



**IEEE Standard for
Local and metropolitan area networks**

Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

Amendment 3: Management Plane Procedures and Services

**IEEE Computer Society
and the
IEEE Microwave Theory and Techniques Society**

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
31 December 2007

IEEE Std 802.16g™-2007
(Amendment to
IEEE Std 802.16™-2004)

IEEE Std 802.16g™-2007

(Amendment to
IEEE Std 802.16™-2004)

**IEEE Standard for
Local and metropolitan area networks**

**Part 16: Air Interface for Fixed and Mobile
Broadband Wireless Access Systems
Amendment 3: Management Plane
Procedures and Services**

Sponsor
LAN/MAN Standards Committee
of the
IEEE Computer Society
and the
IEEE Microwave Theory and Techniques Society



Approved 27 September 2007

IEEE-SA Standards Board

Abstract: This standard defines management procedures as enhancements to the IEEE 802.16 air interface standard for fixed and mobile broadband wireless systems. It specifies the management functions, interfaces, and protocol procedures.

Keywords: broadband wireless access, BWA, cellular layer, fixed broadband wireless access, MAN, management information base, MIB, microwave, mobile broadband wireless access, OFDM, OFDMA, radio, standard, WAS, wireless access systems, wireless metropolitan area network, WirelessMAN[®]

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

Copyright © 2007 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 31 December 2007. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-5687-3 STD95723
Print: ISBN 978-0-7381-5688-0 STDPD95723

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 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. When a document is more than five years old and has not been reaffirmed, 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 the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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.

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. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
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 802.16g-2007, IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems—Amendment 3: Management Plane Procedures and Services.

This amendment updates and expands IEEE Std 802.16 by defining Management Procedures as enhancements to the IEEE 802.16 air interface standard for fixed and mobile broadband wireless systems. It specifies the management functions, interfaces, and protocol procedures. As of the publication date, the current applicable version of IEEE Std 802.16 is IEEE Std 802.16-2004, as amended by IEEE 802.16f™-2005 and IEEE 802.16e™-2005.

Conformance test methodology

The multipart conformance test documents for IEEE Std 802.16 by “IEEE Standard 802.16/ConformanceXX.” For example, the first part of the conformance specification for IEEE 802.16 is designated “IEEE Standard 802.16/Conformance01.”

Notice to users

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 standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. 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 non-discriminatory. Further information may be obtained from the IEEE Standards Association.

Participants

This amendment was developed by the IEEE 802.16 Working Group on Broadband Wireless Access, which develops the WirelessMAN Standard for Wireless Metropolitan Area Networks.

IEEE 802.16 Working Group Officers

Roger B. Marks, *Chair*

Jose Puthenkulam, *Vice Chair*

Peiying Zhu, *Secretary*

Primary development was carried out by the Working Group's NetMan Task Group:

Phillip Barber, *Chair*

Achim Brandt, *Chief Technical Editor, IEEE 802.16g*

Jose Puthenkulam, *Co-Editor, IEEE 802.16g*

The following members of the IEEE 802.16 Working Group on Broadband Wireless Access participated in the Working Group Letter Ballot in which the draft of this standard was prepared and finalized for IEEE Ballot:

Ray Abrishami	Jaeweon Cho	Qiang Guo
Edward Agis	Kihyoung Cho	Zion Hadad
Aditya Agrawal	Seijei Cho	Jun Han
Siavash Alamouti	Seokheon Cho	Jung Ho Han
Murtaza Ali	Hyoung-Jin Choi	Seishi Hanaoka
Mario Aliotta	Yang-Seok Choi	Jeff Harrang
Dov Andelman	Joey Chou	Haixiang He
Gordon Antonello	Jin Young Chun	Gregory Scott Henderson
Eli Avivi	José Costa	Michael Hoghooghi
Phillip Barber	Mark Cudak	Chang-Lung Hsiao
Kevin Baum	Shujun Dang	Haiming Huang
Rajesh Bhalla	Wim Diepstraten	John Humbert
Yufei Blankenship	Frank Draper	Yerang Hur
Eckard Bogenfeld	Krzysztof Dudzinski	InSeok Hwang
Achim Brandt	Lester Eastwood	Bin-Chul Ihm
Thomas Brown	Tomas Edler	Jiho Jang
Sean Cai	Carl Eklund	Jaeho Jeon
James Carlo	Yigal Eliaspur	David Johnston
Giulio Cavalli	Frank Exeler	Panyuh Joo
Jaesun Cha	Torsten Fahldieck	Hyunjeong Kang
Chan-Byoung Chae	Yonggang Fang	Ivy Kelly
Dean Chang	Peretz Feder	Ofer Kelman
Jae Hwan Chang	Dazi Feng	Brian Kiernan
Sungcheol Chang	Mo-Han Fong	Beomjoon Kim
Yong Chang	Avraham Freedman	Bong Ho Kim
Naftali Chayat	Yan Fu	Byoung-Jo Kim
Rémi Chayer	Mike Geipel	Dae-Joong Kim
Jennifer Chen	Pieter-Paul Giesberts	Jaeyoel Kim
Yuehua (Lucy) Chen	Nikhil Goel	Jung Won Kim
Aik Chindapol	Mariana Goldhamer	Min Sung Kim
Hua (Mary) Chion	Reza Golshan	Ronny (Yong-Ho) Kim
Jaehae Cho	David Grandblaise	Youngho Kim

Itzik Kitroser
Chris Knudsen
Changhoi Koo
Havish Koorapaty
Lalit Kotecha
Toshiyuki Kuze
Dong Seung Kwon
Jonathan Labs
Kari Laihonon
Jules Pierre Lamoureux
Chang-jae Lee
Chi-Chen Lee
Jae Hak Lee
Mihyun Lee
Sungjin Lee
Yigal Leiba
Jia-Ru Li
Jiang Li
Kemin Li
Li Li
Thomas Li
Xiaodong Li
Yongmao Li
Gaspard Licitra
Aeri Lim
Geunhwi Lim
Hyoung Kyu Lim
Hyoungsoo Lim
Zhibin Lin
Titus Lo
Hui-Ling Lou
Heinz Lycklama
Michael Lynch
Steve Ma
Seung Joo Maeng
David Maez
Mahesh Makhijani
Jeffrey Mandin
Roger Marks
David McGinniss
Scott Migaldi
James Mollenauer
Roland Muenzner
Willem Mulder

Ronald Murias
Kenichi Nakamura
K.S. Natarajan
Mitsuo Nohara
Paul Odlyzko
Shlomo Ovadia
David Paranchych
Youngsoo Park
Roger Peterson
Bonnie Petti
Greg Phillips
Paul Piggini
Ambroise Popper
Scott Probasco
Jose Puthenkulam
Nanjian (Jeff) Qian
Hongyun Qu
Shyamal Ramachandran
Frank Rayal
Eric Reifsnider
Francis Retnasothie
Maximilian Riegel
Wonil Roh
Herbert Ruck
Kiseon Ryu
Andrew Sago
Yousuf Saifullah
Kenji Saito
Atul Salvekar
Jörg Schmidt
Christian Seagren
Yossi Segal
Radu Selea
N. K. Shankaranarayanan
Eliyahu Shasha
Gang Shen
Yabing Shen
James Simkins
Sten Sjöberg
Jung Je Son
Yeong Moon Son
Kenneth Stanwood
Kyungjoo Suh

Xiangguo Tang
Yongjoo Tcha
Wen Tong
Shiau-He Tsai
Rainer Ullmann
Mano Vafai
Lucia Valbonesi
Richard Van Leeuwen
Eyal Verbin
Dorin Viorel
Frederick Vook
Arthur Wang
Fan Wang
Guo qiang Wang
Irving Wang
Lei Wang
Stanley Wang
Mattias Wennstrom
Alfred Wiecezorek
Geng Wu
Jun Wu
Xuyong Wu
David Xiang
Ling Xu
Shanshan Xu
Hassan Yaghoobi
Weidong Yang
Yunsong Yang
Ran Yaniv
Vladimir Yanover
Choong Il Yeh
Hujun Yin
Chulsik Yoon
Soon Young Yoon
Aeran Youn
Jungnam Yun
Mi-Young Yun
Nader Zein
Wenfeng Zhang
Zhijian Zhang
Ruobin Zheng
Qun Zhou
Peiying Zhu
Ilan Zohaz

The following members of the IEEE Balloting Committee voted on this standard, whether voting for approval or disapproval, or abstaining.

