access category AC_BE shall send them using the access category AC_VO. Management frames are exempted from any and all restrictions on transmissions arising from admission control procedures. ~~A QoS STA shall also send management frames using the access category AC_VO beforeassociating with any BSS and before establishing mesh peerings in an MBSS, even if there is no QoS facility available in that BSS.~~ If dot11QMFActivated is true for a STA, the STA shall send management frames as described in 10.25. BlockAckReq and BlockAck frames shall be sent using the same access category as the corresponding QoS data frames. PS-Poll frames shall be sent using the access category AC_BE (to reduce the likelihood of collision following a Beacon frame) and are exempted from any and all restrictions on transmissions arising from admission control procedures. When the first frame in a frame exchange sequence is an RTS or CTS frame, the RTS or CTS frame shall be transmitted using the access category of the corresponding QoS Data/QoS Null frame(s) or AC_VO for management frames. Control Wrapper frames shall be sent using the access category that would apply to the carried control frame.

9.3 DCF

9.3.2 Procedures common to the DCF and EDCAF

9.3.2.10 Duplicate detection and recovery

Change 9.3.2.10 as follows:

Because MAC-level acknowledgments and retransmissions are incorporated into the protocol, there is the possibility that a frame may be received more than once. The procedures defined in this subclause attempt to filter out these duplicates. Additional duplicate filtering is performed during Receive Buffer Operation for frames that are part of a Block Ack agreement as described in 9.21.4 and 9.21.7.

Duplicate frame filtering is facilitated through the inclusion of a Sequence Control field (consisting of a sequence number and fragment number) within data and management frames ~~as well as,~~ a TID subfield in the QoS Control field within QoS data frames, and an ACI subfield in the Sequence Number field within QMFs. MPDUs that are part of the same MSDU or A-MSDU shall have the same sequence number, and different MSDUs or A-MSDUs have (with a high probability) a different sequence number.

A non-QoS STA shall assign sequence numbers to management frames and data frames (QoS subfield of the Subtype field is equal to 0) from a single modulo-4096 counter, starting at 0 and incrementing by 1, for each MSDU or MMPDU. A QoS STA operating as a non-QoS STA because it is in a non-QoS BSS or non-QoS IBSS shall assign sequence numbers to management frames and data frames (QoS subfield of the Subtype field is equal to 0) from a single modulo-4096 counter, starting at 0 and incrementing by 1, for each MSDU or MMPDU. A transmitting STA should cache the last used sequence number per RA for frames that are assigned sequence numbers from this counter and should ensure that the successively assigned sequence numbers for frames transmitted to a single RA do not have the same value by incrementing the counter by 2, if incrementing by 1 would have produced the same sequence number as is found in the cache for that RA.

A STA operating as a QoS STA shall maintain one modulo-4096 counter per <Address 1, TID> tuple, for individually addressed QoS Data frames. Sequence numbers for these frames are assigned using the counter identified by the Address 1 field and the TID subfield of the QoS Control field of the frame, and that counter is incremented by 1 for each MSDU or A-MSDU corresponding to that <Address 1, TID> tuple. Sequence numbers for management frames, QoS data frames with a group address in the Address 1 field, and all non-QoS data frames transmitted by QoS STAs with dot11QMFActivated false or not present shall be assigned using an additional single modulo-4096 counter, starting at 0 and incrementing by 1 for each such MSDU, A-MSDU or MMPDU, except that a QoS STA may use values from additional modulo-4096 counters per <Address 1, TID> for sequence numbers assigned to time priority management frames. A transmitting STA should cache the last used sequence number per RA for frames that are assigned sequence numbers from this counter and should ensure that the successively assigned sequence numbers for frames transmitted to a single RA do not have the same value by incrementing the counter by 2, if incrementing by 1 would have produced the same sequence number as is found in the cache for that RA.

When transmitted by a QMF STA, the STA shall assign sequence numbers for the frames listed below using a modulo-4096 counter, starting at 0 and incrementing by 1 for each such MSDU or MMPDU:

- Management frames that are not QMFs
- Group addressed QoS data frames
- All non-QoS data frames

and shall assign the sequence number for QMFs from one modulo-1024 counter per <Address 1, AC> tuple starting at 0 and incrementing by 1 for each MMPDU carried in one or more QMFs with Address 1 and ACI fields matching the <Address 1, AC> tuple values corresponding to that counter.

Sequence numbers for QoS (+)Null frames may be set to any value.

