

**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 9: Interworking with External
Networks**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

25 February 2011

IEEE Std 802.11u™-2011
(Amendment to IEEE Std 802.11™-2007
as amended by IEEE Std 802.11k™-2008,
IEEE Std 802.11r™-2008, IEEE Std 802.11y™-2008,
IEEE Std 802.11w™-2009, IEEE Std 802.11n™-2009,
IEEE Std 802.11p™-2010, IEEE Std 802.11z™-2010,
and IEEE Std 802.11v™-2011)

IEEE Std 802.11u™-2011
(Amendment to IEEE Std 802.11™-2007
as amended by IEEE Std 802.11k™-2008,
IEEE Std 802.11r™-2008, IEEE Std 802.11y™-2008,
IEEE Std 802.11w™-2009, IEEE Std 802.11n™-2009,
IEEE Std 802.11p™-2010, IEEE Std 802.11z™-2010,
and IEEE Std 802.11v™-2011)

**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 9: Interworking with External
Networks**

Sponsor

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

Approved 2 February 2011

IEEE-SA Standards Board

Approved 4 August 2011

American National Standards Institute

Abstract: This amendment specifies enhancements to the IEEE 802.11 medium access control (MAC) that support wireless local area network (WLAN) interworking with external networks. It enables higher layer functionalities to provide overall end-to-end solutions. The main goals of this amendment are aiding network discovery and selection, enabling information transfer from external networks, enabling emergency services, and interfacing subscription service provider networks (SSPNs) to IEEE 802.11 networks that support interworking with external networks.

Keywords: E911, emergency alert system, emergency services, generic advertisement service, interface, interworking, interworking with external networks, media-independent handover, MIH, network advertisement, network discovery, network selection, QoS mapping, SSP, SSPN, subscriber service provider, wireless LAN

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

Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 25 February 2011. 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.

The term 3GPP is a registered trademark of the European Telecommunications Standards Institute (ETSI).

PDF: ISBN 978-0-7381-6538-7 STD97071
Print: ISBN 978-0-7381-6539-4 STDPD97071

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.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The 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 the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the 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. The 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 this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, 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 herein 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 five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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 this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. 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 interpretation of the 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, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments on standards and requests for interpretations should be submitted to the following address:

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

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.

Introduction

This introduction is not part of IEEE Std 802.11u-2011, 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 9: Interworking with External Networks.

The interworking with external networks is a key enabler to allow IEEE 802.11 devices to interwork with external networks, as typically found in hotspots or other public networks irrespective of whether the service is subscription-based or free.

The interworking service aids network discovery and selection, which in turn enables information transfer from external networks and enables emergency services. It provides information to the stations (STAs) about the networks prior to association. Interworking will not only help users within home, enterprise, and public access markets, but also assist manufacturers and operators to provide common components and services for IEEE 802.11 customers.

The interworking service addresses medium access control (MAC) layer enhancements that allow higher layer functionality to provide the overall end-to-end interworking solution.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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 Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, 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 at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/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/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence for validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these 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. Other Essential Patent Claims may exist for which a statement 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 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 draft Standard was completed, the IEEE 802.11 Working Group had the following membership:

Bruce Kraemer, *Chair*
Adrian Stephens and Jon Walter Rosdahl, *Vice Chairs*
Stephen McCann, *Secretary*

Osama S. Aboulmagd
Santosh P. Abraham
Tomoko Adachi
Carlos H. Aldana
Gary Anwyl
Lee R. Armstrong
Alex Ashley
Malik Audeh
Geert A. Awater
David Bagby
Michael Bahr
Fan Bai
Gabor Bajko
Raja Banerjee
Kaberi Banerjee
John R. Barr
Gal Basson
Tuncer Baykas
John L. Benko
Mathilde Benveniste

Daniel R. Borges
Anthony Braskich
Joseph Brennan
Walter Buga
George Bumiller
Nancy Cam-Winget
Necati Canpolat
Javier Cardona
Philippe Chambelin
Douglas S. Chan
Clint F. Chaplin
Jiunn-Tsair Chen
Lidong Chen
Minho Cheong
Woong Cho
Jee-Yon Choi
Nakjung Choi
Liwen Chu
Terry L. Cole
Charles I. Cook

Carlos Cordeiro
Xavier Perez Costa
David E. Cypher
Marc De Courville
Rolf J. de Vegt
Theodorus Denteneer
Jeremy deVries
Susan Dickey
John Dorsey
Roger P. Durand
Srinivasa Duvvuri
Donald E. Eastlake III
Peter Ecclesine
Stephen P. Emeott
Marc Emmelmann
Darwin Engwer
Vinko Erceg
Stefan Fechtel
Matthew J. Fischer
Wayne K. Fisher

Wen Gao
 Matthew S. Gast
 James P. K. Gilb
 Jeffrey Gilbert
 Reinhard Gloger
 Michelle Gong
 David Goodall
 Sudheer A. Grandhi
 Mark Grodzinsky
 Jianlin Guo
 Mark Hamilton
 Christopher J. Hansen
 Hiroshi Harada
 Dan N. Harkins
 Brian D. Hart
 Chris Hartman
 Amer A. Hassan
 Vegard Hassel
 Robert F. Heile
 Guido R. Hiertz
 Garth D. Hillman
 Seungeun Hong
 Naoki Honma
 Wendong Hu
 Robert Y. Huang
 Tian-Wei Huang
 David Hunter
 Akio Iso
 Wynona Jacobs
 Hongseok Jeon
 Yeonkwon Jeong
 Lusheng Ji
 Daniel Jiang
 Sunggeun Jin
 V. K. Jones
 Padam Kafle
 Carl W. Kain
 Naveen K. Kakani
 Shuzo Kato
 Douglas Kavner
 Richard H. Kennedy
 John Kenney
 Stuart J. Kerry
 Joonsuk Kim
 Kyeongpyo Kim
 Yongsun Kim
 Youngsoo Kim
 Yunjoo Kim
 Jarkko Knecht
 Mark M. Kobayashi
 Fumihide Kojima
 Tom Kolze
 Thomas M. Kurihara
 Joseph Kwak
 Hyoungjin Kwon
 Ismail Lakkis
 Paul Lambert
 Zhou Lan
 Jeremy A. Landt
 Joseph P. Lauer
 Wooyong Lee
 Yuro Lee
 Sheung Li

Hang Liu
 Pei Liu
 Peter Loc
 Hui-Ling Lou
 Bradley Lynch
 Jakub Majkowski
 Alastair Malarky
 Jouni K. Malinen
 Alexander Maltsev
 Hiroshi Mano
 Bill Marshall
 Roman M. Maslennikov
 Justin P. McNew
 Sven Mesecke
 Robert R. Miller
 Michael Montemurro
 Rajendra T. Moorti
 Hitoshi Morioka
 Yuichi Morioka
 Daniel Camps Mur
 Peter Murray
 Andrew Myles
 Yukimasa Nagai
 Kengo Nagata
 Hiroki Nakano
 Sai Shankar Nandagopalan
 Chiu Ngo
 Paul Nikolich
 Eero Nikula
 Richard H. Noens
 Jisung Oh
 Jong-Ee Oh
 Youko Omori
 Satoshi Oyama
 Richard H. Paine
 Arul Durai Murugan Palanivelu
 Changmin Park
 Minyoung Park
 Vijaykumar Patel
 Bemini Hennadige 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
 Vinuth Rai
 Ali Raissinia
 Harish Ramamurthy
 Stephen G. Rayment
 Ivan Reede
 Alex Reznik
 Randal Roebuck
 Richard Roy
 Alexander Safonov

Kazuyuki Sakoda
 Hemanth Sampath
 Donald Schultz
 Jean Schwoerer
 Yongho Seok
 Huairong Shao
 Stephen J. Shellhammer
 Ian Sherlock
 Kai Shi
 Francois Simon
 Graham Kenneth Smith
 Matt Smith
 Kapil Sood
 Vinay Sridhara
 Robert Stacey
 Dorothy Stanley
 David S. Stephenson
 Carl R. Stevenson
 John Stine
 Guenael T. Strutt
 Chin-Sean Sum
 Arash Tabibiazar
 Eiji Takagi
 Mineo Takai
 Yasushi Takatori
 Teik-Kheong Tan
 Allan Thomson
 Jerry Thrasher
 Eric Tokubo
 Ichihiko Toyoda
 Jason Trachewsky
 Solomon B. Trainin
 Jean Tsao
 Masahiro Umehira
 Richard D. J. Van Nee
 Allert Van Zelst
 Prabodh Varshney
 Ganesh Venkatesan
 Dalton T. Victor
 George A. Vlantis
 Jesse R. Walker
 Chao-Chun Wang
 Junyi Wang
 Qi Wang
 Craig D. Warren
 Fujio Watanabe
 Menzo M. Wentink
 Frank Whetten
 James Worsham
 Harry R. Worstell
 Fonchi Wu
 Takeshi Yamamoto
 James Yee
 Peter Yee
 Su Khiong Yong
 Seiji Yoshida
 Christopher Young
 Artur Zaks
 Hongyuan Zhang
 Shiwei Zhao
 Chunhui Zhu

The following were officers of Task Group u:

Stephen McCann, *Chair*
Matthew S. Gast and Dave Stephenson, *Secretary*
Necati Canpolat, *Technical Editor*

Contributions to this amendment were received from the following individuals:

Osama S. Aboulmagd	Stefano Faccin	Andrew McDonald
Alex Ashley	Lars Falk	Liangyao Mo
Malik Audeh	Matthew J. Fischer	Patrick Mo
Gabor Bajko	Matthew S. Gast	Michael Montemurro
Kaberi Banerjee	Josh Graessley	Andrew Myers
Farooq Bari	Wolfgang Groeting	Bob O'Hara
Moussa Bavafa	Shu Guiming	Henry Ptasinski
Colin Blanchard	Vivek Gupta	Richard Roy
Daniel R. Borges	Dongwoon Hahn	Marian Rudolf
George Bumiller	Brian D. Hart	Ajoy Singh
Nancy Cam-Winget	Eleanor Hepworth	Srinivas Sreemanthula
Necati Canpolat	Frans Hermodsson	Dorothy Stanley
Angelo Centonza	Ulises Olvera-Hernandez	Adrian Stephens
Clint F. Chaplin	Yasuhiko Inoue	Dave Stephenson
Hong Cheng	Jari Jokela	Allan Thomson
Liwen Chu	Eunkyo Kim	Ganesh Venkatesan
David E. Cypher	Ronny Kim	Qi Wang
Sabine Demel	Jouni Korhonen	Michael Williams
Roger P. Durand	Celine Liu	Qiaobing Xie
Peter Ecclesine	Alastair Malarky	Sihoon Yang
Jon Edney	Jouni Malinen	Zhonghui Yao
Mike Ellis	Bill Marshall	Amy Zhang
Stephen P. Emeott	Stephen McCann	Ding Zhiming
Darwin Engwer		

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

Thomas Alexander	Thomas Dineen	Atsushi Ito
Richard Alfvén	Roger P. Durand	Raj Jain
Butch Anton	Sourav Dutta	Tal Kaitz
Danilo Antonelli	Lester Eastwood	Naveen K. Kakani
Lee R. Armstrong	Richard Eckard	Shinkyō Kaku
Arthur Astrin	Wayne K. Fisher	Chol Kang
David Bagby	C. Fitzgerald	Piotr Karocki
Gabor Bajko	Andre Fournier	Ruediger Kays
Raja Banerjee	Avraham Freedman	Stuart J. Kerry
Harry Bims	Devon Gayle	Yongbum Kim
Gennaro Boggia	Pieter-Paul Giesberts	Yongho Kim
George Bumiller	Reinhard Gloger	Jarkko Knecht
William Byrd	Joel Goergen	Bruce Kraemer
Peter J. Calderon	David Goodall	Thomas M. Kurihara
Juan Carreon	Sudheer A. Grandhi	Paul Lambert
Jon Caswell	Ron Greenhalgh	Jeremy A. Landt
Douglas S. Chan	Randall Groves	Charles Lennon
Clint F. Chaplin	Vivek Gupta	Daniel Levesque
Yung-Mu Chen	C. Guy	Zexian Li
Hong Cheng	Christopher J. Hansen	Jan-Ray Liao
Keith Chow	Marco Hernandez	Arthur Light
Charles I. Cook	Oliver Hoffmann	Daniel Lubar
Todor Cooklev	Wendong Hu	William Lumpkins
Joseph Decuir	David Hunter	Greg Luri
Wael Diab	Akio Iso	Bradley Lynch
		Elvis Maculuba