Sassan Ahmadi	John J. Humbert	David W. Paranchych
Butch Anton	David Hunter	Donald M. Parker
Mikio Aoki	Atsushi Ito	Roger L. Peterson
Reza Arefi	Raj Jain	Paul Piggin
Lee R. Armstrong	Alan Jette	Subburajan Ponnuswamy
Phillip Barber	Brian Johnson	Michael S. Probasco
John R. Barr	David Johnston	Vikram Punj
Kevin L. Baum	Oh Jongtaek	Jose Puthenkulam
Gennaro Boggia	Bobby Jose	Maximilian Riegel
Matthew Burnburg	Shinkyoo Kaku	Robert A. Robinson
Alistair Buttar	Hyunjeong Kang	Randall M. Safier
Sean Cai	Piotr Karocki	Andy J. Sago
James Carlo	Stuart J. Kerry	Osman Sakr
Juan C. Carreon	Brian Kiernan	Atul A. Salvekar
David A. Castelow	Eunkyoung Kim	Bartien Sayogo
Jay Catelli	Kyung Ho Kim	Suman Sharma
Giulio Cavalli	Sang Youb Kim	Takashi Shono
Dean Chang	Yongbum Kim	Mario Siller
Naftali Chayat	Yongho Kim	Rajnish D. Singh
Yi-Ming Chen	Patrick W. Kinney	Sten I. Sjoberg
Yung-Mu Chen	Itzik Kitroser	Jung Je Son
Elizabeth Chesnutt	Thomas Kurihara	Amjad A. Soomro
Aik Chindapol	Jules Pierre Lamoureux	Kenneth L. Stanwood
Joey Chou	Jeremy Landt	Thomas Starai
Keith Chow	Yigal Leiba	Rene Struik
Bryan P. Cook	Li Li	Walter Struppler
Tommy Cooper	Jan-Ray Liao	Mark A. Sturza
Jose M. Costa	Chiwoo Lim	Alourdes T. Sully
Javier Del-Prado-Pavon	Hyoung-Kyu Lim	Joseph Tardo
Russell S. Dietz	Xiaoyu Liu	Wen Tong
Thomas J. Dineen	G. Luri	Shiau-He Tsai
Sourav Dutta	Heinz Lycklama	Mark-Rene Uchida
Paul S. Eastman	Dave Maez	Lee B. Valerius
Lester F. Eastwood	Roger Marks	Richard Van Leeuwen
C. J. Fitzgerald	Jon S. Martens	John Visser
Mo-Han Fong	Michael D. Mcinnis	Guo Qiang Wang
Avraham Freedman	Scott F. Migaldi	Lei Wang
Devon L. Gayle	Apurva N. Mody	Michael Wang
Michael D. Geipel	James F. Mollenauer	Stanley Wang
Pieter-Paul Giesberts	Ronald G. Murias	Stephen Webb
Mariana Goldhamer	Michael Newman	Mattias Wennstrom
Ron K. Greenthaler	Richard H. Noens	Yunsong Yang
Randall Groves	Mitsuo Nohara	Vladimir Yanover
C. Guy	Satoshi Obara	Oren Yuen
Siamack Haghighi	Chris Osterloh	Jungnam Yun
C. J. Hansen	Satoshi Oyama	Peiying Zhu
John Hawkins		Juan C. Zuniga

When the IEEE-SA Standards Board approved this standard on 27 September 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio
Alex Gelman
William R. Goldbach
Arnold M. Greenspan
Joanna N. Guenin
Julian Forster*
Kenneth S. Hanus
William B. Hopf
Richard H. Hulett

Hermann Koch
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Tom A. Prevost

Narayanan Ramachandran
Greg Ratta
Robby Robson
Anne-Marie Sahazizian
Virginia C. Sulzberger
Malcolm V. Thaden
Richard L. Townsend
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*

Michelle D. Turner
IEEE Standards Program Manager, Document Development

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

Contents

1. Overview	1
1.1 Scope	1
1.1.1 Interpretation	1
1.2 Purpose	2
1.4 Reference model	2
1.4.2 IEEE 802.16 entity	3
1.4.3 Network Control and Management System	3
1.4.4 Network reference model	4
1.4.4.1 SS/MS and BS interface	4
1.4.4.2 IEEE 802.16 entity to NCMS interface	4
1.4.5 Management SAP (M-SAP)	5
1.4.6 Control SAP (C-SAP)	5
2. References	5
3. Definitions	6
4. Abbreviations and acronyms	6
5. Service-specific CS	9
5.3 Generic packet convergence sublayer (GPCS)	9
5.3.1 Mapping of the GPCS service to upper layers	10
5.3.2 Operation of GPCS with SSs that do not support the GPCS	10
5.3.3 GPCS SAP parameters	11
5.3.4 GPCS_DATA.request	11
5.3.4.1 Function	11
5.3.4.2 Semantics of the service primitive	11
5.3.4.3 When generated	11
5.3.4.4 Effect of receipt	12
5.3.5 GPCS_DATA.indication	12
5.3.5.1 Function	12
5.3.5.2 Semantics of the service primitive	12
5.3.5.3 When generated	12
5.3.5.4 Effect of receipt	12
5.3.6 PHS operation	12
6. MAC common part sublayer	13
6.3 Data/Control plane	13
6.3.2 MAC PDU formats	13
6.3.2.3 MAC management messages	13
6.3.2.3.1 Downlink Channel Descriptor (DCD) message	13
6.3.2.3.2 Downlink map (DL-MAP) message	13
6.3.2.3.3 Uplink Channel Descriptor (UCD) message	14
6.3.2.3.6 Ranging Response (RNG-RSP) message	14
6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)	14