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. ~~The~~A receiving QoS STA shall also keep a cache of recently received <Address 2, TID, sequence-number, fragment-number> tuples from QoS Data frames 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 should omit tuples obtained from group addressed or 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 shall omit from the caches all tuples obtained from group addressed data frames and tuples obtained from ATIM frames.

A receiving STA shall reject as a duplicate frame any frame that is not a QoS Data frame in which the Retry bit in the Frame Control field is 1 and that matches an <Address 2, sequence-number, fragment-number> tuple of an entry in the cache that contains tuples of that format, unless the frame is a management frame and the STA is maintaining separate caches for <Address 2, sequence-number, fragment-number> tuples from received management frames. A receiving QoS STA shall also reject as a duplicate frame any QoS Data frame in which the Retry bit in the Frame Control field is 1 and that matches an <Address 2, TID, sequence-number, fragment number> tuple of an entry in the cache that contains tuples of that format. A STA that is maintaining separate caches for <Address 2, sequence-number, fragment-number> tuples from received management frames shall reject as a duplicate frame any management frame that is not a time priority management frame in which the Retry bit in the Frame Control field is 1 and that matches an <Address 2, sequence-number, fragment-number> tuple of an entry in the management cache that contains tuples from frames that are not time priority management frames. A STA that is maintaining separate caches for <Address 2, sequence-number, fragment- number> tuples from received management frames shall reject as a duplicate frame any time priority management frame in which the Retry bit in the Frame Control field is 1 and that matches an <Address 2, sequence-number, fragment-number> tuple of an entry in the cache that contains tuples from time priority management frames. A receiving QoS STA shall also reject as a duplicate frame any QMF in which the Retry bit in the Frame Control field is 1 and that matches an <Address 2, AC, sequence-number, fragment number> tuple of an entry in the cache of tuples obtained from QMFs.

There is a small possibility that a frame may be improperly rejected due to such a match; however, this occurrence would be rare and simply results in a lost frame (similar to an FCS error in other LAN protocols).

NOTE—The receiver STA performs the ACK and (for an AP) PS procedures on all successfully received frames requiring acknowledgment, even if the frame is discarded due to duplicate filtering.

10. MLME

10.23 Wireless network management procedures

10.23.14 Channel usage procedures

Change the 6th paragraph of 10.23.14 as follows:

Upon receipt of a Channel Usage element in the Probe Response or Channel Usage Response frame, the receiving STA may use the following:

— The channel usage information as part of channel selection processing to start a non-infrastructure network or an off-channel TDLS direct link

— The Power Constraint element, if present, as part of determining its maximum transmit power for transmissions for the non-infrastructure network or an off-channel TDLS direct link

— The EDCA Parameter Set element, if present, as part of determining its EDCA parameters for transmissions for the non-infrastructure network or an off-channel TDLS direct link

— The QMF Policy element, if present and dot11QMFActivated is true, as part of determining its classification of management frames for transmissions for the non-infrastructure network or an off-channel TDLS direct link

Insert the following new subclauses at the end of Clause 10:

10.25 Quality-of-service management frame (QMF)

10.25.1 General

10.25.1.1 Overview

A QMF STA shall set dot11QMFActivated and dot11QosOptionImplemented to true. The QMF STA shall assign an access category to each management frame according to the access category assignments indicated in the QMF policy that has been configured using the configuration procedures described in 10.25.2.

A QMF STA shall set the QMFActivated subfield in the Extended Capabilities element to 1.

A management frame shall be transmitted as an IQMF when all five of the following conditions are met:

— The RA of the management frame corresponds to an individual MAC address.

— The frame is transmitted by a QMF STA.

— The transmitting STA has previously received an Extended Capabilities element from the STA corresponding to the RA of the frame being transmitted.

— The most recently received such Extended Capabilities element indicated that the STA is a QoS STA and has the value of 1 in the QMFActivated subfield.

— The frame is not a time priority management frame.

A QMF AP shall transmit a management frame as a GQMF when all three of the following conditions are met:

— The RA of the management frame corresponds to a group MAC address.

— The transmitting STA has received an Extended Capabilities element that has the QMFActivated subfield equal to 1 from every member of the BSS corresponding to the BSSID of the management frame.

— The frame is not a time priority management frame.

A non-AP QMF STA shall transmit a management frame as a GQMF when all three of the following conditions are met:

— The RA of the management frame corresponds to a group MAC address.

— The transmitting STA has received an Extended Capabilities element that has the QMFActivated subfield equal to 1 from its associated AP.

— The frame is not a time priority management frame.

NOTE—This standard assumes all APs within an ESS are configured consistently for QMF service when GQMF has been enabled for use by associated non-AP STAs.