Alastair Malarkey
Jouni Malinen
Mark Maloney
Stephen McCann
Gary Michel
Robert R. Miller
Apurva Mody
Michael Montemurro
Rick Murphy
Peter Murray
Andrew Myles
Michael S. Newman
Kevin Noll
John Notor
Satoshi Obara
Robert O'Hara
Satoshi Oyama
Stephen Palm
James E. Petranovich
Subburajan Ponnuswamy
Michael Probasco

Rudy Rawlins
Ivan Reede
Maximilian Riegel
Robert Robinson
Randal Roebuck
Benjamin Rolfe
Jon Walter Rosdahl
Richard Roy
Rashid Saeed
Randall Safier
John Santhoff
John Sargent
Peter Saunderson
Bartien Sayogo
Michael Seaman
Yongho Seok
Ian Sherlock
Gil Shultz
Kapil Sood
Amjad Soomro
Manikantan Srinivasan
Dorothy Stanley

Thomas Starai
Adrian Stephens
Walter Struppler
Mark Sturza
Masahiro Takagi
Patricia Thaler
Allan Thomson
Solomon Trainin
Mark-Rene Uchida
Dmitri Varsanofiev
Prabodh Varshney
Ganesh Venkatesan
George A. Vlantis
Stanley Wang
Fujio Watanabe
Menzo M. Wentink
Ludwig Winkel
James Worsham
Harry R. Worstell
Oren Yuen
Paolo Zangheri

When the IEEE-SA Standards Board approved this amendment on 2 February 2011, it had the following membership:

Robert M. Grow, *Chair*
Richard H. Hulett, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Karen Bartleson
Victor Berman
Ted Burse
Clint F. Chaplin
Andy Drozd
Alexander Gelman
Jim Hughes

Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Hung Ling
Oleg Logvinov
Ted Olsen

Ronald C. Petersen
Thomas Prevost
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Don Wright

*Member Emeritus

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

Satish Aggarwal, NRC Representative
Richard DeBlasio, DOE Representative
Michael Janezic, NIST Representative

Michelle Turner
IEEE Standards Program Manager, Document Development

Michael K. Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1.	Overview.....	2
1.2	Purpose.....	2
2.	Normative references.....	2
3.	Definitions	2
4.	Abbreviations and acronyms	4
5.	General description.....	5
5.2	Components of the IEEE 802.11 architecture	5
5.2.13	Subscription service provider network (SSPN) interface	5
5.4	Overview of the services.....	6
5.4.8	Interworking with external networks	6
5.7	Reference model	6
5.7.1	General.....	6
5.7.2	Interworking reference model.....	7
5.9	Generic advertisement service (GAS)	8
6.	MAC service definition	9
6.1	Overview of MAC services	9
6.1.5	MAC data service architecture	9
6.2	Detailed service specification	11
6.2.1	MAC data services.....	11
6.2.1.1	MA-UNITDATA.request	11
6.2.1.2	MA-UNITDATA.indication	12
6.2.1.3	MA-UNITDATA.confirm	14
7.	Frame formats	14
7.1	MAC frame formats.....	14
7.2	Format of individual frame types.....	14
7.2.3	Management frames.....	14
7.2.3.1	Beacon frame format	14
7.2.3.4	Association Request frame format.....	15
7.2.3.5	Association Response frame format	15
7.2.3.6	Reassociation Request frame format	16
7.2.3.7	Reassociation Response frame format	16
7.2.3.8	Probe Request frame format	16
7.2.3.9	Probe Response frame format.....	16
7.3	Management frame body components.....	17
7.3.1	Fields that are not information elements.....	17
7.3.1.7	Reason Code field.....	17
7.3.1.9	Status Code field.....	17
7.3.1.33	GAS Query Response Fragment ID field	18
7.3.1.34	Venue Info field	18
7.3.2	Information elements	22
7.3.2.27	Extended Capabilities information element.....	22
7.3.2.92	Interworking information element	23

7.3.2.93	Advertisement Protocol element.....	24
7.3.2.94	Expedited Bandwidth Request information element	26
7.3.2.95	QoS Map Set information element	27
7.3.2.96	Roaming Consortium information element	28
7.3.2.97	Emergency Alert Identifier information element.....	29
7.3.4	Access Network Query Protocol (ANQP) elements.....	30
7.3.4.1	ANQP Query list.....	31
7.3.4.2	ANQP Capability list.....	31
7.3.4.3	Venue Name information.....	32
7.3.4.4	Emergency Call Number information.....	33
7.3.4.5	Network Authentication Type information.....	34
7.3.4.6	Roaming Consortium list	35
7.3.4.7	ANQP vendor-specific list	36
7.3.4.8	IP Address Type Availability Information	36
7.3.4.9	NAI Realm list	37
7.3.4.10	3GPP Cellular Network information	41
7.3.4.11	AP Geospatial Location element	41
7.3.4.12	AP Civic Location element.....	42
7.3.4.13	AP Location Public Identifier URI element	42
7.3.4.14	Domain Name list element	42
7.3.4.15	Emergency Alert URI information	43
7.3.4.16	Emergency NAI element	43
7.4	Action frame format details	44
7.4.1	Spectrum management action details	44
7.4.2	QoS Action frame details.....	44
7.4.2.1	ADDTS Request frame format	44
7.4.2.2	ADDTS Response frame format.....	45
7.4.2.5	QoS Map Configure frame format.....	45
7.4.7	Public Action details.....	46
7.4.7.1	Public Action frames	46
7.4.7.13	GAS Initial Request frame format	46
7.4.7.14	GAS Initial Response frame format.....	47
7.4.7.15	GAS Comeback Request frame format	48
7.4.7.16	GAS Comeback Response frame format	49
7.4.9	SA Query Action frame details.....	50
7.4.9a	Protected Dual of Public Action details.....	50
7.4.9a.1	Protected Dual of Public Action frames	50
8.	Security	51
8.1.6	Emergency service establishment in an RSN	51
9.	MAC sublayer functional description.....	51
9.2	DCF.....	51
9.2.7	Broadcast and multicast MPDU transfer procedure	51
9.9	HCF.....	51
9.9.3.1	Contention-based admission control procedures	51
9.9.3.2	Controlled-access admission control	52
10.	Layer management.....	52
10.3	MLME SAP Interface	52
10.3.2	Scan.....	52

10.3.2.1	MLME-SCAN.request	52
10.3.6	Associate	53
10.3.6.1	MLME-ASSOCIATE.request	53
10.3.6.2	MLME-ASSOCIATE.confirm	54
10.3.6.4	MLME-ASSOCIATE.response	55
10.3.7	Reassociate	55
10.3.7.1	MLME-REASSOCIATE.request	55
10.3.7.2	MLME-REASSOCIATE.confirm	56
10.3.7.4	MLME-REASSOCIATE.response	57
10.3.10	Start	58
10.3.10.1	MLME-START.request	58
10.3.24	TS management interface	59
10.3.24.1	MLME-ADDTS.request	59
10.3.24.2	MLME-ADDTS.confirm	59
10.3.24.3	MLME-ADDTS.indication	60
10.3.24.4	MLME-ADDTS.response	61
10.3.74	Network discovery and selection support	62
10.3.74.1	MLME-GAS.request	62
10.3.74.2	MLME-GAS.confirm	63
10.3.74.3	MLME-GAS.indication	64
10.3.74.4	MLME-GAS.response	65
10.3.75	Protected dual of network discovery and selection support	66
10.3.75.1	MLME-PDGAS.request	66
10.3.75.2	MLME-PDGAS.confirm	67
10.3.75.3	MLME-PDGAS.indication	68
10.3.75.4	MLME-PDGAS.response	68
10.3.76	QoS Map Set element management	69
10.3.76.1	MLME-QoSMap.request	70
10.3.76.2	MLME-QoSMap.indication	70
11.	MLME	71
11.1	Synchronization	71
11.1.3	Acquiring synchronization, scanning	71
11.1.3.2	Active scanning	71
11.3	STA authentication and association	72
11.3.2	Association, reassociation, and disassociation	72
11.3.2.1	STA association procedures	72
11.3.2.2	AP association procedures	72
11.3.2.3	STA reassociation procedures	72
11.3.2.4	AP reassociation procedures	72
11.4	TS Operation	72
11.4.1	Introduction	72
11.4.3	TS lifecycle	73
11.4.4	TS setup	73
11.7	DLS operation	74
11.7.1.2	Setup procedure at the AP	74
11.23	WLAN interworking with external networks procedures	75
11.23.1	General	75
11.23.2	Interworking capabilities and information	75
11.23.3	Interworking procedures: generic advertisement service (GAS)	75
11.23.3.1	GAS Protocol	76
11.23.3.2	ANQP procedures	83
11.23.4	Interworking procedures: IEEE 802.21 MIH support	86

11.23.5	Interworking procedures: interactions with SSPN.....	86
11.23.5.1	General operation.....	86
11.23.5.2	Authentication and cipher suites selection with SSPN.....	87
11.23.5.3	Reporting and session control with SSPN	87
11.23.6	Interworking procedures: emergency services support	88
11.23.7	Interworking procedures: emergency alert system (EAS) support.....	89
11.23.8	Interworking procedures: support for the advertisement of roaming consortiums.....	90
11.23.9	Interworking procedures: support for QoS mapping from external networks.....	90
11A	Fast transition.....	91
11A.11	Resource request procedures.....	91
11A.11.2	Resource information container	91
11A.11.3	Creation and handling of a resource request.....	92
11A.11.3.1	STA procedures	92
11A.11.3.2	AP procedures	92
11B	MAC state generic convergence function (MSGCF)	92
11B.1	Overview of the convergence function	92
11B.2	Convergence function state machine	93
11B.2.1	Overview of state machine.....	93
11B.2.2	State list.....	93
11B.2.2.1	ESS_CONNECTED	93
11B.2.2.2	ESS_DISCONNECTED	94
11B.2.2.3	ESS_DISENGAGING	94
11B.2.2.4	STANDBY.....	94
11B.2.3	State transitions	94
11B.2.3.1	Transitions to ESS_CONNECTED	94
11B.2.3.2	Transitions to ESS_DISCONNECTED	94
11B.2.3.3	Transitions to ESS_DISENGAGING	95
11B.2.3.4	Transitions to STANDBY	95
11B.3	Informational events.....	95
11B.4	MAC state generic convergence SAP	95
11B.4.1	ESS status reporting	95
11B.4.1.1	MSGCF-ESS-Link-Up.....	95
11B.4.1.2	MSGCF-ESS-Link-Down.indication.....	96
11B.4.1.3	MSGCF-ESS-Link-Going-Down	98
11B.4.1.4	MSGCF-ESS-Link-Event-Rollback.indication	99
11B.4.1.5	MSGCF-ESS-Link-Detected.indication	100
11B.4.1.6	MSGCF-ESS-Link-Scan.request	101
11B.4.1.7	MSGCF-ESS-Link-Scan.confirm	102
11B.4.2	Network configuration	103
11B.4.2.1	MSGCF-ESS-Link-Capability.request	103
11B.4.2.2	MSGCF-ESS-Link-Capability.confirm	103
11B.4.2.3	MSGCF-Set-ESS-Link-Parameters.request.....	105
11B.4.2.4	MSGCF-Set-ESS-Link-Parameters.confirm.....	106
11B.4.2.5	MSGCF-Get-ESS-Link-Parameters.request	107
11B.4.2.6	MSGCF-Get-ESS-Link-Parameters.confirm	108
11B.4.3	Network events.....	109
11B.4.3.1	MSGCF-ESS-Link-Threshold-Report.indication	109
11B.4.4	Network command interface	110
11B.4.4.1	MSGCF-ESS-Link-Command.request	110
11B.5	MAC State SME SAP	111