6.3.2.3.23	SS Basic Capability Request (SBC-REQ) message	16
6.3.2.3.24	SS Basic Capability Response (SBC-RSP) message	16
6.3.2.3.47	Neighbor Advertisement (MOB_NBR-ADV) message	17
6.3.2.3.62	MIH Payload Transfer message (MOB_MIH-MSG)	17
6.3.2.3.63	Service Identity Information (SII-ADV) message	18
6.3.2.3.64	Location-based services (LBS-ADV) message	19
6.3.9.2	Obtain downlink parameters	19
6.3.9.3	Obtain uplink parameters	20
6.3.9.5.1	Contention-based initial ranging and automatic adjustments	20
6.3.9.8	SS authorization and key exchange	21
6.3.10.3	OFDMA-based ranging	21
6.3.10.3.1	Contention-based initial ranging and automatic adjustments	21
6.3.10.3.4	Dedicated ranging and automatic adjustments	21
6.3.22.2.2	HO decision and initiation	22
6.3.24.2	Cell selection	23
6.3.25	MIHF support	23
6.3.26	Location-based services	24
6.3.26.1	Time Difference of Arrival (TDOA)	24
8. PHY		25
8.4.4.5	Uplink transmission allocations	25
8.4.5.4	UL-MAP IE format	25
9. Configuration		27
9.1.2	Mobile IP v4 fields used by the MS	27
10. Parameters and constants		28
10.1 Global values		28
11. TLV encodings		29
11.1 Common encodings		29
11.1.2.1	HMAC Tuple	29
11.1.3	MAC version encoding	30
11.1.8	NSP List encodings	30
11.1.8.1	NSP List	30
11.1.8.2	Verbose NSP Name List	30
11.1.9	MIH message encodings	31
11.1.9.1	MIHF frame	31
11.1.9.2	MIHF frame type	31
11.1.9.3	Cycle	32
11.1.9.4	Delivery method and status code	32
11.1.9.5	Query ID	32
11.3.1	UCD channel encodings	33
11.4.1	DCD channel encodings	34
11.6 RNG-RSP management message encodings		35
11.7.7.1	Classification/PHS options and SDU encapsulation support	36
11.8.9	Service Information Query (SIQ)	36

11.8.10	MIH Capability Supported.....	37
11.8.11	Visited NSP ID	37
11.8.12	Auth Type for Single EAP	38
11.8.13	Visited NSP Realm	38
11.8.14	SII-ADV Message Pointer	38
11.13	Service flow management encodings	39
11.13.19	CS specific service flow encodings	39
11.13.19.1	CS specification	39
11.13.19.2	CS Parameter encoding rules.....	40
11.13.19.5	GPCS CS encodings for configuration and MAC messaging	40
11.13.19.5.1	GPCS PROTOCOL_TYPE encoding.....	40
11.13.38	Packet Error Rate (PER).....	41
11.20	Device Coordinates	42
14.	Management interfaces and procedures.....	47
14.1	Service primitive template	47
14.1.1	Universal naming schema for SAP service primitive	47
14.1.2	SAP service primitive object format.....	48
14.1.2.1	M-SAP/C-SAP operation service primitive:.....	48
14.1.2.2	M-SAP/C-SAP notification service primitive:	49
14.1.3	SAP service primitive flow diagram template	51
14.2	Management and control functions.....	51
14.2.1	Accounting management	51
14.2.1.1	Accounting procedure	51
14.2.1.2	Service primitives for accounting management.....	53
14.2.1.2.1	M-ACM-REQ	53
14.2.1.2.2	M-ACM-RSP	53
14.2.1.2.3	M-ACM-IND	54
14.2.2	Security management.....	55
14.2.2.1	EAP-based authentication procedure.....	55
14.2.2.1.1	C-SM-IND	56
14.2.2.2	RSA-based authentication procedure.....	62
14.2.2.2.1	C-SM-IND	62
14.2.2.2.2	C-SM-REQ	64
14.2.2.2.3	C-SM-RSP	65
14.2.2.3	Security for handoffs (EAP only)	66
14.2.2.3.1	Service primitives	67
14.2.3	IP management with Secondary Management Connection	69
14.2.3.1	M-SMC-IND.....	70
14.2.3.1.1	M-SMC-IND (Event_Type = SMC-PAYLOAD)	70
14.2.3.1.2	M-SMC-IND(Event_Type = IP_ALLOCATION).....	71
14.2.4	Subscriber mode management	72
14.2.4.1	Managing device states	72
14.2.4.2	Idle mode management primitives.....	74

14.2.4.2.1	C-IMM-REQ	76
14.2.4.2.2	C-IMM-RSP	79
14.2.4.2.3	C-IMM-ACK	82
14.2.4.2.4	C-IMM-IND	83
14.2.4.3	Location Update procedure	84
14.2.4.3.1	C-IMM-REQ	85
14.2.4.3.2	C-IMM-RSP	86
14.2.4.3.3	C-IMM-IND	88
14.2.5	Handover management	89
14.2.5.1	Handover context for connections	89
14.2.5.2	Handover control protocol procedures	89
14.2.5.2.1	C-HO-REQ	94
14.2.5.2.2	C-HO-RSP	100
14.2.5.2.3	C-HO-IND	105
14.2.5.3	MIH control protocol procedures	109
14.2.5.3.1	C-MIH-IND	110
14.2.6	Radio resource management	111
14.2.6.1	C-RRM-REQ	113
14.2.6.1.1	C-RRM-REQ (Action_Type = spare capacity report)	113
14.2.6.1.2	C-RRM-REQ (Action_Type = PHY report)	114
14.2.6.2	C-RRM-RSP	115
14.2.6.2.1	C-RRM-RSP (Action_Type = spare capacity report)	115
14.2.6.2.2	C-RRM-RSP (Action_Type = PHY Report)	116
14.2.6.3	C-RRM-IND	117
14.2.6.3.1	C-RRM-IND (Event_Type = spare capacity report)	118
14.2.6.3.2	C-RRM-IND (Event_Type = Neighbor-BS Radio Resource Status Update)	119
14.2.7	Network entry and exit management	121
14.2.7.1	C-NEM-REQ	125
14.2.7.1.1	C-NEM-REQ (Action_Type = Ranging)	125
14.2.7.1.2	C-NEM-REQ (Action_Type = SS Basic Capability)	127
14.2.7.1.3	C-NEM-REQ (Action_Type = Registration)	128
14.2.7.1.4	C-NEM-REQ (Action_Type = Deregistration)	129
14.2.7.2	C-NEM-RSP	130
14.2.7.2.1	C-NEM-RSP (Action_Type = Ranging)	131
14.2.7.2.2	C-NEM-RSP (Action_Type = SS Basic Capability)	132
14.2.7.2.3	C-NEM-RSP (Action_Type = Registration)	133
14.2.7.2.4	C-NEM-RSP (Action_Type = Deregistration)	135
14.2.7.3	C-NEM-IND (Event_Type = NBR_BS_Update)	136
14.2.7.3.1	Function	136
14.2.7.3.2	Semantics	136
14.2.7.3.3	When generated	137
14.2.7.3.4	Effect of receipt	137
14.2.7.4	C-NEM-IND (Event_Type = network attached)	137