When the QMFActivated subfield is zero in the most recently received Extended Capabilities element from a destination STA, or when an Extended Capabilities element has not been received from a destination STA,

a transmitting QMF STA shall transmit individually addressed management frames to that destination STA using access category AC_VO.

If the QMFActivated subfield in the most recently received Extended Capabilities element from a destination QMF STA is equal to one, but no QMF Policy element has been received from the destination QMF STA, and, if associated, no QMF Policy element has been received from the QMF AP with which the STA is associated, then a QMF STA shall transmit all IQMFs to the destination QMF STA using the default QMF policy access categories defined in Table 10-12. Otherwise, the QMF STA shall transmit individually addressed management frames as defined in the QMF policy included in the QMF Policy element accepted from the destination QMF STA. In either case, the transmitted management frames are IQMFs, and the transmitting QMF STA shall indicate the access category used to transmit the frame in the ACI subfield of the sequence number field.

A QMF STA in an unassociated state shall transmit all group-addresses management frames as non-QMF. An associated QMF STA shall follow the QMF policy dictated by its associated AP for transmitting GQMFs as described in 10.25.2. The specific access category assignments of different management frames within a non-default QMF policy are beyond the scope of this document. The transmitting QMF STA shall indicate the access category used to transmit GQMFs in the ACI subfield of the sequence number field.

Time-priority management frames, when not sent as an immediate response, shall be transmitted using AC_VO.

10.25.1.2 Default QMF policy

The default QMF policy is as defined in Table 10-12. It defines the access category of each management frame based on management subtype value, category value, and action value. QMFs not included in this table shall be assigned an access category AC_BE.

Table 10-12—Default QMF policy

Description	Management Frame Subtype value from Table 8-1	Category value from Table 8-38	Action class	QMF access category
(Re)Association Request/ Response	0000–0011	N/A	N/A	AC_VO
Probe Request (individually addressed	0100	N/A	N/A	AC_VO
Probe Request (group addressed)	0100	N/A	N/A	AC_BE
Probe Response	0101	N/A	N/A	AC_BE
Timing Advertisement	0110	N/A	N/A	AC_BE
Beacon, ATIM, Disassociation, Authentication, Deauthentication	1000–1100	N/A	N/A	AC_VO
Spectrum management	1101	0	0–3	AC_BE
Spectrum management—channel switch announcement	1101	0	4	AC_VO
QoS	1101	1	0–3	AC_VO

Table 10-12—Default QMF policy *(continued)*

Description	Management Frame Subtype value from Table 8-1	Category value from Table 8-38	Action class	QMF access category
DLS	1101	2	0–2	AC_BE
Block Ack	1101	3	0–2	AC_VO
Public	1101	4	0, 1, 3, 5–6, 8–9	AC_BE
Public—DSE deenable-ment, extended channel switch announcement	1101	4	2, 4	AC_VO
Public—measurement pilot	1101	4	7	AC_VO
Public—TDLS Discovery Response	1101	4	14	AC_VO
Radio measurement	1101	5	0–5	AC_BE
Fast BSS Transition	1101	6	0–4	AC_VO
HT	1101	7	0–3	AC_VO
HT	1101, 1110	7	4–7	AC_VO
SA Query	1101	8	0–1	AC_VO
Protected Dual of Public Action	1101	9	1–2, 5–6, 8–9	AC_BE
Protected Dual of Public Action—extended channel switch announcement	1101	9	4	AC_VO
WNM	1101	10	0–24	AC_BE
Unprotected WNM	1101	11	0–1	AC_BE
Mesh Action—HWMP Mesh Path Selection	1101	13	1	AC_VO
Mesh Action—Congestion Control	1011	13	3	AC_VO
Mesh Action	1101	13	0, 2, 4–10	AC_BE
Multihop Action	1101	14	0–1	AC_BE
Self Protected	1101	15	0–5	AC_VI
Reserved (used by WFA)	1101	17	All	AC_BE
Vendor-specific Protected	1101	126	N/A	AC_BE
Vendor-specific	1101	127	N/A	AC_BE

10.25.2 QMF policy advertisement and configuration procedures

10.25.2.1 Overview

QMF policies are exchanged and implemented between two QMF STAs. QMF policy is communicated through the QMF Policy element as described in 8.4.2.122.

A non-AP QMF STA operating in a BSS shall not transmit a QMF Policy frame to an AP.