11B.5.1 Mobility Management.....	111
11B.5.1.1 MSSME-ESS-Link-Down-Predicted.indication.....	111
Annex A (normative) Protocol Implementation Conformance Statement (PICS) proforma	113
Annex D (normative) ASN.1 encoding of the MAC and PHY MIB.....	116
Annex K (informative) Admission control.....	173
Annex P (informative) Bibliography	174
Annex X (informative) Interworking with external networks	175

List of figures

Figure 5-6a—SSPN interface service architecture	5
Figure 5-10a—Interworking reference model	7
Figure 5-10b—ESS link illustration	8
Figure 6-1—MAC data plane architecture	10
Figure 7-36r—GAS Query Response Fragment ID field	18
Figure 7-36s—Venue Info field format	18
Figure 7-95o118—Interworking element format	23
Figure 7-95o119—Access Network Options format	23
Figure 7-95o120—Advertisement Protocol element format	24
Figure 7-95o121—Advertisement Protocol Tuple format	25
Figure 7-95o122—Query Response Info format	25
Figure 7-95o123—Expedited Bandwidth Request element format	26
Figure 7-95o124—QoS Map Set element description	27
Figure 7-95o125—DSCP Exception format	27
Figure 7-95o126—DSCP Range description	28
Figure 7-95o127—Roaming Consortium information element format	28
Figure 7-95o128—OI #1 and #2 Lengths field format	29
Figure 7-95o129—Emergency Alert Identifier information element format	29
Figure 7-95q—ANQP element format	30
Figure 7-95r—ANQP Query list format	31
Figure 7-95s—ANQP Capability list format	32
Figure 7-95t—Venue Name information format	32
Figure 7-95u—Venue Name Duple field	33
Figure 7-95v—Emergency Call Number information format	33
Figure 7-95w—Emergency Call Number Unit field format	33
Figure 7-95x—Network Authentication Type information format	34
Figure 7-95y—Network Authentication Type Unit field format	34
Figure 7-95z—Roaming Consortium list format	35
Figure 7-95aa—OI Duple format	35
Figure 7-95ab—ANQP vendor-specific query format	36
Figure 7-95ac—IP Address Type Availability information	36
Figure 7-95ad—IP Address field format	36
Figure 7-95ae—NAI Realm list format	37
Figure 7-95af—NAI Realm Data field format	38
Figure 7-95ag—NAI Realm Encoding subfield format	38
Figure 7-95ah—EAP Method subfield format	38
Figure 7-95ai—Authentication Parameter subfield format	39
Figure 7-95aj—3GPP Cellular Network information format	41
Figure 7-95ak—AP Geospatial Location format	41
Figure 7-95al—AP Civic Location format	42
Figure 7-95am—AP Location Public Identifier URI format	42
Figure 7-95ao—Domain Name field format	43
Figure 7-95ap—Emergency Alert URI information format	43
Figure 7-95aq—Emergency NAI element format	43
Figure 7-95an—Domain Name list format	43
Figure 7-101h10—Query Request length field	47
Figure 7-101h11—Query Request field	47
Figure 7-101h12—GAS Comeback Delay field	48
Figure 7-101h13—Query Response length field	48
Figure 7-101h14—Query Response field	48
Figure 11-24—GAS message sequence with dot11GASPauseForServerResponse set to true	76

Figure 11-25—GAS message sequence with GAS fragmentation and
dot11GASPauseForServerResponse set to true 77

Figure 11-26—GAS message sequence with GAS fragmentation and
dot11GASPauseForServerResponse set to false..... 78

Figure 11A-24—Resource Request example #2 92

Figure 11B-1—MSGCF state machine..... 93

Figure X-1—Interworking IEEE 802.11 infrastructure supporting multiple SSPNs 180

Figure X-2—Basic architecture of the interworking service..... 183

List of tables

Table 7-10—Association Request frame body	15
Table 7-11—Association Response frame body	15
Table 7-8—Beacon frame body.....	15
Table 7-12—Reassociation Request frame body.....	16
Table 7-13—Reassociation Response frame body	16
Table 7-14—Probe Request frame body	16
Table 7-22—Reason codes	17
Table 7-15—Probe Response frame body	17
Table 7-23—Status codes	18
Table 7-25m—Venue Group codes and descriptions	19
Table 7-25n—Venue Type assignments.....	19
Table 7-26—Element IDs.....	22
Table 7-35a—Capabilities field.....	22
Table 7-43bh—Access network type.....	24
Table 7-43bi—Advertisement protocol ID definitions.....	26
Table 7-43bj—Precedence Level field description.....	27
Table 7-43bk—ANQP information ID definitions	30
Table 7-43bl—Network Authentication Type Indicator definitions	34
Table 7-43bn—IPv4 Address field values.....	37
Table 7-43bm—IPv6 Address field values.....	37
Table 7-43bo—Authentication Parameter types.....	39
Table 7-43bp—Authentication Parameter format for the Expanded EAP method	40
Table 7-43bq—Vendor-Specific Authentication Parameters	41
Table 7-45—QoS Action field values	44
Table 7-46—ADDTS Request frame body	44
Table 7-47—ADDTS Response frame body	45
Table 7-49a—QoS Map configure frame body	45
Table 7-57e—Public Action field values.....	46
Table 7-57f6—GAS Initial Request frame body format	46
Table 7-57f7—GAS Initial Response frame body format.....	47
Table 7-57f9—GAS Comeback Response frame body format	49
Table 7-57f8—GAS Comeback Request frame body format.....	49
Table 7-57m—Protected Dual of Public Action field values	50
Table 11-2—Encoding of ResultCode to Status Code field value	74
Table 11-14—GAS MLME primitive’s encoding of Result Code to Status Code field	79
Table 11-15—ANQP usage	83
Table 11-16—ESR and UESA field settings.....	89
Table 11A-2—Resource types and resource descriptor definitions	91
Table 11B-1—Reason codes for network down.....	97
Table 11B-2—Reason codes for ESS link down.....	98
Table 11B-3—ESS description.....	100
Table 11B-4—Trigger support values	101
Table 11B-5—Event Capability Set	104
Table 11B-6—ESS Link Parameter Set.....	105
Table X-2—Example Enterprise DSCP to UP/AC mapping.....	181
Table X-1—Mapping table of DSCP to 3GPP QoS information and EDCA ACs	181
Table X-3—UP to DSCP range mapping example	182
Table X-4—SSPN Interface information or permission parameters	183

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 9: Interworking with External Networks

(This amendment is based on IEEE Std 802.11™-2007, as amended by IEEE Std 802.11k™-2008, IEEE Std 802.11r™-2008, IEEE Std 802.11y™-2008, IEEE Std 802.11w™-2009, IEEE Std 802.11n™-2009, IEEE Std 802.11p™-2010, IEEE Std 802.11z™-2010, and IEEE Std 802.11v™-2011.)

IMPORTANT NOTICE: *This standard is not intended to ensure 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>.

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. 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. Editorial notes 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

1.2 Purpose

Insert the following new list item at end of the dashed list in 1.2:

- Defines functions and procedures aiding network discovery and selection by STAs, information transfer from external networks using QoS mapping, and a general mechanism for the provision of emergency services.

2. Normative references

Insert the following new references in alphanumeric order into Clause 2:

3GPP TS 24.234, 3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3.²

IANA EAP Method Type Numbers, <http://www.iana.org/assignments/eap-numbers>.

IEEE Std 802.21™-2008, IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, January 2009.^{3, 4}

IETF RFC 1035, Domain Names — Implementation and Specification, P. Mockapetris, November 1987.⁵

IETF RFC 3629, UTF-8, a transformation format of ISO 10646, F. Yergeau, November 2003.

IETF RFC 3748, Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowitz, June 2004.

IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, January 2005.

IETF RFC 4282, The Network Access Identifier, December 2005.

IETF RFC 5216, The EAP-TLS Authentication Protocol, D. Simon, B. Aboba, R. Hurst, March 2008.

OASIS Emergency Management Technical Committee, “Emergency Data Exchange Language (EDXL) Distribution Element, v. 1.0.” OASIS Standard EDXL-DE v1.0, May 2006.

3. Definitions

Insert the following new definitions in alphabetical order into Clause 3, renumbering as necessary:

3.267 Access Network Query Protocol (ANQP): The query protocol for access network information retrieval transported by generic advertisement service (GAS) Public Action frames.

²3GPP documents are available from the 3rd Generation Partnership Project Web site (<http://www.3gpp.org>).

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

⁴The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

⁵Internet RFCs are available from the Internet Engineering Task Force at <http://www.ietf.org/>.

3.268 advertisement protocol: Access Network Query Protocol (ANQP) and higher layer protocols defined external to IEEE Std 802.11 that are used for network and service discovery.

3.269 advertisement server: A logical server that provides the information repository for a specific advertisement protocol. The location of the physical server that instantiates the advertisement server is outside the scope of this specification.

3.270 authorization: The act of determining if a particular right, such as access to some resource, can be granted to an authenticated entity.

NOTE—See RFC 2903 [B44].⁶

3.271 emergency alert system (EAS): A U.S. national public warning system.

3.272 emergency services association: A robust security network association (RSNA) between an access point (AP) and a non-AP station (STA) without security credentials; the non-AP STA is granted access to emergency services using unprotected frames via this association.

3.273 extended service set (ESS) link: In the context of an IEEE 802.11 medium access control (MAC) entity, a connection path through the wireless medium between a non-access point (non-AP) station (STA) and one of the APs that is a member of the ESS.

3.274 generic advertisement service (GAS): An IEEE 802.11 service that provides over-the-air transportation for frames of higher layer advertisements between stations (STAs) or between an advertisement server and a non-access point (non-AP) STA. The protocol(s) used to relay frames between an AP, portal, and advertisement server is outside the scope of this standard. GAS supports higher layer protocols that employ a query/response mechanism.

3.275 infrastructure authorization information: The information that specifies the access rights of the user of a non-access point (non-AP) station (STA) in an IEEE 802.11 infrastructure. This information may include the rules for routing the user traffic, a set of permissions about services that a user is allowed to access, quality of service (QoS) configuration information, or the accounting policy to be applied by the IEEE 802.11 infrastructure.

3.276 homogenous extended service set (ESS): A collection of basic service sets (BSSs), within the same extended service set (ESS), in which every subscription service provider network (SSPN) or other external network reachable at one BSS is reachable at all of them.

3.277 interworking service: A service that supports use of an IEEE 802.11 network with non-IEEE 802.11 networks. Functions of the interworking service assist non-access point (non-AP) stations (STAs) in discovering and selecting IEEE 802.11 networks, in using appropriate quality of service (QoS) settings for transmissions, in accessing emergency services, and in connecting to subscription service providers (SSPs).

3.278 multi-level precedence and preemption (MLPP): A framework used with admission control for the treatment of traffic streams based on precedence, which supports the preemption of an active traffic stream by a higher precedence traffic stream when resources are limited. Preemption is the act of forcibly removing a traffic stream in progress in order to free up resources for another higher precedence traffic stream.

3.279 network access identifier (NAI): The user identity submitted by the Supplicant during IEEE 802.1X authentication.