14.2.7.4.1	Function	137
14.2.7.4.2	Semantics of the service primitive.....	137
14.2.7.4.3	When generated	137
14.2.7.4.4	Effect of receipt	137
14.2.8	Subscriber Station Management	137
14.2.8.1	M-SSM-REQ	140
14.2.8.1.1	M-SSM-REQ (Action_Type = Power On)	140
14.2.8.1.2	M-SSM-REQ (Action_Type = Power Down)	140
14.2.8.1.3	M-SSM-REQ (Action_Type = Reset)	141
14.2.8.1.4	M-SSM-REQ (Action_Type = Hold)	142
14.2.8.1.5	M-SSM-REQ (Action_Type = Normal)	142
14.2.8.2	M-SSM-RSP	143
14.2.8.2.1	M-SSM- RSP (Action_Type = Power On)	143
14.2.8.2.2	M-SSM- RSP (Action_Type = Power Down)	144
14.2.8.2.3	M-SSM- RSP (Action_Type = Reset)	144
14.2.8.2.4	M-SSM-RSP (Action_Type = Hold)	145
14.2.8.2.5	M-SSM-RSP (Action_Type = Normal)	145
14.2.8.3	M-SSM-IND	146
14.2.8.3.1	M-SSM-IND (Event_Type = Reset).....	146
14.2.8.3.2	M-SSM-IND (Event_Type = Hold).....	147
14.2.8.3.3	M-SSM-IND (Event_Type = Normal)	147
14.2.9	QoS management.....	148
14.2.9.1	C-SFM-REQ	151
14.2.9.1.1	C-SFM-REQ (Operation_Type = Create).....	151
14.2.9.1.2	C-SFM-REQ (Operation_Type = Set)	152
14.2.9.1.3	C-SFM-REQ (Operation_Type = Delete).....	153
14.2.9.2	C-SFM-RSP	154
14.2.9.2.1	C-SFM-RSP (Operation_Type = Create)	154
14.2.9.2.2	C-SFM-RSP (Operation_Type = Set).....	156
14.2.9.2.3	C-SFM-RSP(Operation_Type = Delete)	157
14.2.10	Multicast and Broadcast Service Management.....	157
14.2.10.1	MBS capability discovery.....	158
14.2.10.1.1	C-MBS-REQ (Get)	158
14.2.10.1.2	C-MBS-RSP (Get)	159
14.2.10.2	MBS Configuration Management Setting	160
14.2.10.2.1	C-MBS-REQ (Set).....	160
14.2.10.2.2	C-MBS-RSP (Set).....	161
14.2.10.3	MBS Configuration Management Layout	162
14.2.10.3.1	C-MBS-IND (MBS Portion Layout)	163
14.2.10.3.2	C-MBS-REQ.....	165
14.2.10.3.3	C-MBS-RSP.....	166
14.2.11	LBS Management	168
14.2.11.1	C-LBS-REQ.....	168

14.2.11.1.1	Function	168
14.2.11.1.2	Semantics of the service primitive.....	168
14.2.11.1.3	When generated	169
14.2.11.1.4	Effect of receipt:	169
14.2.11.2	C-LBS-ACK	169
14.2.11.2.1	Function	169
14.2.11.2.2	Semantics of the service primitive.....	169
14.2.11.2.3	When generated	169
14.2.11.2.4	Effect of receipt	169
14.2.11.3	C-LBS-RSP.....	170
14.2.11.3.1	Function	170
14.2.11.3.2	Semantics of the service primitive.....	170
14.2.11.3.3	When generated	170
14.2.11.3.4	Effect of receipt	170
Annex I (informative)	Handover, ranging, and MIH procedures	169
I.1	Hard handover procedures	169
I.2	End-to-end handover procedures	171
I.3	Fast base station switching procedures	172
I.4	Ranging primitives usage.....	174
I.5	MIH exchange procedure prior to authentication	175
Annex J (informative)	U-TDOA measurement	177
J.1	General U-TDOA method	178
J.2	Special U-TDOA method	180

List of Tables

Table 14—MAC management messages.....	13
Table 26—PKM message codes.....	14
Table 37s—MIH Initial Request attributes.....	15
Table 37t—MIH Acknowledge attributes.....	15
Table 37u—MIH Comeback Response attributes.....	16
Table 109f—MOB_NBR-ADV message format.....	17
Table 109ya—MOB_MIH-MSG message format.....	17
Table 109yb—Service Identity Information (SII-ADV) message format.....	18
Table 109yc—Location-based services (LBS-ADV) message format.....	19
Table 287—OFDMA UL-MAP IE format.....	25
Table 342—Parameters and constants.....	28
Table 346—Type values for common TLV encodings.....	29
Table 347—HMAC Tuple definition.....	29
Table 348a—CMAC Tuple definition.....	29
Table 349—UCD channel encodings.....	33
Table 358—DCD channel encodings.....	34
Table 367—RNG-RSP message encodings.....	35
Table 367—RNG-RSP message encodings.....	35
Table 383—Service flow encodings.....	39

List of Figures

Figure 1—IEEE Std 802.16 protocol architecture model.....	2
Figure 1a—Illustration of the Network Control and Management System (informative)	3
Figure 1b—IEEE 802.16 network reference model	4
Figure 17c—GPCS layering model	10
Figure 470—SAP Service primitive flow diagram template.....	51
Figure 471—Accounting primitive initiated by a BS	52
Figure 472—Accounting primitives initiated by the NCMS.....	52
Figure 473—EAP-based authentication procedure	56
Figure 474—RSA-based authentication procedure	62
Figure 475—Context transfer primitives initiated by a serving BS	66
Figure 476—Context transfer primitives initiated by a target BS	67
Figure 477—SMC IP address signaling transport and notification.....	70
Figure 478—Subscriber mode transition diagram at MS and BS	73
Figure 479—Subscriber mode transition diagram at NCMS (on BS and MS side)	74
Figure 480—Idle mode initiation (initiated by the NCMS on the MS side)	74
Figure 481—Idle mode initiation (initiated by the NCMS on the BS side)	75
Figure 482—Paging Announce	75
Figure 483—Network re-entry from Idle mode primitives	76
Figure 484—Location Update primitives.....	84
Figure 485—HO primitives flow between Serving BS and NCMS, BS initiated.....	90
Figure 486—HO primitives flow between serving BS and NCMS, NCMS initiated	90
Figure 487—Primitive flow between NCMS at the MS and the MS when HO is initiated.....	91
Figure 488—HO primitives flow between MS and NCMS(MS side) for sending MOB_HO-IND	91
Figure 489—HO primitives flow between target BS and NCMS	92
Figure 490—HO primitives flow between IEEE 802.16 entity (BS) and NCMS for scanning.....	92
Figure 491—HO primitives flow between IEEE 802.16 entity (MS) and NCMS for local scanning report.....	93
Figure 492—HO primitives flow between IEEE 802.16 entity (MS) and NCMS for Remote Scanning Report	93
Figure 493—Primitives for association ranging report	94
Figure 494—MIH primitive flow between IEEE 802.16 entity and NCMS for IEEE P802.21 support	110
Figure 495—Primitive flow of C-RRM-REQ/RSP.....	111
Figure 496—Primitive flow of C-RRM-IND (Neighbor-BS Radio Resource Status Update)	112
Figure 497—Primitive flow of C-RRM-IND (spare capacity report)	112
Figure 498—Ranging primitives	121
Figure 499—SS basic capability negotiation primitives	122
Figure 500—Registration primitives (SS and BS)	122
Figure 501—Network attachment	123
Figure 502—IEEE 802.16 entity (MS) and NCMS primitives when MOB_NBR_ADV message is received	123
Figure 503—Network deregistration primitives by SS	124
Figure 504—Network deregistration primitives by BS	124
Figure 505—M-SSM primitives flow for Reset / Power On / Power Down at SS side.....	138
Figure 506—M-SSM primitives flow for Reset.....	138
Figure 507—M-SSM primitives flow for Hold and Normal resumption.....	139
Figure 508—M-SSM primitives flow for Hold and Reset	139
Figure 509—SFM-REQ(Create/Set) and C-SFM-RSP(Create/Set) flow, IEEE 802.16 entity initiated....	149
Figure 510—C-SFM-REQ (create and Set) and C-SFM-RSP (Create and Set) primitives flow, NCMS initiated.....	149
Figure 511—C-SFM-REQ(Delete) and C-SFM-RSP(Delete) primitives flow, IEEE 802.16 entity initiated	150