The access category for a QMF that is transmitted by a non-AP QMF STA to a peer QMF STA shall be determined from the QMF policy received from the peer if a QMF policy has been received from the peer. Otherwise, the default policy shall be used. The access category for a QMF that is transmitted by a QMF AP is determined from the QMF policy configured at that AP.

In a BSS or MBSS, the access category for any management frame may be reconfigured. For example, vendor-specific and vendor-specific protected management frames might be reconfigured to suit the vendor application requirements.

10.25.2.2 QMF policy change in an infrastructure BSS or in an MBSS

A QMF Policy Change frame is transmitted by a QMF STA to request a change to the QMF policy that the requesting QMF STA will use for transmitting management frames to the peer QMF STA in an infrastructure BSS or in an MBSS.

A STA may transmit a QMF Policy Change frame to request a change in the QMF policy for transmitting to a peer STA. A non-AP QMF STA that receives a QMF Policy Change frame may either accept or reject the request. An associated non-AP QMF STA may transmit a QMF Policy Change to the QMF AP in its BSS only if the most recently received Extended Capabilities element from the AP has its QMFReconfiguration-Activated subfield equal to 1. If the AP rejects the request, the associated QMF STA shall not request the same policy reconfiguration from the AP within the lifetime of its association.

An AP shall respond to a QMF Policy Change frame received from an associated STA by transmitting a QMF Policy frame. If the QMFReconfigurationActivated subfield is zero in the Extended Capabilities element in the Beacon frame, an AP that receives a QMF Policy Change frame from an associated STA shall respond with a QMF Policy frame, with Status Code set to 37 (The request has been declined). If the QMFReconfigurationActivated subfield is 1 in the Extended Capabilities element in the Beacon frame, an AP that receives a QMF Policy Change frame from an associated STA shall evaluate the QMF Policy included in the frame, and shall respond to the request with the resulting QMF Policy element and Status Code set to 0 (Successful) if it accepts the policy change, or 37 (The request has been declined) if it rejects the policy change. A QMF AP may transmit a QMF Policy frame with Status Code set to 0 (Successful) to an associated QMF STA without having first received a QMF Policy Change frame from that STA.

If an accept status is received in a QMF Policy frame within dot11QMFPolicyChangeTimeout of having transmitted a QMF Policy Change frame with the same dialog token to the STA that transmitted the QMF Policy frame, then the requesting QMF STA shall transmit any subsequently queued management frames to the peer QMF STA in accordance with the changes to the QMF policy that were indicated in the QMF Policy Change frame.

If a reject status is received in a QMF Policy frame within dot11QMFPolicyChangeTimeout of having transmitted a QMF Policy Change frame with the same dialog token to the STA that transmitted the QMF Policy frame as a response to a QMF Policy Change frame, then the configuration change request is rejected and the requesting QMF STA shall continue to transmit Management frames to the peer QMF STA in accordance with the previously configured QMF policy. The requesting QMF STA shall not transmit a QMF

Policy Change frame with a previously rejected QMF policy to a peer QMF STA within dot11QMFPolicyChangeTimeout from the time the requesting STA received the rejection frame.

If the requesting STA does not receive a QMF Policy frame in response to a QMF Policy Change frame within dot11QMFPolicyChangeTimeout, then the requesting STA shall continue to transmit frames according to the previously configured QMF policy.

If a QMF STA has received an Extended Capabilities element with the QMFReconfigurationActivated subfield equal to zero or has not received an Extended Capabilities element from a destination QMF STA, the QMF STA shall not transmit a QMF Policy Change frame to the destination QMF STA.

A QMF STA in an MBSS or a QMF AP may set dot11QMFReconfigurationActivated to true or false. A non-AP QMF STA in an infrastructure BSS shall set dot11QMFReconfigurationActivated to true and shall set the QMFReconfigurationActivated subfield to one in transmitted (re)association requests. A non-AP QMF STA with dot11QMFReconfiguationActivated equal to true shall accept any received QMF Policy frame from its associated AP. A QMF STA with dot11QMFReconfigurationActivated equal to false shall respond with a QMF Policy frame, with the current QMF Policy element and Status Code set to 37 (The request has been declined).

The QMFReconfigurationActivated subfield shall be set to one in the Extended Capabilities element when dot11QMFReconfigurationActivated is true. The QMFReconfigurationActivated subfield shall be set to zero in the Extended Capabilities element when dot11QMFReconfigurationActivated is false.