NOTE—See RFC 4282.⁷

⁶The numbers in brackets correspond to the numbers of the bibliography in Annex P.

⁷Information on references can be found in Clause 2.

3.280 public safety answering point (PSAP): A physical location where emergency calls are received and routed to the proper emergency services such as police and ambulance.

NOTE—See NENA 08-002 [B51].

3.281 roaming consortium: A group of subscription service providers (SSPs) having inter-SSP roaming agreements.

3.282 subscription service provider (SSP): An organization (operator) offering connection to network services, perhaps for a fee.

3.283 subscription service provider network (SSPN): The network controlled by a subscription service provider (SSP). The network maintains user subscription information.

3.284 subscription service provider (SSP) roaming: The act when a station (STA) uses an SSP's IEEE 802.11 infrastructure, with which the terminal has no direct agreement, based on a subscription and formal agreement with the STA's own SSP.

4. Abbreviations and acronyms

Insert the following new abbreviations and acronyms into Clause 4 in alphabetical order:

3GPP™	3rd Generation Partnership Project
802.x LAN	IEEE 802®-based local area networks such as IEEE 802.3 and IEEE 802.11
AAA	authentication, authorization, and accounting
ANQP	Access Network Query Protocol
ASRA	additional step required for access
DN	destination network
EAS	emergency alert system
EBR	expedited bandwidth request
ESR	emergency services reachable
GAS	generic advertisement service
GPRS	general packet radio service
HESSID	homogenous extended service set identifier
MIH	media-independent handover
MLPP	multi-level precedence and preemption
MSGCF	MAC state generic convergence function
NAI	network access identifier
OI	organization identifier
PHB	per-hop behavior
PSAP	public safety answering point
SSP	subscription service provider
SSPN	subscription service provider network
UESA	unauthenticated emergency service accessible
URL	uniform resource locator
URI	uniform resource identifier
VLAN	virtual local area network

5. General description

5.2 Components of the IEEE 802.11 architecture

Insert the following new subclause (5.2.13) after 5.2.12.22:

5.2.13 Subscription service provider network (SSPN) interface

An AP can interact with external networks using a SSPN interface for the purpose of authenticating users and provisioning services, as shown in Figure 5-6a. The exchange of authentication and provisioning information between the SSPN and the AP passes transparently through the Portal. The protocol used to exchange this information is outside the scope of this standard. The logical SSPN interface provides the means for an AP to consult an SSPN for authenticating and authorizing a specific non-AP STA and to report statistics and status information to the SSPN. Authentication and provisioning information for non-AP STAs received from the SSPN are stored in the AP management information base (MIB) and are used to limit layer-2 services provided to that non-AP STA. Detailed interactions describing the SSPN interface are provided in 11.23.5.

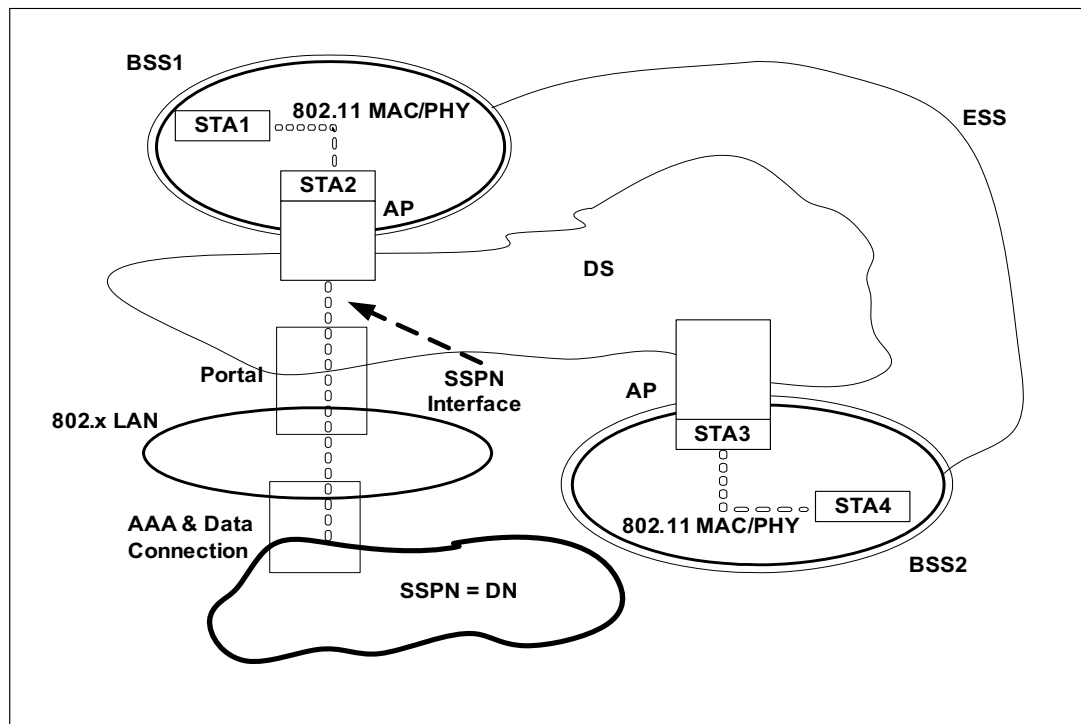


Figure 5-6a—SSPN interface service architecture

The SSPN interface provides the non-AP STA access to the services provisioned in the SSPN via the currently associated BSS. SSPN access may involve virtual local area network (VLAN) mapping or tunnel establishment that are transparent to the non-AP STA and outside the scope of this standard. The SSPN interface also allows the non-AP STA to access services in destination networks (DNs) other than the SSPN. An example of a DN other than SSPN is the provision of Internet access via the IEEE 802 LAN, or an intermediary network that connects the IEEE 802.11 infrastructure and the SSPN.

NOTE—The SSPN Interface Service is not supported in an IBSS.

5.4 Overview of the services

Insert the following new subclause (5.4.8) after 5.4.7:

5.4.8 Interworking with external networks

The interworking service allows non-AP STAs to access services provided by an external network according to the subscription or other characteristics of that external network. An IEEE 802.11 non-AP STA may have a subscription relationship with an external network, e.g., with an SSPN.

An overview of the interworking functions addressed in this standard is provided below:

- Network discovery and selection
 - Discovery of suitable networks through the advertisement of access network type, roaming consortium and venue information, via management frames
 - Selection of a suitable IEEE 802.11 infrastructure using advertisement services (e.g., Access Network Query Protocol (ANQP) or an IEEE 802.21 Information Server) in the BSS or in an external network reachable via the BSS.
 - Selection of an SSPN or external network with its corresponding IEEE 802.11 infrastructure
- Emergency services
 - Emergency Call and Network Alert support at the link level
- QoS Map distribution
- SSPN interface service between the AP and the SSPN

The generic advertisement service (GAS), described in 5.9, can be used by a STA to provide support for the network selection process and as a conduit for communication by a non-AP STA with other information resources in a network before joining the wireless LAN.

The interworking service supports emergency services by providing methods for users to access emergency services via the IEEE 802.11 infrastructure, advertising that emergency services are supported (see 11.23.6) and identifying that a traffic stream is used for emergency services.

The interworking service provides QoS mapping for SSPNs and other external networks. Since each SSPN or other external network may have its own layer-3 end-to-end packet marking practice (e.g., DSCP usage conventions), a means to re-map the layer-3 service levels to a common over-the-air service level is necessary. The QoS Map service provides STAs a mapping of network-layer QoS packet marking to over-the-air QoS frame marking (i.e., user priority).

The SSPN Interface service supports service provisioning and transfer of user permissions from the SSPN to the AP. The method and protocol by which these permissions are transferred from the SSPN are outside the scope of this standard.

5.7 Reference model

Insert the following new subclause heading 5.7.1 immediately after the subclause heading 5.7 and before the existing text:

5.7.1 General

Change the first paragraph of 5.7.1 as follows:

This standard presents the architectural view, emphasizing the separation of the system into two major parts: the MAC of the data link layer (DLL) and the PHY. These layers are intended to correspond closely to the lowest layers of the ISO/IEC basic reference model of Open Systems Interconnection (OSI) (ISO/IEC 7498-1: 1994). The MAC state generic convergence function (MSGCF) provides services to higher layer protocols based on MAC state machines and interactions between the layers. The layers and sublayers described in this standard are shown in Figure 5-10.

Insert the following new subclause (5.7.2) after 5.7.1:**5.7.2 Interworking reference model**

Interworking functions may require correlating information from multiple management entities. It is the function of the MSGCF to correlate information for higher layer entities. The MSGCF observes the interactions between the MLME and SME, and between the PLME and SME. After correlation of lower-layer MLME and PLME events, the MSGCF may synthesize indications to higher layer entities.

Figure 5-10a shows an entity, the MSGCF, defined in Clause 11B, that has access to all management information through exposure to the MAC and PHY Sublayer Management Entities, and provides management information to higher level entities, such as Mobility Managers, supporting heterogeneous medium mobility.

An example of how the MSGCF interfaces to these higher layer entities, is provided by the media-independent handover (MIH) interface, as defined in IEEE 802.21-2008.

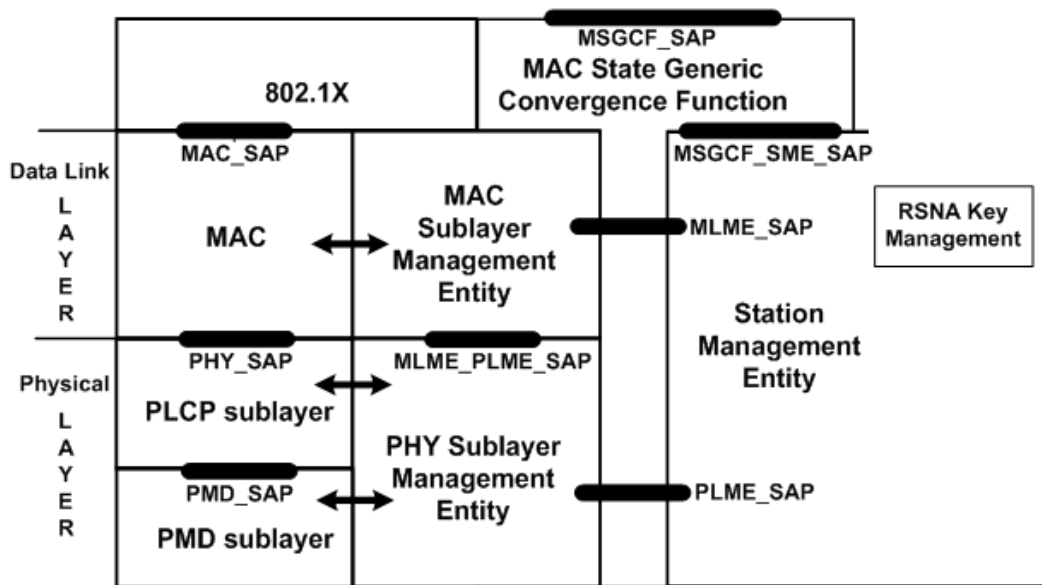


Figure 5-10a—Interworking reference model

The MSGCF is designed to provide the status of the connection of a non-AP STA to a set of BSSs comprising a single ESS. Figure 5-10b illustrates the concept of an ESS Link. This reflects the state of a connection to an ESS independent of any particular access point. In Figure 5-10b, STA3 is associated with either AP1 or AP2. The state of the ESS Link is up when STA3 is associated with any of the APs comprising an ESS.