Figure 512—C-SFM-REQ(Delete) and C-SFM-RSP(Delete) primitives flow, NCMS initiated	150
Figure 513—C-MBS-REQ (Get) and C-MBS-RSP (Get) primitives flow	158
Figure 514—MBS Zone Configuration and Management	160
Figure 515—C-MBS-IND (Layout) primitive flow	162
Figure 516—MBS Service Flow (Create and Delete)	162
Figure 517—LBS Management primitives	168
Figure I.1—Example primitive flow of HO initiated by MS	169
Figure I.2—Example primitive flow of HO initiated by the NCMS	170
Figure I.3—MS Initiated HO: End-to-end HO exchange between MS, Serving BS, and Target BS	171
Figure I.4—BS Initiated HO: End-to-end HO exchange between MS, Serving BS, and Target BS	171
Figure I.5—Example primitive flow of Active Set Update (Add)	172
Figure I.6—Example primitive flow of Active Set Update (Drop)	172
Figure I.7—Example primitive flow of Anchor BS Update (Using MAC messages)	173
Figure I.8—Example primitive flow of Anchor BS Update (Using selection feedback mechanism)	173
Figure I.9—Use of ranging primitives	174
Figure I.10—Use of fast ranging primitives	174
Figure I.11—Pre-authenticated MIH exchange using broadcast delivery method	175
Figure I.12—Pre-authenticated MIH exchange using unicast delivery method	176
Figure J.1—Network diagram for U-TDOA measurement	177
Figure J.2—U-TDOA measurement timing diagram (general U-TDOA method)	178
Figure J.3—U-TDOA measurement algorithm (general U-TDOA method)	179
Figure J.4—U-TDOA measurement timing diagram (special U-TDOA method)	181
Figure J.5—U-TDOA measurement algorithm (special U-TDOA method)	182

IEEE Standard for Local and metropolitan area networks

Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

Amendment 3: Management Plane Procedures and Services

NOTE—The editing instructions contained in this amendment define how to merge the material contained herein into the existing base standard IEEE Std 802.16TM, which consists of IEEE Std 802.16-2004 and its errata and amendments at the time of IEEE Std 802.16gTM approval (i.e., IEEE Std 802.16eTM and IEEE Std 802.16fTM).

The editing instructions are shown ***bold italic***. Four editing instructions are used: ***change***, ***delete***, ***insert***, and ***replace***. ***Change*** is used to make small 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 large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

1.1 Scope

Insert the following text into 1.1 after the last paragraph, before 1.2:

In addition, based on IEEE Std 802.16g, this document provides enhancements to the MAC and PHY management entities of IEEE Std 802.16-2004, as amended by IEEE Std 802.16e-2005¹ and IEEE Std 802.16f-2005, to create standardized procedures and interfaces for the management of conformant IEEE 802.16 devices.

1.1.1 Interpretation

This document includes material for the following:

- a) Enhancements of the radio interface MAC Management messages

¹Information on references can be found in Clause 2.

- b) Enhancements of the radio interface data plane capabilities
- c) Introduction of a set of control and management primitives for the IEEE 802.16 entities, as a specification for the design of protocols for control and management of IEEE 802.16 entities in a network

1.2 Purpose

Insert the following text into 1.2 after the last paragraph, before 1.3:

In addition, based on IEEE Std 802.16g, the purpose of this standard is to provide conformant IEEE 802.16 equipment with procedures and services to enable interoperable and efficient management of network resources, mobility, and spectrum, and to standardize management plane behavior in IEEE 802.16 fixed and mobile devices.

1.4 Reference model

Replace Figure 1 with the following:

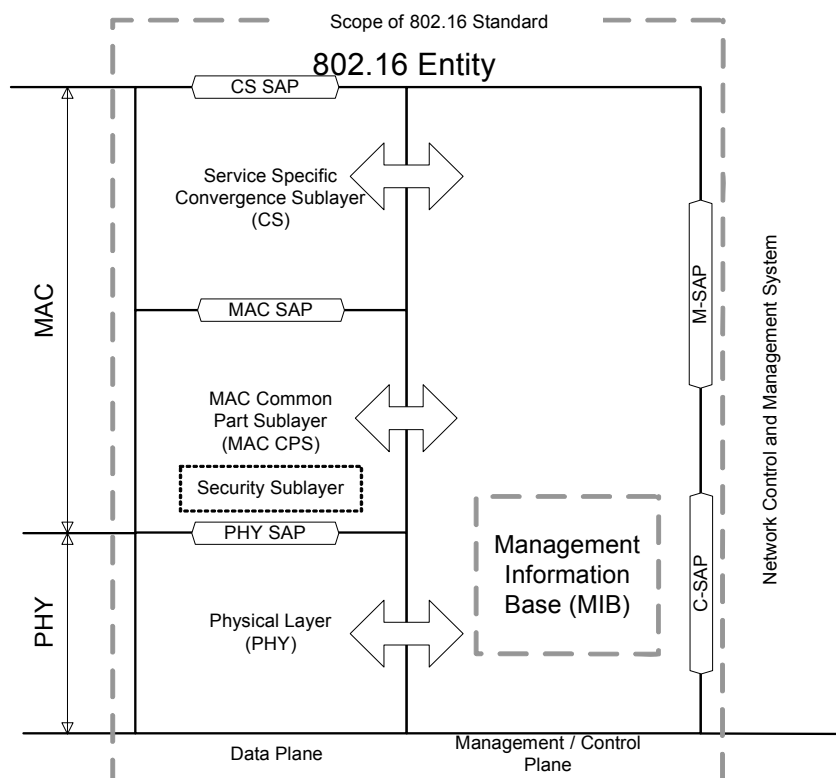


Figure 1—IEEE Std 802.16 protocol architecture model

Insert the following new paragraph at the end of 1.4, before 1.4.1:

The IEEE 802.16 devices can include subscriber stations (SS), mobile stations (MS), or base stations (BS). As the IEEE 802.16 devices may be part of a larger network and therefore would require interfacing with entities for management and control purposes, a Network Control and Management System (NCMS) abstraction has been introduced in this standard as a “black box” containing these entities. The NCMS

abstraction allows the PHY/MAC layers specified in IEEE Std 802.16 to be independent of the network architecture, the transport network, and the protocols used at the backend and therefore allows greater flexibility. NCMS logically exists at BS side and SS/MS side of the radio interface, termed NCMS(BS) and NCMS(SS/MS), respectively. Any necessary inter-BS coordination is handled through the NCMS(BS).

This standard includes a Control SAP (C-SAP) and Management SAP (M-SAP) that expose control plane and management plane functions to upper layers. The C_SAP and M-SAP interfaces are described in Clause 14. The NCMS uses the C-SAP and M-SAP to interface with the IEEE 802.16 entity. In order to provide correct MAC operation, NCMS shall be present within each SS/MS. The NCMS is a layer independent entity that may be viewed as a management entity or control entity. General system management entities can perform functions through NCMS and standard management protocols can be implemented in the NCMS.

Insert the following new subclauses into 1.4:

1.4.2 IEEE 802.16 entity

An IEEE 802.16 entity is defined as the logical entity in an SS/MS or BS that comprises the PHY and MAC layers of the Data Plane and the Management/Control Plane.