The SME of a peer QMF STA uses the MLME-QMFPOLICY primitives (see 6.3.83.2 to 6.3.83.3) to transmit a QMF Policy frame to a peer STA. The SME of a peer STA uses the MLME-QMFPOLICY.request primitive to transmit a QMF Policy frame to a peer STA. The MLME of a peer QMF STA shall set the Dialog Token to 0 and set the Status Code to 0 (Successful) when the QMF Policy frame is transmitted unsolicited to the peer STA.

The SME of a peer QMF STA uses the MLME-QMFPOLICYCHANGE primitives (see 6.3.83.4 to 6.3.83.7) to exchange the QMF Policy Change and QMF Policy frames. The SME of a peer STA uses the MLME-QMFPOLICYCHANGE.request primitive to transmit a QMF Policy Change frame to a peer STA. The value of the dialog token in the MLME-QMFPOLICYCHANGE.request shall be set to a value in the range of 1 to 255.

The SME of the peer STA evaluates the QMF policy and uses the MLME-QMFPOLICYCHANGE.response primitive to transmit a QMF Policy frame to the STA including the result of the QMF policy change. The value of the dialog token in the MLME-QMFPOLICYCHANGE.response shall be set to the value of the dialog token received in the corresponding MLME-QMFPOLICYCHANGE.indication.

When the QMF STA SME receives an MLME-QMFPOLICYCHANGE.confirm or MLME-QMFPOLICY.indication with Result Code of SUCCESS, it shall set the new QMF policy using the MLME-QMFPOLICYSET.request.

10.25.2.3 QMF policy configuration in an infrastructure BSS

A QMF AP shall include the QMF Policy element in Beacon frames that it transmits. Non-AP QMF STAs acquire QMF policy configuration information from QMF Policy elements received in Beacon, Association Response, Reassociation Response, Probe Response, and QMF Policy frames. The interpretation of the QMF Policy element is described in 10.25.3.

An associated QMF STA transmitting QMFs shall transmit those frames in accordance with the QMF policy received from its associated AP in the following order of precedence, from highest to lowest:

— QMF policy defined in an unsolicited QMF Policy frame from the associated QMF AP or the QMF Policy Change frame that resulted in a successful response QMF Policy frame from the associated AP, whichever occurred most recently

— QMF policy defined in the QMF Policy element received in the successful (Re)Association Response frame

All unassociated QMF STAs transmitting management frames to a QMF AP shall transmit those frames to the AP in accordance with the QMF policy in the most recently received Beacon or Probe Response frame from that AP. If no frame containing a QMF Policy element has been received from the AP prior to the transmission of the management frame(s), then the management frame(s) shall be transmitted using the access categories of the default QMF policy defined in Table 10-12.

A QMF STA shall transmit all management frames that are individually addressed to non-QMF STAs using access category AC_VO.

A QMF AP shall set a QMF policy for the transmission of QMFs to its associated STAs. The QMF policy used by the AP for transmission of QMFs to associated STAs is not required to be the same as the QMF policy it advertises.

If the QMFReconfigurationActivated subfield is equal to one in the Extended Capabilities element of the Beacon or Probe Response frame transmitted by the AP, an associated QMF STA may use the QMF Policy Change frame to request a change in its existing QMF policy.

10.25.2.4 QMF policy configuration in an IBSS or OCB

QMF STAs in an IBSS or OCB shall use the default QMF policy for all individually addressed management frames transmitted to other QMF STAs within the IBSS or OCB.

10.25.2.5 QMF policy configuration in an MBSS

A QMF STA operating in an MBSS shall set the QMFActivated subfield in the Extended Capabilities element to true. The Mesh Beacon shall not include a QMF Policy element. Within an MBSS, the QMF policy shall be set on a per link basis between two QMF STAs.

The QMF Policy Change and QMF Policy frames are used by QMF STAs in an MBSS to configure QMF policy. See 10.25.2.2.

A QMF STA shall always accept the QMF policy from the QMF Policy frame transmitted by the peer QMF STA and shall transmit all individually addressed management frames destined to the peer QMF STA using the received QMF policy.

A QMF STA may request a change in the QMF policy from a peer QMF STA by transmitting a QMF Policy Change to the peer QMF STA. The peer QMF STA may accept or reject this change request. If the peer QMF STA accepts the change, it shall respond with a QMF Policy frame with Status Code set to 0 (Successful) and the QMF STA shall transmit IQMFs using the new QMF policy to the peer QMF STA. If the peer QMF STA rejects the change, it shall respond with QMF Policy frame with Status Code set to 37 (The request has been declined) and the QMF STA shall continue transmitting IQMFs according to the previously configured QMF policy.