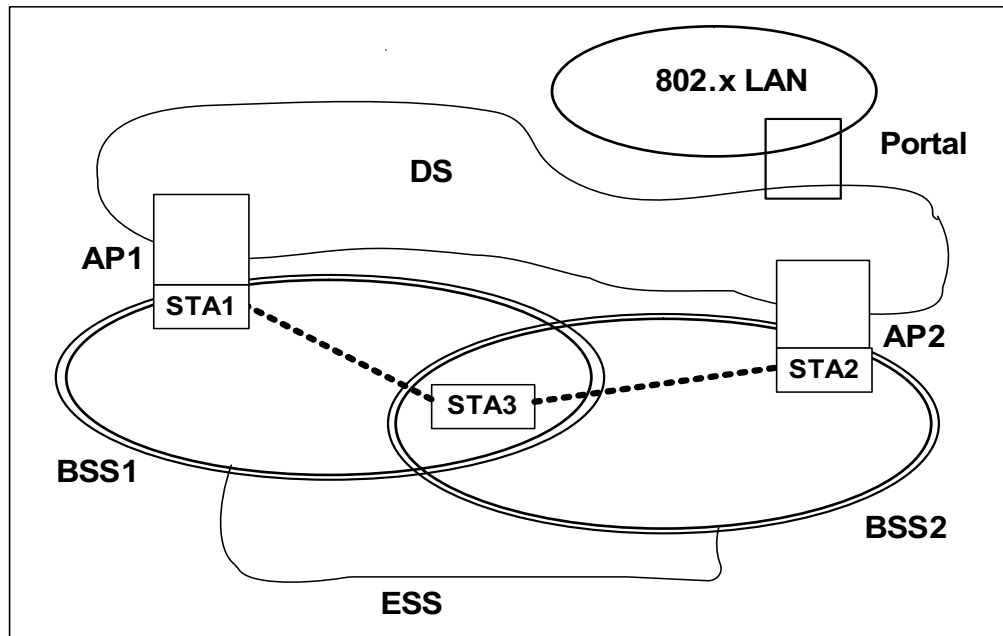


Figure 5-10b—ESS link illustration

Insert the following new subclause (5.9) after 5.8:

5.9 Generic advertisement service (GAS)

GAS provides functionality that enables STAs to discover the availability of information related to desired network services, e.g., information about services such as provided in an IBSS, local access services, available subscription service providers (SSPs) and/or SSPNs or other external networks. GAS uses a generic container to advertise network services' information over an IEEE 802.11 network. Public Action frames are used to transport this information.

While the specification of network services information is outside the scope of this standard, in an Infrastructure BSS there is a need for STAs to query for information on network services provided by SSPNs or other external networks beyond an AP, before they associate to the wireless LAN. The exchange of information may also be performed after associating to the BSS.

In an IBSS, GAS functionality enables a STA to access the availability and information related to desired services provided by other STAs in the IBSS. Exchange of information using GAS may be performed either prior to joining an IBSS or after joining the IBSS.

There are a number of reasons why providing information to a STA in a pre-associated state is beneficial:

- It supports more informed decision making about an IEEE 802.11 infrastructure with which to associate. This is generally more efficient than requiring a non-AP STA to associate with an AP before discovering the information and then deciding whether or not to stay associated.
- It is possible for the non-AP STA to query multiple networks in parallel.
- The non-AP STA can discover information about APs that are not part of the same administrative group as the AP with which it is associated, supporting the selection of an AP belonging to a different IEEE 802.11 infrastructure that has an appropriate SSP roaming agreement in place.

6. MAC service definition

6.1 Overview of MAC services

6.1.5 MAC data service architecture

Change the first two paragraphs of 6.1.5 as follows:

The MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 6-1. During transmission, an MSDU goes through some or all of the following processes: MSDU rate limiting, A-MSDU aggregation, frame delivery deferral during power save mode, sequence number assignment, fragmentation, encryption, integrity protection, and frame formatting and A-MPDU aggregation. IEEE Std 802.1X-2004 may block the MSDU at the Controlled Port. At some point, the data frames that contain all or part of the MSDU are queued per AC/TS. This queuing may be at any of the three points indicated in Figure 6-1.

During reception, a received data frame goes through processes of possible A-MPDU de-aggregation, MPDU header and cyclic redundancy code (CRC) validation, duplicate removal, possible reordering if the Block Ack mechanism is used, decryption, defragmentation, integrity checking, and replay detection. After replay detection (or defragmentation if security is used), ~~and possible A-MSDU de-aggregation~~ and possible MSDU rate limiting, the one or more MSDUs ~~is~~ are delivered to the MAC_SAP or to the DS. The IEEE 802.1X Controlled/Uncontrolled Ports discard ~~the~~ any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame. TKIP and CCMP MPDU frame order enforcement occurs after decryption, but prior to MSDU defragmentation; therefore, defragmentation will fail if MPDUs arrive out of order.

Replace Figure 6-1—MAC data plane architecture with the following figure:

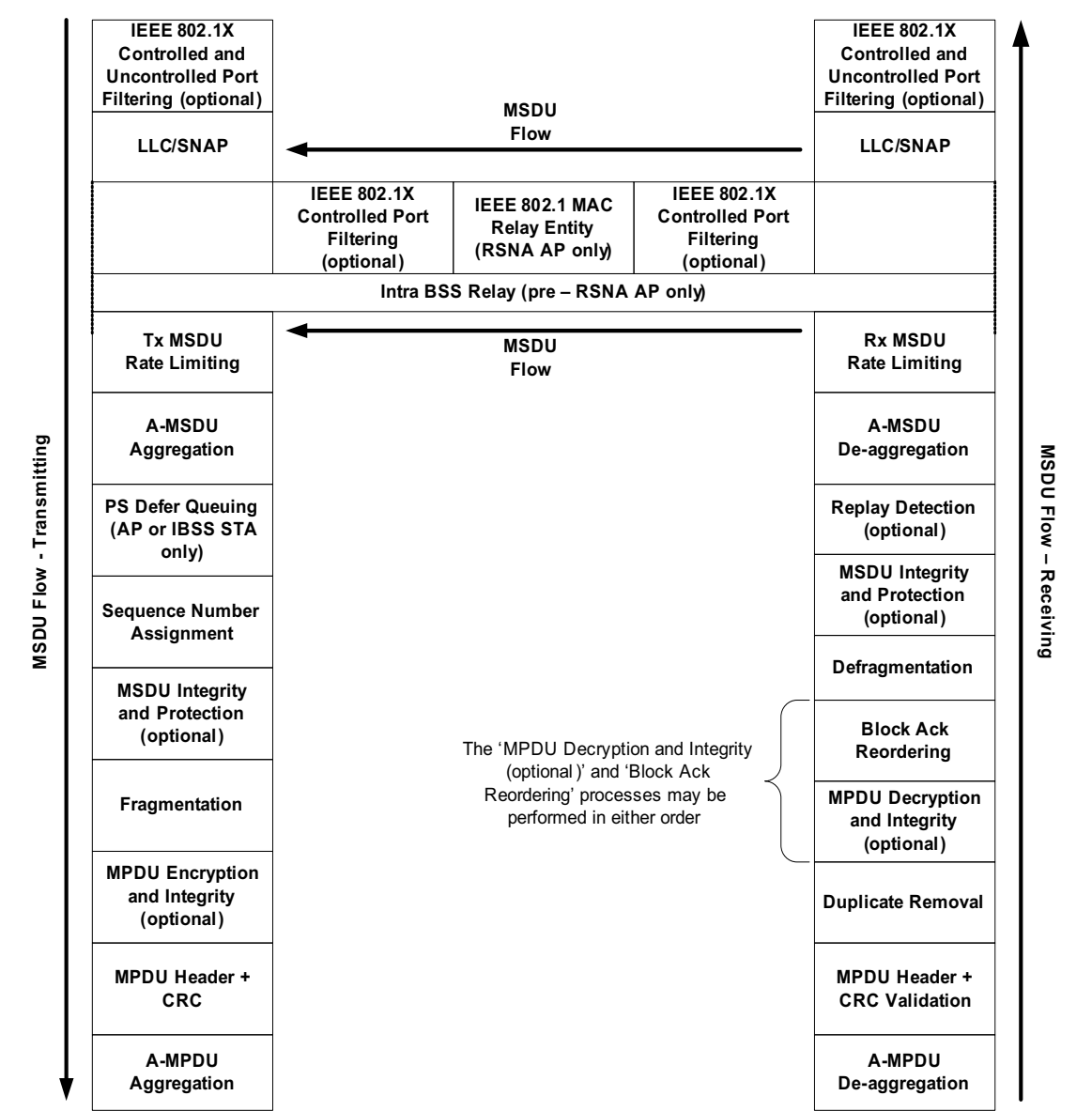


Figure 6-1—MAC data plane architecture

6.2 Detailed service specification

6.2.1 MAC data services

6.2.1.1 MA-UNITDATA.request

6.2.1.1.4 Effect of receipt

Insert the following text after the first paragraph of 6.2.1.1.4:

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address and a priority of Contention or Contention-Free, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingEntry identified by the destination MAC address of the frame to be transmitted. The specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address for which the priority is an integer in the range of 0 to 7, inclusive, then the AP's MAC sublayer shall derive the access category from the priority using the mapping in Table 9-1. The AP's MAC sublayer shall retrieve the MIB variables listed below from the dot11InterworkingEntry identified by the destination MAC address of the frame to be transmitted and perform the following operations:

- If the access category is AC_VO, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVoiceRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate limiting mechanism does not discard the frame, then dot11NonAPStationVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationVoiceOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVoiceOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_VI, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVideoRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVideoMSDUCount shall be incremented by 1 and dot11NonAPStationVideoOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVideoMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVideoOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BE, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and

dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

- If the access category is AC_BK, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBackgroundRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationBackgroundOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBackgroundOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an MA-UNITDATA.request primitive having an individually addressed destination address whose priority is an integer in the range of 8 to 15, inclusive, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxHCCAHEMMRate; the specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationHCCAHEMM-MSDUCount shall be incremented by 1, and dot11NonAPStationHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedHCCAHEMM-MSDUCount shall be incremented by 1 and dot11NonAPStationDroppedHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.

6.2.1.2 MA-UNITDATA.indication

6.2.1.2.4 Effect of receipt

Insert the following text after the first paragraph of 6.2.1.2.4:

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of a frame of type data having a broadcast/multicast DA, the AP's MAC sublayer shall discard the frame if dot11NonAPStationAuthSourceMulticast is false in the dot11InterworkingEntry identified by the source MAC address of the received frame. If dot11NonAPStationAuthSourceMulticast is true, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxSourceMulticastRate in the dot11InterworkingEntry identified by the source MAC address of the received frame. The specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate limiting mechanism does not discard the frame, then dot11NonAPStationMulticast-MSDUCount shall be incremented by 1 and dot11NonAPStationMulticastOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedMulticast-MSDUCount shall be incremented by 1 and dot11NonAPStationDroppedMulticastOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an individually addressed frame of type data and a priority of Contention or ContentionFree, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingEntry identified by the source MAC address of the received frame. The specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an individually addressed frame of type data, for which the priority is an integer in the range of 0 to 7, inclusive, then the AP's MAC sublayer shall derive the access category from the priority using the mapping in Table 9-1. The AP's MAC sublayer shall retrieve the MIB variables from the dot11InterworkingEntry identified by the source MAC address of the received frame and perform the following operations:

- If the access category is AC_VO, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVoiceRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationVoiceOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVoiceMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVoiceOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_VI, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthVideoRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationVideoMSDUCount shall be incremented by 1 and dot11NonAPStationVideoOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedVideoMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedVideoOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BE, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBestEffortRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationBestEffortOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBestEffortMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBestEffortOctetCount shall be incremented by the number of octets in the MSDU.
- If the access category is AC_BK, then the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationMaxAuthBackgroundRate; the specific mechanism to perform rate limiting is outside the scope of this specification. If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationBackgroundOctetCount shall be incremented by the number of octets in the MSDU. If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedBackgroundMSDUCount shall be incremented by 1 and dot11NonAPStationDroppedBackgroundOctetCount shall be incremented by the number of octets in the MSDU.