1.4.3 Network Control and Management System

This abstraction is detailed in Figure 1a to show the different functional entities that make up such a NCMS. These entities may be centrally located or distributed across the network. The exact functionality of these entities and their services is outside the scope of this specification, but shown here for illustration purposes and to better enable the description of the management and control procedures.

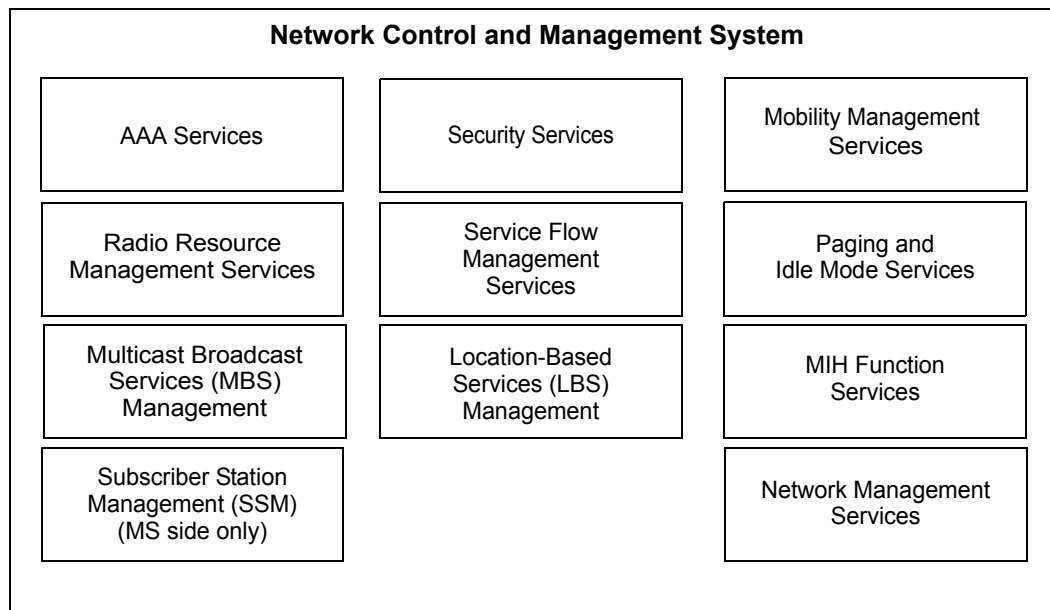


Figure 1a—Illustration of the Network Control and Management System (informative)

NCMS protocols are not defined in this specification; however, information elements (IEs) and protocol primitives for these IEs are exposed using primitives via SAP. This includes MAC and PHY layer context information used by NCMS protocols to manage and control the air interface. NCMS service manifestations on the SS/MS and BS may have different configurations and functions.

NOTE—For the NAS-Port-Type RADIUS Attribute 61 [see IETF RFC 2865], the IEEE 802.16 AAA service in the NCMS is assigned the value “27”.²

1.4.4 Network reference model

Figure 1b describes a simplified network reference model. Multiple SS or MS may be attached to a BS. SS or MS communicate to the BS over the U interface using a Primary Management connection, a Basic connection, or a Secondary Management connection.

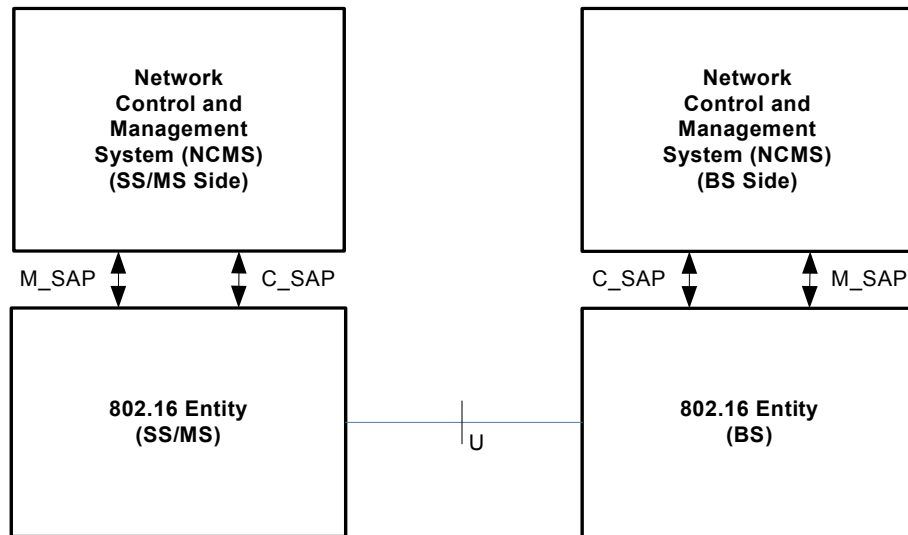


Figure 1b—IEEE 802.16 network reference model

1.4.4.1 SS/MS and BS interface

This standard observes the following correlation:

- MAC management PDUs that are exchanged on the Basic Management connection trigger or are triggered by primitives that are exchanged over the C-SAP.
- MAC management PDUs that are exchanged on the Primary Management connection trigger or are triggered by primitives that are exchanged over either the C-SAP or the M-SAP depending on the particular management or control operation.
- Messages that are exchanged over the Secondary Management connection trigger or are triggered by primitives that are exchanged over the M-SAP.

1.4.4.2 IEEE 802.16 entity to NCMS interface

This interface is a set of SAP between an IEEE 802.16 entity and NCMS and is represented in Figure 1 and Figure 1b. It is decomposed into two parts: the M-SAP is used for less time-sensitive Management plane primitives and the C-SAP is used for more time sensitive Control plane primitives that support handovers,

²Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

security context management, radio resource management, and low power operations (such as Idle mode and paging functions).

1.4.5 Management SAP (M-SAP)

The Management SAP may include, but is not limited to primitives related to the following:

- System configuration
- Monitoring statistics
- Notifications/Triggers
- Multi-mode interface management

The NCMS interacts with the MIB through the M-SAP in a method not defined in this document.

1.4.6 Control SAP (C-SAP)

The Control SAP may include, but is not limited to primitives related to the following:

- Handovers (e.g., notification of HO request from MS)
- Idle mode mobility management (e.g., Mobile entering idle mode)
- Subscriber and session management (e.g., Mobile requesting session setup)
- Radio resource management
- AAA server signaling (e.g., EAP payloads)
- Media Independent Handover Function Services
- Location detection reporting capability

2. References

Insert the following references in alphanumerical order:

IEEE Std 802.16e-2005, IEEE Standard for Local and Metropolitan area networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems—Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, February 2006.^{3, 4}

IEEE Std 802.16f-2005, IEEE Standard for Local and Metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Amendment 1: Management Information Base, December 2005.

IEEE P802.21/D7.1, Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.⁵

IETF RFC 2865, “Remote Authentication Dial In User Service (RADIUS),” C. Rigney, et al., June 2000. (<http://www.ietf.org/rfc/rfc2865.txt>).

IETF RFC 3825, “DHCP for Coordinate-based Location Configuration Information,” July 2004. (<http://www.ietf.org/rfc/rfc3825.txt>).

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 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.

⁵Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining drafts, contact the IEEE.