If a QMF STA does not receive a QMF Policy frame from a peer QMF STA, it shall transmit management frames to that peer STA using the default QMF policy.

QMF STAs in an MBSS shall not include policies for group addressed management frames in the QMF Policy Config Request.

10.25.3 Interpreting QMF access categories

The QMF Policy element, as defined in 8.4.2.122, indicates the transmit access categories of different management frames. A QMF Policy element with Length field of value 1 means that the access category of all management frames is as defined in the default QMF policy in Table 10-12.

When the value of the Individually Addressed subfield is 1, then the QACM applies to IQMFs. When the value of the Group Addressed subfield is 1, then the QACM applies to GQMFs. A STA shall not transmit a QMF Policy element with both the Individually Addressed and Group Addressed subfields set to 0 in any of the included QACM subfields.

The QMF Policy element contains zero or more QACM fields. When included in the QMF Policy element, each QACM field indicates the access category of a group of management frames. Using the description from Table 10-13, access categories for all management frames belonging to either a given subtype or a given action category may be indicated in a single QACM field. When multiple action frames of the same Category are to be mapped to the same Access Category, this is indicated by setting multiple bits in the Action Value Bitmap. For example, setting Bit 0 and Bit 1 indicates Event Request/Response frames when the Management Frame Subtype subfield refers to management frames of subtype Action and the Category Value subfield refers to the WNM category. The QACM field also may be used to indicate the access category of a single management frame subtype.

A QMF STA that received a QMF Policy element from its associated QMF AP shall discard any previously received QMF Policy elements. If a management frame is indicated in multiple QACM fields, the access category of the management frame is determined by the access category defined in the last QACM field within the QMF Policy that contains the access category assignment of the corresponding management frame. For example, if an QACM field sets the entire WNM category to access category AC_BE and a later QACM field sets Event Request/Report of WNM category to AC_BK, then all action frames of WNM category are transmitted using access category AC_BE with the exception of Event Requests/Reports, which are transmitted using access category AC_BK.

Table 10-13—QMF policy description for valid combination of optional fields in the QACM field

QACM Field Length subfield	Action Frame Category	Action Value Bitmap subfield	Description
0	Not included	Not included	Policy to be applied to all management frames of the corresponding subtype
1	Included	Not included	Policy to be applied to all Action frames of corresponding category value belonging to the management subtype frames
≥ 2	Included	Included	Policy to be applied only to Action frames indicated via the action value bitmap for management frames of the subtype indicated in Management Frame Subtype subfield and category value indicated in Action Frame Category subfield in corresponding QACM field

11. Security

11.4 RSNA confidentiality and integrity protocols

11.4.3 CTR with CBC-MAC Protocol (CCMP)

11.4.3.3 CCMP cryptographic encapsulation

11.4.3.3.4 Construct CCM nonce

Change the first list item after the second paragraph of this clause as follows:

The Nonce field has an internal structure of Nonce Flags || A2 || PN ("||" is concatenation), where

— ~~The Priority subfield of the Nonce Flags field shall be set to the fixed value 0 when there is no QC field present in the MPDU header. When the QC field is present, bits 0 to 3 of the Priority subfield shall be set to the value of the QC TID (bits 0 to 3 of the QC field).~~ If the Type field of the Frame Control field is 10 (Data frame) and there is a QC field present in the MPDU header, bits 0 to 3 of the Priority subfield of the Nonce Flags field shall be set to the value of the QC TID (bits 0 to 3 of the QC field). If the Type field of the Frame Control field is 00 (Management frame), and the frame is a QMF, the Priority subfield of the Nonce Flags field shall be set to the value in the ACI subfield of the Sequence Number field. Otherwise, the Priority subfield of the Nonce Flags field shall be set to the fixed value 0.

11.4.3.4 CCMP decapsulation

11.4.3.4.4 PN and replay detection

Change the clause as follows:

f) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust management frames that do not use the QMF service and shall use the PN from the received frame to detect replays. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed Robust Management frames that use the QMF service. The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame~~value~~. The transmitter shall preserve the order of protected robust management frames that are transmitted ~~sent~~ to the same DA without the QMF service. When the QMF service is used, the transmitter shall not reorder robust IQMFs within an AC when the frames are transmitted to the same RA.

g) If dot11RSNAProtectedManagementFramesActivated is true and dot11MeshSecurityActivated is true, the recipient shall maintain a single replay counter for received group addressed robust management frames that do not use the QMF service and shall use the PN from the received frame to detect replays. If dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received group addressed Robust Management frames that use the QMF service. The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the value of the management frame replay counter that corresponds to the ACI of the frame. The transmitter shall preserve the order of protected robust management frames transmitted

to the same DA without the QMF service. When the QMF service is used, the transmitter shall not reorder robust GQMFs within an AC when the frames are transmitted to the same RA.