At an AP for which dot11SSPNInterfaceActivated is true, upon receipt of an individually addressed frame of type data for which the priority is an integer in the range of 8 to 15, inclusive, the AP's MAC sublayer shall perform rate limiting to enforce the resource utilization limit in dot11NonAPStationAuthMaxHCCAHEMMRate; the specific mechanism to perform rate limiting is outside the scope of this specification.

- If the rate-limiting mechanism does not discard the frame, then dot11NonAPStationHCCAHEMM-MSDUCount shall be incremented by 1, and dot11NonAPStationHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.
- If the rate limiting mechanism discards the frame, then dot11NonAPStationDroppedHCCAHEMM-MSDUCount shall be incremented by 1 and dot11NonAPStationDroppedHCCAHEMMOctetCount shall be incremented by the number of octets in the MSDU.

6.2.1.3 MA-UNITDATA.confirm

6.2.1.3.1 Function

Insert the following items into the lettered list in 6.2.1.3.1 after item i):

- j) For an AP in which dot11SSPNInterfaceActivated is true, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthVoiceRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).
- k) For an AP in which dot11SSPNInterfaceActivated is true, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthVideoRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).
- l) For an AP in which dot11SSPNInterfaceActivated is true, Undeliverable (violation of limit specified by dot11NonAPStationMaxAuthBestEffortRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).
- m) For an AP in which dot11SSPNInterfaceActivated is true, Undeliverable (violation of limit specified by dot11NonAPStationBackgroundRate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).
- n) For an AP in which dot11SSPNInterfaceActivated is true, Undeliverable (violation of limit specified by dot11NonAPStationAuxMaxHCCAHEMMrate in the dot11InterworkingTable for the non-AP STA identified by the destination address of the MA-UNITDATA.request primitive).

7. Frame formats

7.1 MAC frame formats

7.2 Format of individual frame types

7.2.3 Management frames

7.2.3.1 Beacon frame format

Change order 31 information field and insert order 45 through 48 information fields into Table 7-8 as follows (note that the entire table is not shown here):

Table 7-8—Beacon frame body

Order	Information	Notes
31	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RRMMeasurementPilotCapability is a value between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 11.10.11) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, <u>or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.</u>
45	<u>Interworking</u>	<u>The Interworking element is present if dot11InterworkingServiceActivated is true.</u>
46	<u>Advertisement Protocol</u>	<u>Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.</u>
47	<u>Roaming Consortium</u>	<u>The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.</u>
48	<u>Emergency Alert Identifier</u>	<u>One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.</u>

7.2.3.4 Association Request frame format

Insert the order 18 information field into Table 7-10 (note that the entire table is not shown here):

Table 7-10—Association Request frame body

Order	Information	Notes
18	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true and the non-AP STA is requesting unauthenticated access to emergency services (see 11.3.2).

7.2.3.5 Association Response frame format

Insert the order 21 information field into Table 7-11 (note that the entire table is not shown here):

Table 7-11—Association Response frame body

Order	Information	Notes
21	QoS Map	QoS Map is present if dot11QoSMapActivated is true and the QoS Map field in the Extended Capabilities element of the corresponding Association Request frame is 1.

7.2.3.6 Reassociation Request frame format

Insert the order 23 information field into Table 7-12 (note that the entire table is not shown here):

Table 7-12—Reassociation Request frame body

Order	Information	Notes
23	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true and the non-AP STA is requesting unauthenticated access to emergency services (see 11.3.2).

7.2.3.7 Reassociation Response frame format

Insert the order 25 information field into Table 7-13 (note that the entire table is not shown here):

Table 7-13—Reassociation Response frame body

Order	Information	Notes
25	QoS Map	QoS Map is present if dot11QosMapActivated is true and the QoS Map field in the Extended Capabilities element of the corresponding Reassociation Request frame is 1.

7.2.3.8 Probe Request frame format

Insert order 12 information field into Table 7-14 (note that the entire table is not shown here):

Table 7-14—Probe Request frame body

Order	Information	Notes
12	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.

7.2.3.9 Probe Response frame format

Change order 24 information field and insert order 44 through 47 information fields into Table 7-15 as follows (note that the entire table is not shown here):

Table 7-15—Probe Response frame body

Order	Information	Notes
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11IRRMMeasurementPilotCapability is a value between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 11.10.11) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, <u>or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.</u>
44	<u>Interworking</u>	<u>The Interworking element is present if dot11InterworkingServiceActivated is true.</u>
45	<u>Advertisement Protocol</u>	<u>Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.</u>
46	<u>Roaming Consortium</u>	<u>The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.</u>
47	<u>Emergency Alert Identifier</u>	<u>One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.</u>

7.3 Management frame body components

7.3.1 Fields that are not information elements

7.3.1.7 Reason Code field

Insert reason codes 27 through 30 and 46 and 47 into Table 7-22 (note that the entire table is not shown here):

Table 7-22—Reason codes

Reason code	Meaning
27	Disassociated because session terminated by SSP request
28	Disassociated because of lack of SSP roaming agreement
29	Requested service rejected because of SSP cipher suite or AKM requirement
30	Requested service not authorized in this location
46	Disassociated because authorized access limit reached
47	Disassociated due to external service requirements

7.3.1.9 Status Code field

Insert status codes 59 through 65 and 67, 68, and 79 into Table 7-23 as follows (note the entire table is not shown here):

Table 7-23—Status codes

Status code	Meaning
59	GAS Advertisement Protocol not supported
60	No outstanding GAS request
61	GAS Response not received from the Advertisement Server
62	STA timed out waiting for GAS Query Response
63	GAS Response is larger than query response length limit
64	Request refused because home network does not support request
65	Advertisement Server in the network is not currently reachable
67	Request refused due to permissions received via SSPN interface
68	Request refused because AP does not support unauthenticated access
79	Transmission failure

Insert the following new subclauses (7.3.1.33 and 7.3.1.34) after 7.3.1.32:

7.3.1.33 GAS Query Response Fragment ID field

A GAS Query Response Fragment ID field is used by the STA to indicate when a GAS Query Response spans multiple MMPDUs. STAs responding to GAS request use this field to inform the requesting STA of the GAS fragment number of the transmitted frames as well as identifying the last GAS fragment of the Query Response. Requesting STAs use this field to determine if any fragments of the Query Response are missing. The maximum value permitted in the GAS Query Response Fragment ID is 127. The More GAS Fragments field is set to 1 in GAS Query Response fragments of GAS Comeback Response frames that have another GAS fragment of the current query response to follow; otherwise, it is set to 0. The format of GAS Query Response Fragment ID is shown in Figure 7-36r.

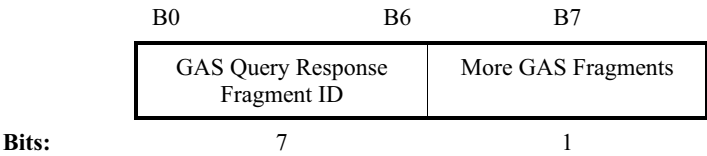


Figure 7-36r—GAS Query Response Fragment ID field

7.3.1.34 Venue Info field

The Venue Info field is a 2-octet field. It contains Venue Group and Venue Type subfields. The format of Venue Info subfield is shown in Figure 7-36s.

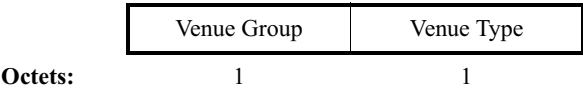


Figure 7-36s—Venue Info field format

The Venue Group and Venue Type subfields are both one octet values selected from Table 7-25m and Table 7-25n respectively. The entries in Table 7-25m and Table 7-25n are drawn from the International Building Code's Use and Occupancy Classifications [B48].

Table 7-25m—Venue Group codes and descriptions

Venue Group code	Venue Group description
0	Unspecified
1	Assembly
2	Business
3	Educational
4	Factory and Industrial
5	Institutional
6	Mercantile
7	Residential
8	Storage
9	Utility and Miscellaneous
10	Vehicular
11	Outdoor
12 – 255	Reserved

Table 7-25n—Venue Type assignments

Venue Group code	Venue Type code	Venue description
0	0	Unspecified
0	1 – 255	Reserved
1	0	Unspecified Assembly
1	1	Arena
1	2	Stadium
1	3	Passenger Terminal (e.g., airport, bus, ferry, train station)
1	4	Amphitheater
1	5	Amusement Park
1	6	Place of Worship
1	7	Convention Center
1	8	Library
1	9	Museum
1	10	Restaurant
1	11	Theater
1	12	Bar
1	13	Coffee Shop

Table 7-25n—Venue Type assignments (continued)

Venue Group code	Venue Type code	Venue description
1	14	Zoo or Aquarium
1	15	Emergency Coordination Center
1	16 – 255	Reserved
2	0	Unspecified Business
2	1	Doctor or Dentist office
2	2	Bank
2	3	Fire Station
2	4	Police Station
2	6	Post Office
2	7	Professional Office
2	8	Research and Development Facility
2	9	Attorney Office
2	10 – 255	Reserved
3	0	Unspecified Educational
3	1	School, Primary
3	2	School, Secondary
3	3	University or College
3	4 – 255	Reserved
4	0	Unspecified Factory and Industrial
4	1	Factory
4	2 – 255	Reserved
5	0	Unspecified Institutional
5	1	Hospital
5	2	Long-Term Care Facility (e.g., Nursing home, Hospice, etc.)
5	3	Alcohol and Drug Re-habilitation Center
5	4	Group Home
5	5	Prison or Jail
5	6 – 255	Reserved
6	0	Unspecified Mercantile
6	1	Retail Store
6	2	Grocery Market
6	3	Automotive Service Station
6	4	Shopping Mall
6	5	Gas Station
6	6 – 255	Reserved
7	0	Unspecified Residential
7	1	Private Residence

Table 7-25n—Venue Type assignments (continued)

Venue Group code	Venue Type code	Venue description
7	2	Hotel or Motel
7	3	Dormitory
7	4	Boarding House
7	5 – 255	Reserved
8	0	Unspecified Storage
8	1 – 255	Reserved
9	0	Unspecified Utility and Miscellaneous
9	1 – 255	Reserved
10	0	Unspecified Vehicular
10	1	Automobile or Truck
10	2	Airplane
10	3	Bus
10	4	Ferry
10	5	Ship or Boat
10	6	Train
10	7	Motor Bike
10	8 – 255	Reserved
11	0	Unspecified Outdoor
11	1	Muni-mesh Network
11	2	City Park
11	3	Rest Area
11	4	Traffic Control
11	5	Bus Stop
11	6	Kiosk
11	7 – 255	Reserved

7.3.2 Information elements

Insert element identifiers (IDs) 107 through 112 and change the Reserved row in Table 7-26 as follows (note the entire table is not shown here):

Table 7-26—Element IDs

Information element	Element ID	Length (in octets)	Extensible
<u>Interworking (see 7.3.2.92)</u>	<u>107</u>	<u>3, 5, 9, 11</u>	
<u>Advertisement Protocol (see 7.3.2.93)</u>	<u>108</u>	<u>variable</u>	
<u>Expedited Bandwidth Request (see 7.3.2.94)</u>	<u>109</u>	<u>3</u>	
<u>QoS Map Set (see 7.3.2.95)</u>	<u>110</u>	<u>18 to 60</u>	<u>Yes</u>
<u>Roaming Consortium (see 7.3.2.96)</u>	<u>111</u>	<u>variable</u>	<u>Yes</u>
<u>Emergency Alert Identifier (see 7.3.2.97)</u>	<u>112</u>	<u>10</u>	
Reserved	<u>113–107 –140</u> <u>and 143 – 220</u>		