3. Definitions

Insert the following new definitions in alphabetical order and renumber appropriately:

3.89 Authenticator: Authenticator functionality is part of the AAA Services, which is included in the NCMS. An authenticator is an entity at one end of a point-to-point link that facilitates authentication of a supplicant (e.g., the mobile station) attached to the other end of that link. It can enforce authentication before allowing access to services that are accessible to the supplicant. Authenticator incorporates an AAA client functionality that enables it to communicate with AAA backend infrastructure (AAA based Authentication Server). The AAA server provides the Authenticator with authentication and authorization services over AAA protocols. The authenticator function contains a Key Distributor and may also include a Key Receiver function.

3.90 location-based services (LBSs): Services that are based on location data of the MS and/or BS in a network of IEEE 802.16 devices. Examples can be found in location-sensitized applications, emergency call origination tracking, equipment tracking etc.

3.91 paging controller: Paging controller is a unit that belongs to the idle mode services in the NCMS. The paging controller retains the mobile station (MS) state and operational parameters and/or administers paging activity for the MS while in idle mode.

3.92 U interface: The management and control interface that exists between the subscriber station (SS) and the base station (BS) over the air interface.

4. Abbreviations and acronyms

Insert the following abbreviations and acronyms in alphabetical order:

ACM	accounting management
ATC	automatic timing correction
D-TDOA	downlink time difference of arrival
FRF	frequency reuse factor
GPCS	generic packet convergence sublayer
IMM	idle mode management
LBS	location-based service
LCI	Location Configuration Information
MIB	management information base
MIH	media independent handover
MIHF	MIH function
NAI	network access identifier
NAS	network access server
NCMS	network control and management system
NCMS(BS)	network control and management system at the BS side (network side)

NCMS(SS/MS) network control and management system at the SS/MS side

NEM	network entry management
NRM	network reference model
NSP	network service provider
PER	packet error rate
RRA	radio resource agent
RRC	radio resource controller
RRM	radio resource management
SAP	service access point
SFM	service flow management
SIQ	service information query
SM	security management
SSM	subscriber station management
TDOA	time difference of arrival
U-TDOA	uplink time difference of arrival

5. Service-specific CS

Change the third paragraph of the subclause as follows:

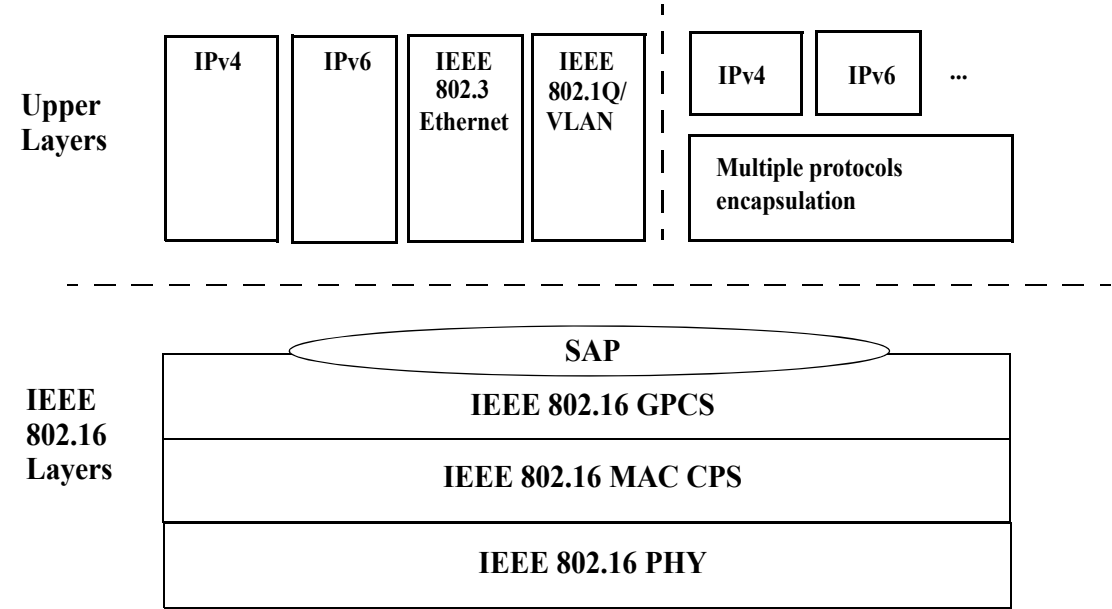
Currently, ~~two~~^{three} CS specifications are provided: the asynchronous transfer mode (ATM) CS, ~~and the packet CS, and the generic packet CS.~~ Other CSs may be specified in the future.

Insert new subclause 5.3 as follows:

5.3 Generic packet convergence sublayer (GPCS)

The generic packet CS (GPCS) is an upper-layer protocol-independent packet convergence sublayer that supports multiple protocols over IEEE 802.16 air interface. It is defined as follows:

- GPCS provides a generic packet convergence layer. This layer uses the MAC SAP and exposes a SAP to GPCS applications.
- GPCS does not re-define or replace other convergence sublayers. Instead, it provides a SAP that is not protocol specific.
- With GPCS, packet parsing happens “above” GPCS. The results of packet parsing are classification parameters given to the GPCS SAP for “parameterized classification,” but upper layer packet parsing is left to the GPCS application.
- With GPCS, the upper-layer protocol that is immediately above the IEEE 802.16 GPCS is identified by a TLV parameter, GPCS protocol type, as defined in 11.13.19.5.1. The GPCS protocol type shall be included in C-SFM primitives and DSx messages during connection establishment.
- GPCS defines a set of SAP parameters as the result of upper layer packet parsing. These are passed from upper layer to the GPCS in addition to the data packet. The SAP parameters include SFID, MS MAC Address, data, and length. Each is defined in 5.3.3.
- GPCS allows multiplexing of multiple layer protocol types (e.g., IPv4, IPv6, Ethernet) over the same IEEE 802.16 connection. An appropriate upper protocol layer that supports protocol multiplexing is used to do this, and it is signaled in the GPCS_PROTOCOL_TYPE TLV in DSx messages to indicate that multiple protocols are supported for a connection/service flow. It is outside the scope of the GPCS to specify how the upper layer multiplexes and demultiplexes multiple protocol data packets over an IEEE 802.16 connection/service flow.
- For interoperability, upper-layer protocol type may need an interface specification. Such a standard specification is out of scope of this document.
- With GPCS, the IEEE 802.1D bridging will be supported transparently by IEEE 802.16 air interface, because the GPCS requires the upper layer to provide the MS MAC Address and SFID with every packet, where the MS MAC Address and SFID can represent a port and a port is either a unicast port or broadcast port.
- PHS as defined in 5.2.3 defines rules how packets with suppressed fields are reconstructed based on the PHSI and the associated PHS rule. This reconstruction method can also be applied on packets transferred over the GPCS. Details are given in 5.3.6.



Protocol structure with the generic packet convergence sublayer (GPCS)

Figure 17c—GPCS layering model

5.3.1 Mapping of the GPCS service to upper layers

In the case where a GPCS instance services only a single GPCS peer on an SS, the MS MAC Address field of the GPCS_DATA primitive shall be constant and set to the MAC address of the SS. The SFID field of the GPCS_DATA primitive shall be set to the SFID of the service flow being carried.

In the case where a GPCS instance services more than one SS, the MS MAC Address field of the GPCS_DATA primitive will indicate the SS that is the source or destination for the PDU. The SFID field of the GPCS_DATA primitive shall be set to the SFID of the service flow being carried.