h) ~~g)~~ The receiver shall discard MSDUs, A-MSDUs, and MMPDUs whose constituent MPDU PN values are not sequential. A receiver shall discard any MPDU that is received with its PN less than or equal to the replay counter. When discarding a frame, the receiver shall increment by 1 the value of dot11RSNAStatsCCMPReplays for data frames or dot11RSNAStatsRobustMgmtCCMPReplays for robust management frames.

i) ~~h)~~ For MSDUs or A-MSDUs sent using the Block Ack feature, reordering of received MSDUs or A-MSDUs according to the Block Ack receiver operation (described in 9.21.4) is performed prior to replay detection.

11.4.4 Broadcast/Multicast Integrity Protocol (BIP)

11.4.4.4 BIP replay protection

Insert the following text at the end of 11.4.4.4:

When dot11QMFActivated is true, the receiver shall maintain an additional replay counter for each ACI for received group-addressed Robust Management frames that use QMF. The receiver shall use the ACI encoded in the Sequence Number field of received GQMFs protected by BIP to select the replay counter to use for the received frame, and shall use the IPN from the received frame to detect replays.

11.4.4.5 BIP transmission

Change 11.4.4.5 as follows:

When a STA transmits a protected group addressed robust management frame, it shall

a) Select the IGTK currently active for transmission of frames to the intended group of recipients and construct the MME (see 8.4.2.57) with the MIC field masked to zero and the KeyID field set to the corresponding IGTK KeyID value. If the frame is not a GQMF, the transmitting STA~~The transmitter~~ shall insert a monotonically increasing non-negative integer into the MME IPN field. If the frame is a GQMF, then the transmitting STA shall maintain a 48-bit counter for use as the IPN, the counter shall be incremented for each GQMF until the two least significant bits of the counter match the ACI of the AC that is used to transmit the frame, and the counter value shall be inserted into the MME IPN field of the frame.

11.4.4.6 BIP reception

Change 11.4.4.6 as follows:

When a STA with management frame protection negotiated receives a group addressed robust management frame protected by BIP, it shall

a) Identify the appropriate IGTK key and associated state based on the MME KeyID field. If no such IGTK exists, silently drop the frame and terminate BIP processing for this reception.

b) Perform replay protection on the received frame. The receiver shall interpret the MME IPN field as a 48-bit unsigned integer.

   1) If the frame is not a GQMF, the receiver~~It~~ shall compare this MME IPN integer value to the value of the receive replay counter for the IGTK identified by the MME Key ID field. If the integer value from the received MME IPN field is less than or equal to the replay counter value for this IGTK, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

2) If the frame is a GQMF, the receiver shall compare this MME IPN integer value to the value of the receive replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame. If the integer value from the received MME IPN field is less than or equal to the replay counter value for this IGTK and AC, the receiver shall discard the frame and increment the dot11RSNAStatsCMACReplays counter by 1.

If the received frame is not discarded after comparison of the MME IPN to the replay counter, ~~T~~the receiver shall extract and save the received MIC value, and compute the AES-128-CMAC over the concatenation of (AAD || Management Frame Body including MME) with the MIC field masked to 0 in the MME. If the result does not match the received MIC value, then the receiver shall discard the frame and increment the dot11RSNAStatsCMACICVErrors counter by 1. If replay protection fails, terminate BIP processing for this reception.

c) ~~If the replay protection succeeds, c~~Compute AAD for this management frame, as specified in 11.4.4.3.

d) Extract and save the received MIC value, and compute the AES-128-CMAC over the concatenation of (AAD || Management Frame Body || MME) with the MIC field masked to 0 in the MME. If the result does not match the received MIC value, then the receiver shall discard the frame, ~~and~~ increment the dot11RSNAStatsCMACICVErrors counter by 1, and terminate BIP processing for this reception.

e) Update the replay counter for the IGTK identified by the MME Key ID field with the integer value of the MME IPN field if the frame is not a GQMF.

f) Update the replay counter for the IGTK identified by the MME Key ID field and the AC represented by the value of the ACI subfield of the received frame with the integer value of the MME IPN field if the frame is a GQMF.

If management frame protection is negotiated, group addressed robust management frames that are received without BIP protection shall be discarded.