7.3.2.27 Extended Capabilities information element

Insert the rows for Bit 31 through Bit 36 into Table 7-35a as follows (note the entire table is not shown here):

Table 7-35a—Capabilities field

Bit(s)	Information	Notes
<u>31</u>	<u>Interworking</u>	<u>When dot11InterworkingServiceActivated is true, the Interworking field is set to 1 to indicate the STA supports interworking service as described in 11.23. When dot11InterworkingServiceActivated is false, the Interworking field is set to 0 to indicate the STA does not support this capability.</u>
<u>32</u>	<u>QoS Map</u>	<u>When dot11QosMapActivated is true, the QoS Map field is set to 1 to indicate the STA supports QoS Map service as described in 11.23.9. When dot11QosMapActivated is false, the QoS Map field is set to 0 to indicate the STA does not support this capability.</u>
<u>33</u>	<u>EBR</u>	<u>When dot11EBRActivated is true, the EBR field is set to 1 to indicate the STA supports EBR operation as described in 11.4. When dot11EBRActivated is false, the EBR field is set to 0 to indicate the STA does not support this capability.</u>
<u>34</u>	<u>SSPN Interface</u>	<u>When dot11SSPNInterfaceActivated is true, the SSPN Interface field is set to 1 to indicate the AP supports SSPN Interface service as described in 11.23.5. When dot11SSPNInterfaceActivated is false, the SSPN Interface is set to 0 to indicate the AP does not support this capability. Non-AP STAs set this field to 0.</u>
<u>35</u>	<u>Reserved</u>	This bit is reserved and is set to 0 on transmission and ignored on reception.
<u>36</u>	<u>MSGCF Capability</u>	<u>When dot11MSGCFActivated is true, the MSGCF Capability field is set to 1 to indicate the non-AP STA supports the MSGCF in 11B. When dot11MSGCFActivated is false, the MSGCF Capability is set to 0 to indicate the non-AP STA does not support this capability. APs set this field to 0.</u>

Insert the following new subclauses (7.3.2.92 through 7.3.2.97) after 7.3.2.91:

7.3.2.92 Interworking information element

The Interworking information element contains information about the interworking service capabilities of a STA as shown in Figure 7-95o118.

	Element ID	Length	Access Network Options	Venue Info (optional)	HESSID (optional)
Octets:	1	1	1	0 or 2	0 or 6

Figure 7-95o118—Interworking element format

The Length is a one-octet field whose value is 1 plus the sum of the lengths of each optional field present in the element.

The format of Access Network Options field is shown in Figure 7-95o119.

Bits:	B0 – B3	B4	B5	B6	B7
	Access Network Type	Internet	ASRA	ESR	UESA

Figure 7-95o119—Access Network Options format

A non-AP STA sets Internet, ASRA, ESR, and UESA fields to 0 when including the Interworking element in the Probe Request frame. A non-AP STA sets the Internet, ASRA and ESR bits to 0 when including the Interworking element in (Re)association Request frames. In (Re)association Request frames, a non-AP STA sets the UESA bit according to the procedures in 11.3.2. The Access Network Types are shown in Table 7-43bh. The Access Network Type field is set by the AP to advertise its Access Network Type to non-AP STAs. A non-AP STA uses this field to indicate the desired Access Network Type in an active scan. See X.1 for informative text on usage of fields contained within the Interworking element.

Bit 4 is the Internet field. The AP sets this field to 1 if the network provides connectivity to the Internet; otherwise it is set to 0 indicating that it is unspecified whether the network provides connectivity to the Internet.

Bit 5 is the Additional Step Required for Access (ASRA) field. It is set to 1 by the AP to indicate that the network requires a further step for access. It is set to 0 whenever dot11RSNAEnabled is true. For more information, refer to Network Authentication Type Information in 7.3.4.5.

Bit 6 is the ESR (emergency services reachable) field. It is set to 1 by the AP to indicate that emergency services are reachable through the AP; otherwise it is set to 0 indicating that it is unspecified whether emergency services are reachable, see 11.23.6.

Bit 7 is the UESA (unauthenticated emergency service accessible) field. When the AP sets it to 0, this field indicates that no unauthenticated emergency services are reachable through this AP. When set to 1, this field indicates that higher layer unauthenticated emergency services are reachable through this AP. A STA uses the Interworking information element with the UESA bit set to 1 to gain unauthenticated access to a BSS to access emergency services. See 11.3.2.

Table 7-43bh—Access network type

Access network type	Meaning	Description
0	Private network	Non-authorized users are not permitted on this network. Examples of this access network type are home networks and enterprise networks, which may employ user accounts. Private networks do not necessarily employ encryption.
1	Private network with guest access	Private network but guest accounts are available. Example of this access network type is enterprise network offering access to guest users.
2	Chargeable public network	The network is accessible to anyone, however, access to the network requires payment. Further information on types of charges may be available through other methods (e.g., IEEE 802.21, http/https redirect or DNS redirection). Examples of this access network type is a hotspot in a coffee shop offering internet access on a subscription basis or a hotel offering in-room internet access service for a fee.
3	Free public network	The network is accessible to anyone and no charges apply for the network use. An example of this access network type is an airport hotspot or municipal network providing free service.
4	Personal device network	A network of personal devices. An example of this type of network is a camera attaching to a printer, thereby forming a network for the purpose of printing pictures.
5	Emergency services only network	A network dedicated and limited to accessing emergency services.
6 to 13	Reserved	Reserved
14	Test or experimental	The network is used for test or experimental purposes only.
15	Wildcard	Wildcard access network type

The Venue Info field is defined in 7.3.1.34.

The HESSID field, which is the identifier for a homogeneous ESS, specifies the value of HESSID, see 11.23.2. A STA uses this field to indicate the desired HESSID in an active scan per 11.1.3. The HESSID field for an AP is set to the value of dot11HESSID.

7.3.2.93 Advertisement Protocol element

The Advertisement Protocol element contains information that identifies a particular advertisement protocol and its corresponding Advertisement Control. The Advertisement Protocol element format is shown in Figure 7-95o120.

Element ID	Length	Advertisement Protocol Tuple # 1	Advertisement Protocol Tuple # 2 (optional)	...	Advertisement Protocol Tuple # n (optional)
Octets:	1	1	variable	variable	variable

Figure 7-95o120—Advertisement Protocol element format

The Length is a one-octet field whose value is equal to the sum of the lengths of the Advertisement Protocol Tuple fields.

The format of Advertisement Protocol Tuple is shown in Figure 7-95o121.

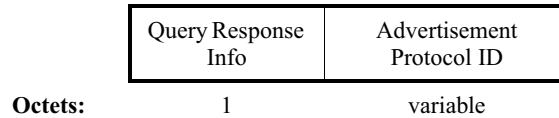


Figure 7-95o121—Advertisement Protocol Tuple format

The format of Query Response Info field is shown in Figure 7-95o122.

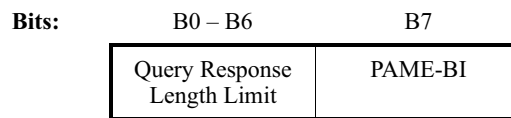


Figure 7-95o122—Query Response Info format

The Query Response Info field is defined as follows:

- The Query Response Length Limit indicates the maximum number of octets a STA will transmit in the Query Response field contained within one or more GAS Comeback Response frames. The Query Response Length Limit may be set to a value larger than the maximum MMPDU size in which case the Query Response spans multiple MMPDUs. The Query Response Length Limit is encoded as an integer number of 256 octet units. A value of zero is not permitted. A value of 0x7F means the maximum limit enforced is determined by the maximum allowable number of fragments in the GAS Query Response Fragment ID (see 7.3.1.33). The requesting STA sets the Query Response Length Limit to zero on transmission and the responding STA ignores it upon reception.
- Bit 7, the Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, is used by an AP to indicate whether the Advertisement Server, which is the non-AP STA's peer for this Advertisement Protocol, will return a Query Response that is independent of the BSSID used for the GAS frame exchange. This bit is set to 1 to indicate the Query Response is independent of the BSSID; it is set to zero to indicate that the Query Response may be dependent on the BSSID. See 11.23.3.1 for further information. Bit 7 is reserved for non-AP STAs.

The Advertisement Protocol ID is a variable length field. When this field contains a vendor specific Advertisement Protocol ID then this field will be structured per the Vendor Specific information element defined in 7.3.2.26, where the Element ID of the Vendor Specific information element of 7.3.2.26 is the first octet of the field and contains the vendor specific value for Advertisement Protocol ID defined in Table 7-43bi; otherwise its length is one octet and its value is one of the values in Table 7-43bi. When one or more vendor-specific tuples are included in the Advertisement Protocol element, their total length needs to be constrained such that the total length of all the Advertisement Protocol Tuple fields (both vendor specific and otherwise) is less than or equal to 255 octets.

- ANQP supports information retrieval from an Advertisement Server. ANQP is a protocol used by a requesting STA to query another STA (i.e., the receiving STA can respond to queries with or without proxying the query to a server in an external network). See 11.23.3.2 for information on ANQP procedures.
- MIH Information Service is a service defined in IEEE Std 802.21-2008 to support information retrieval from an information repository.

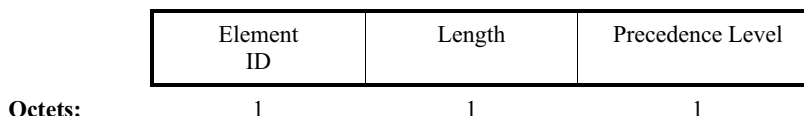
Table 7-43bi—Advertisement protocol ID definitions

Name	Value
Access Network Query Protocol (ANQP)	0
MIH Information Service	1
MIH Command and Event Services Capability Discovery	2
Emergency Alert System (EAS)	3
Reserved	4 – 220
Vendor Specific	221
Reserved	222 – 255

- MIH Command and Event Services capability discovery is a mechanism defined in IEEE 802.21 (see IEEE Std 802.21-2008) to support discovering capabilities of command service and event service entities in a STA or an external network.
- The EAS allows a network to disseminate emergency alert notifications from an external network to non-AP STAs. EAS uses the message format as defined in OASIS EDXL.
- Advertisement Protocol ID 221 is reserved for Vendor Specific Advertisement Protocols. When the Advertisement Protocol ID is equal to 221, the format of the Advertisement Protocol ID subfield follows the format of the Vendor Specific information element in 7.3.2.26.

7.3.2.94 Expedited Bandwidth Request information element

The Expedited Bandwidth Request information element is transmitted from a non-AP STA to an AP in an ADDTS Request frame containing a TSPEC element and provides usage information for the bandwidth request. The Expedited Bandwidth Request element format is shown in Figure 7-95o123.

**Figure 7-95o123—Expedited Bandwidth Request element format**

The Length field is 1.

The precedence level field is provided in Table 7-43bj.

The precedence levels are derived from the 3rd Generation Partnership Project (3GPP) document 3GPP TS 22.067 [B40].

The first responders (public) in Table 7-43bj are government agencies or entities acting on behalf of the government, and the first responders (private) are private entities, such as individuals or companies.

Table 7-43bj—Precedence Level field description

Precedence level value	Description
0 – 15	Reserved
16	Emergency call, defined in NENA 08-002 [B51]
17	First responder (public)
18	First responder (private)
19	MLPP Level A
20	MLPP Level B
21	MLPP Level 0
22	MLPP Level 1
23	MLPP Level 2
24	MLPP Level 3
25	MLPP Level 4
26 – 255	Reserved

7.3.2.95 QoS Map Set information element

The QoS Map Set information element is transmitted from an AP to a non-AP STA in a (Re)association Response frame or a QoS Map Configure frame and provides the mapping of higher layer quality of service constructs to User Priorities defined by transmission of Data frames in this standard. This information element maps the higher layer priority from the DSCP field used with the Internet Protocol to User Priority as defined by this standard. The QoS Map Set element is shown in Figure 7-95o124.

Element ID	Length	DSCP Exception #1 (optional)	...	DSCP Exception #n (optional)	UP 0 DSCP Range	UP 1 DSCP Range	UP 2 DSCP Range	...	UP 7 DSCP Range
Octets:	1	1	2	2	2	2	2	2	2

Figure 7-95o124—QoS Map Set element description

The Length field is set to $16+2 \times n$, where n is the number of Exception fields in the QoS Map set.

DSCP Exception fields are optionally included in the QoS Map Set. If included, the QoS Map Set has a maximum of 21 DSCP Exception fields. The format of the exception field is shown in Figure 7-95o125.

Figure 7-95o125—DSCP Exception format

	DSCP Value	User Priority
Octets:	1	1

The DSCP value in the DSCP Exception field is in the range 0 to 63 inclusive, or 255; the User Priority value is between 0 and 7, inclusive.

- When a non-AP STA begins transmission of a Data frame containing the Internet Protocol, it matches the DSCP field in the IP header to the corresponding DSCP value contained in this element. The non-AP STA will first attempt to match the DSCP value to a DSCP exception field and uses the UP from the corresponding UP in the same DSCP exception field if successful; if no match is found then the non-AP STA attempts to match the DSCP field to a UP n DSCP Range field, and uses the n as the UP if successful; and otherwise uses a UP of 0.
- Each DSCP Exception field has a unique DSCP Value.

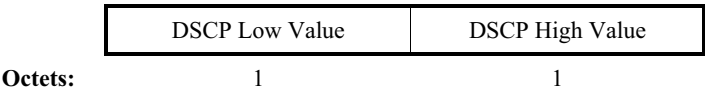


Figure 7-95o126—DSCP Range description

The QoS Map Set has a DSCP Range field corresponding to each of the 8 user priorities. The format of the range field is shown in Figure 7-95o126. The DSCP Range value is between 0 and 63 inclusive, or 255.

- The DSCP range for each user priority is non-overlapping.
- The DSCP High Value is greater than or equal to the DSCP Low Value.
- If the DSCP Range high value and low value are both equal to 255, then the corresponding UP is not used.

7.3.2.96 Roaming Consortium information element

The Roaming Consortium Information element contains information identifying the roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP transmitting this element; see 11.23.8. The element’s format is shown in Figure 7-95o127.

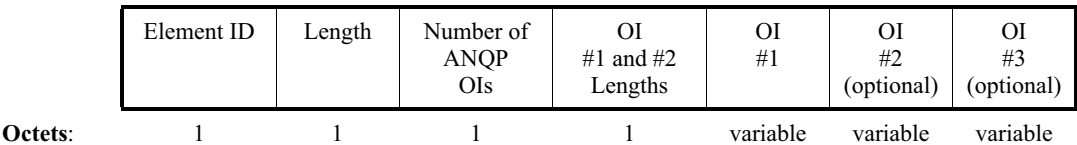


Figure 7-95o127—Roaming Consortium information element format

The Length is a one-octet field whose value is equal to 2 plus the sum of the number of octets in each OI field present.

The format of the Number of ANQP OIs field is a one-octet unsigned integer whose value is the number of additional roaming consortium organization identifiers (OIs) obtainable via ANQP. A value of zero means that no additional OIs will be returned in response to a ANQP query for the Roaming Consortium list. A value of 255 means that 255 or more additional OIs are obtainable via ANQP.

The OI #1 and #2 Lengths field format is shown in Figure 7-95o128.

- The value of the OI #1 Length subfield is the length in octets of the OI #1 field.
- The value of the OI #2 Length subfield is the length in octets of the OI #2 field. If the OI #2 field is not present, the value of the OI #2 Length subfield is set to zero.

NOTE—When there are three OIs, the OI #3 Length is calculated by subtracting sum of 2 plus the value of the OI #1 Length subfield plus the value of the OI #2 Length subfield from the value of the Length field.

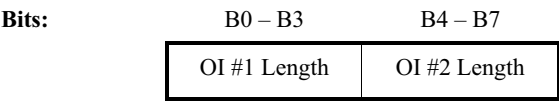


Figure 7-95o128—OI #1 and #2 Lengths field format

The OI field is defined in 7.3.1.31. Each OI identifies a roaming consortium (group of SSPs with inter-SSP roaming agreement) or a single SSP. The value of the OI(s) in this table are equal to the value of the first 3 OIs in the dot11RoamingConsortiumTable. If fewer than 3 values are defined in the dot11RoamingConsortiumTable, then only as many OIs as defined in the table are populated in this element. The values of the OIs in this element are equal to the values of the first OIs, up to 3, from the table.

7.3.2.97 Emergency Alert Identifier information element

The Emergency Alert Identifier information element provides a hash to identify instances of the active EAS messages that are currently available from the network. The hash allows the non-AP STA to assess whether an EAS message advertised by an AP has been previously received and therefore whether it is necessary to download from the network. The format of the Emergency Alert Identifier information element is provided in Figure 7-95o129.

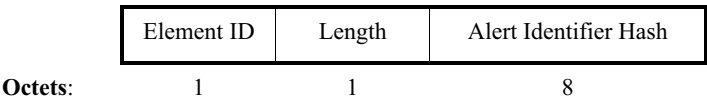


Figure 7-95o129—Emergency Alert Identifier information element format

The Length is a 1-octet field whose value is equal to 8.

The Alert Identifier Hash (AIH) is a 8-octet field. It is a unique value used to indicate an instance of an EAS message. The value of this field is the hash produced by the HMAC-SHA1-64 hash algorithm operating on the EAS message.

AIH =HMAC-SHA1-64(“ES_ALERT”, Emergency_Alert_Message)

Where AIH is then truncated to the first 64 bits of this function.

Emergency_Alert_Message is the EAS message itself.

Insert the following new subclauses (7.3.4 through 7.3.4.16) after 7.3.3:

7.3.4 Access Network Query Protocol (ANQP) elements

ANQP elements are defined to have a common format consisting of a 2-octet Info ID field, a 2-octet length field, and a variable-length element-specific information field. Each element is assigned a unique Info ID as defined in this standard. The ANQP element format is shown in Figure 7-95q. See X.1 for informative text on ANQP usage.

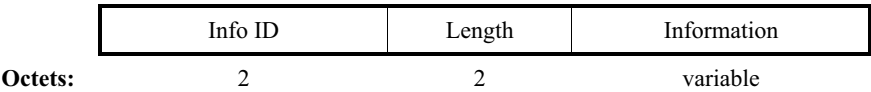


Figure 7-95q—ANQP element format

Each ANQP element in 7.3.4 is assigned a unique 2-octet Info ID. The set of valid Info IDs are defined in Table 7-43bk. The 2-octet Info ID is encoded following the conventions given in 7.1.1.

The Length field specifies the number of octets in the Information field and is encoded following the conventions given in 7.1.1.

The ANQP elements that may be configured are shown in Table 7-43bk. If information is not configured for a particular ANQP element, then a query for that element will return that element with all optional fields not present.

Table 7-43bk—ANQP information ID definitions

Information name	Information ID	ANQP information element (clause)
Reserved	0 – 255	n/a
ANQP Query list	256	7.3.4.1
ANQP Capability list	257	7.3.4.2
Venue Name information	258	7.3.4.3
Emergency Call Number information	259	7.3.4.4
Network Authentication Type information	260	7.3.4.5
Roaming Consortium list	261	7.3.4.6
IP Address Type Availability information	262	7.3.4.8
NAI Realm list	263	7.3.4.9
3GPP Cellular Network information	264	7.3.4.10
AP Geospatial Location	265	7.3.4.11
AP Civic Location	266	7.3.4.12
AP Location Public Identifier URI	267	7.3.4.13
Domain Name list	268	7.3.4.14

Table 7-43bk—ANQP information ID definitions (continued)

Information name	Information ID	ANQP information element (clause)
Emergency Alert Identifier URI	269	7.3.4.15
Emergency NAI	271	7.3.4.16
Reserved	272– 56796	n/a
ANQP vendor-specific list	56797	7.3.4.7
Reserved	56798 – 65535	n/a

7.3.4.1 ANQP Query list

The ANQP Query list provides a list of identifiers of ANQP elements for which the requesting STA is querying in an ANQP Query. The ANQP Query list element is included in a GAS Query Request.

The format of the ANQP Capability list is provided in Figure 7-95t.

	Info ID	Length	ANQP Query ID #1	ANQP Query ID #2 (optional)	...	ANQP Query ID #N (optional)
Octets:	2	2	2	0 or 2	...	0 or 2

Figure 7-95r—ANQP Query list format

The Info ID is a 2-octet field whose value is drawn from Table 7-43bn corresponding to the ANQP Query list.

The Length is a 2-octet field whose value is equal to 2 times the number of ANQP Query ID fields.

Each ANQP Query ID field value is an Info ID drawn from Table 7-43bn. Including an Info ID in the ANQP Query list declares that the STA performing the ANQP Query is requesting the ANQP element corresponding to that Info ID be returned in the ANQP Query Response. The Info IDs included in the ANQP Query list are ordered by monotonically increasing Info ID value.

7.3.4.2 ANQP Capability list

The ANQP Capability list provides a list of information/capabilities that has been configured on a STA. The ANQP Capability list element is returned in response to a GAS Query Request.

The format of the ANQP Capability list is provided in Figure 7-95s.

Info ID	Length	ANQP Capability #1	ANQP Capability #2 (optional)	...	ANQP Capability #N (optional)	ANQP Vendor- Specific list #1 (optional)	...	ANQP Vendor- Specific list #N (optional)
Octets:	2	2	0 or 2	...	0 or 2	variable	...	variable

Figure 7-95s—ANQP Capability list format

The Info ID is a 2-octet field whose value is drawn from Table 7-43bk corresponding to the ANQP Capability list.

The Length is a 2-octet field whose value is equal to 2 times the number of ANQP Capability fields following the Length field plus the sum of the lengths of the ANQP Vendor Specific lists.

Each ANQP Capability field value is an Info ID drawn from Table 7-43bk. If included in the ANQP Capability list, it declares that a query request for that Info ID will return the requested ANQP element. The Info ID for ANQP Capability list is always included in the ANQP Capability list returned in a GAS Query Response. The list does not include any duplicate Info IDs, except possibly the Info ID for the ANQP Vendor-specific list. The Info IDs returned in the ANQP Capability list are ordered by non-decreasing Info ID value.

The ANQP Vendor-specific list is defined in 7.3.4.7. The ANQP Vendor-specific list is structured such that the first 2 octets of the ANQP Vendor-specific list is the Info ID whose value corresponds to the ANQP Vendor-specific list (see Table 7-43bk). When an ANQP Vendor-specific list is present in the ANQP Capability list, the ANQP Vendor-specific list element contains the capabilities of that vendor-specific query protocol.

7.3.4.3 Venue Name information

The Venue Name information provides zero or more venue names associated with the BSS. The format of the Venue Name information is shown in Figure 7-95t. The Venue Name information may be used to provide additional metadata on the BSS. For example, this information may be used to assist a user in selecting the appropriate BSS with which to associate. Zero or more Venue Name fields may be included in the same or different languages.

Info ID	Length	Venue Info	Venue Name Duple #1 (optional)	Venue Name Duple #2 (optional)	...	Venue Name Duple #N (optional)
Octets:	2	2	variable	variable	...	variable

Figure 7-95t—Venue Name information format

The Info ID field is equal to the value in Table 7-43bk corresponding to the Venue Name information as defined in Figure 7-95t.

The Length is a 2-octet field whose value is equal to two plus the number of octets in Venue Name Duple fields.

The Venue Info field is defined in 7.3.1.34.