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 new abbreviation in alphabetical order in B.2.2:

QMF quality-of-service management frame

B.4 PICS proforma—IEEE Std 802.11-2012[2]

B.4.3 IUT configuration

Change the entry for CF12 in the IUT configuration table as follows:

Item	IUT configuration	References	Status	Support
*CF12	Quality of service (QoS) supported	9.19, 9.21, 4.3.10, 4.3.15.3	O ~~(CF16 or CF21): M~~ (CF16 OR CF21 OR CF22):M	Yes ☐ No ☐ N/A ☐

Insert the following new entry to the end of the IUT configuration table:

Item	IUT configuration	References	Status	Support
*CF22	Is QMF policy supported?	10.25	O	Yes ☐ No ☐ N/A ☐

[2]*Copyright release for PICS proforma:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

Insert a new subclause at the end of B.4 as follows:

B.4.24 QMF extensions

Item	Protocol capability	References	Status	Support
QMF1	Extended Capabilities element	8.4.2.29	CF22:M	Yes ☐ No ☐ N/A ☐
QMF2	Channel access procedures for QMFs	9.2.4.2	CF22:M	Yes ☐ No ☐ N/A ☐
QMF3	Duplicate detection and recovery for QMFs	9.3.2.10	CF22:M	Yes ☐ No ☐ N/A ☐
QMF4	QMF policy Configuration	10.25.2	CF22:M	Yes ☐ No ☐ N/A ☐
QMF5	Interpreting QMF priority	10.25.3	CF22:M	Yes ☐ No ☐ N/A ☐
QMF6	CCMP cryptographic encapsulation for QMFs	11.4.3.3	(CF22 AND PC34.1.10):M	Yes ☐ No ☐ N/A ☐

Annex C

(normative)

ASN.1 encoding of the MAC and PHY MIB

C.3 MIB Detail

Change the end of the "Dot11StationConfigEntry" of the "dot11StationConfig TABLE" as follows:

```
    dot11RejectUnadmittedTraffic          TruthValue,
    dot11BSSBroadcastNullCount            Unsigned32,
    dot11QMFActivated                     TruthValue,
    dot11QMFReconfigurationActivated      TruthValue,
    dot11QMFPolicyChangeTimeout           Unsigned32
   }
```

Insert the following elements at the end of the dot11StationConfigTable element definitions:

```
dot11QMFActivated 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.
          For an AP, changes take effect for the next MLME-START.request
          primitive. For a non-AP STA that is not associated and is not a
          member of an IBSS, changes take effect as soon as practical in
          the implementation. For a non-AP STA that is associated,
          changes take effect at the end of the lifetime of the
          association. For a STA that is a member of an IBSS, changes
          take effect for the next MLME-START.request primitive or MLME-
          JOIN.request primitive.
          This attribute indicates whether the entity is QMF enabled or
          disabled."
     DEFVAL { false }
     ::= { dot11StationConfigEntry 137 }

dot11QMFReconfigurationActivated 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
          or MLME-JOIN.request primitive.
          The purpose of dot11QMFReconfigurationActivated is to allow an
          SME to accept a QMF Policy Change request from another STA and
          respond with a QMF Policy frame."
     DEFVAL { false }
```

```
    ::= { dot11StationConfigEntry 138 }

dot11QMFPolicyChangeTimeout OBJECT-TYPE
    SYNTAX Unsigned32
    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 as soon as practical in the implementation.
        This attribute indicates the minimum number of TUs that a STA
        waits to receive a response to a QMF Policy Change request
        before declaring that the request has failed and also the
        number of TUs that a STA must wait after it has received a
        rejection to a QMF Policy Change request before issuing a
        repeat QMF Policy Change request to the same destination STA."
    DEFVAL { 5000 }
    ::= { dot11StationConfigEntry 139 }
```

Insert the following compliance statement after the "Compliance Statements – WNM" section:

```
-- ************************************************************
-- * Compliance Statements - QMF
-- ************************************************************

dot11QMFComplianceGroup OBJECT-GROUP
    OBJECTS {
        dot11QMFActivated,
        dot11QMFReconfigurationActivated,
        dot11QMFPolicyChangeTimeout }
    STATUS current
    DESCRIPTION
        "This object group provides the objects from the IEEE 802.11
        MIB required to manage QoS Management Frame functionality."
    ::= { dot11Groups 63 }

dot11QMFCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "This object class provides the objects from the IEEE 802.11
        MIB required to manage QoS Management Frame functionality."
        MODULE -- this module
    MANDATORY-GROUPS {
        dot11QMFComplianceGroup }
    ::= { dot11Compliances 6 }
```