5.3.2 Operation of GPCS with SSs that do not support the GPCS

A BS that supports GPCS may interoperate with an SS that does not support GPCS. It can be observed that a GPCS service with GPCS_PROTOCOL_TYPE 0x0000 (Ethernet MAC Service) carries packets formatted identically to the packets used in the IEEE 802.3 specific part of the Packet CS. Also, a GPCS service with GPCS_PROTOCOL_TYPE 0x0003 (Raw IP) carries packets formatted identically to the packets used in the IP specific part of the Packet CS.

A BS may operate using GPCS at the base station, locally using GPCS_PROTOCOL_TYPE=0x0000, while signaling to the SS during connection setup that the IEEE 802.3 specific part of the packet CS is being used.

A BS may operate using GPCS at the base station, locally using GPCS_PROTOCOL_TYPE=0x0003, while signaling to the SS during connection setup that the IP specific part of the packet CS is being used.

5.3.3 GPCS SAP parameters

The GPCS uses the GPCS SAP, an instance of the logical CS SAP. The GPCS SAP parameters enable the upper-layer protocols to generically pass information to the GPCS so that the GPCS does not need to interpret upper-layer protocol headers in order to map the upper layer data packets into proper IEEE 802.16 MAC connections. Since the SAP parameters are explicit, the parsing portion of the classification process is the responsibility of the upper layer. The parameters are relevant for SAP data path primitives, GPCS_DATA.request, and GPCS_DATA.indication as described in 5.3.4 and 5.3.5, respectively.

Service flow ID (SFID):

Unique identifier to identify a unidirectional service flow for an MS. A GPCS implementation shall map the combination of SFID and MS MAC Address directly to a MAC connection ID. During connection/service flow establishment, the IEEE 802.16 control plane function shall provide GPCS the mapping information.

MS MAC Address:

48-bit unique identifier used by MS.

DATA:

The payload delivered by the GPCS upper layer to the GPCS, or by the GPCS to the upper layer.

LENGTH:

Number of bytes in DATA.

5.3.4 GPCS_DATA.request

5.3.4.1 Function

This primitive defines the transfer of data from the upper layer to the GPCS.

5.3.4.2 Semantics of the service primitive

The parameters of the primitive are as follows:

GPCS_DATA.request

```
(  
    SFID,  
    MS MAC Address,  
    length,  
    data  
)
```

The parameters, SFID, MS MAC Address, length, and data are described in 5.3.3.

5.3.4.3 When generated

This primitive is generated by an upper-layer protocol when a GPCS SDU is to be transferred to a peer entity or entities.

5.3.4.4 Effect of receipt

The receipt of this primitive causes GPCS to map the SFID and MS MAC Address to a unidirectional service flow and thereby a connection. GPCS invokes MAC functions, for example the MAC SAP (an example MAC SAP definition is provided in Annex C) to effectuate transfer of the SDU to the MAC layer.

5.3.5 GPCS_DATA.indication

5.3.5.1 Function

This primitive defines the transfer of data from the GPCS to an upper-layer protocol.

5.3.5.2 Semantics of the service primitive

The parameters of the primitive are as follows:

```
GPCS_DATA.indication
(
    SFID,
    MS MAC Address,
    length,
    data
)
```

The parameters, SFID, MS MAC Address, length, and data are described in 5.3.3.

Note that SFID and MS MAC Address are not transferred over the IEEE 802.16 air interface. The GPCS shall map the CID to SFID and MS MAC Address, and then pass them to the upper layer of the GPCS through GPCS_DATA.indication, where the CID is provided in MAC SAP.

5.3.5.3 When generated

This primitive is generated by the GPCS whenever a GPCS SDU is to be delivered to an upper-layer protocol resulting from receipt of a MAC PDU.

5.3.5.4 Effect of receipt

The effect of receipt of this primitive by the upper-layer protocol entity is dependent on the validity and content of the SDU.

5.3.6 PHS operation

PHS header suppression and reconstruction according to 5.2.3 may be deployed on particular GPCS service flows by installing PHS rules at the receiving side of the service flow using the procedures described in 5.2.3.2. As classification is outside of the scope of GPCS, the Classifier Rule Index in the DSC-REQ message should be set to '0' when configuring the PHS rules.

6. MAC common part sublayer

6.3 Data/Control plane

6.3.2 MAC PDU formats

6.3.2.3 MAC management messages

After deleting the last row, add the following entries to Table 14:

Table 14—MAC management messages

Type	Message name	Message description	Connection
67	MOB_MIH-MSG	MIH Payload Transfer message	Primary Management
68	SII-ADV	Service Identity Broadcast	Broadcast
69	LBS-ADV	Location information broadcast for LBS	Broadcast
70-255		<i>Reserved</i>	

6.3.2.3.1 Downlink Channel Descriptor (DCD) message

Change “Configuration Change Count” text as follows:

Configuration Change Count

Incremented by one (modulo 256) by the BS whenever any of the values of this channel descriptor change, except for the Frame Number for the OFDM PHY and the available DL radio resources. If the value of this count in a subsequent DCD remains the same, the SS can quickly decide that the remaining fields have not changed and may be able to disregard the remainder of the message. An SS performing initial network entry should decode the available DL radio resources even if the DCD Configuration Change Count remains unchanged.

6.3.2.3.2 Downlink map (DL-MAP) message

Change “Base Station ID” text as follows:

Base Station ID

The Base Station ID is a 48-bit long field identifying the BS. The least significant 24 bits of the Base Station ID shall be programmable. The most significant 24 bits shall be used as the ~~Operator ID~~. This is a network management hook that can be ~~combined with the Downlink Channel ID of the~~ sent with the DCD message for handling edge-of-sector and edge-of-cell situations. The 24-bit Operator ID shall be assigned as an IEEE 802.16 Operator ID by the IEEE Registration Authority.⁶ The IEEE Registration Authority shall be the sole authorized number space administrator for this function.

⁶The IEEE Registration Authority is a committee of the IEEE Standards Association Board of Governors. General information as well as details on the allocation of IEEE 802.16 Operator ID can be obtained at <http://standards.ieee.org/regauth>.

6.3.2.3.3 Uplink Channel Descriptor (UCD) message

Change “Configuration Change Count” text as follows:

Configuration Change Count

Incremented by one (modulo 256) by the BS whenever any of the values of this channel descriptor change, except for the available UL radio resources. If the value of this count in a subsequent UCD remains the same, the SS can quickly decide that the remaining fields have not changed and may be able to disregard the remainder of the message. An SS performing initial network entry should decode the available UL radio resources even if the UCD Configuration Change Count remains unchanged. This value is also referenced from the UL-MAP messages.

6.3.2.3.6 Ranging Response (RNG-RSP) message

Insert the following at the end of 6.3.2.3.6:

The following TLV parameters may be included in an unsolicited RNG-RSP message:

Rendezvous time

This is the offset, measured in units of frame duration, when the BS is expected to provide a non-contention-based ranging opportunity for the MS. The offset is calculated from the frame where RNG-RSP message is transmitted. The BS is expected to provide the non-contention-based ranging opportunity at the frame specified by the rendezvous time parameter.

CDMA code

A unique code assigned to the MS, to be used for dedicated ranging. The code is from the initial ranging code set.

Transmission Opportunity Offset

A unique transmission opportunity assigned to the MS, to be used for dedicated ranging, in units of symbol duration.

6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

In Table 26, insert new entries and change the last row as follows:

Table 26—PKM message codes

Code	PKM message type	MAC Management message name
31	MIH Initial Request	PKM-REQ
32	MIH Acknowledge	PKM-RSP
33	MIH Comeback Response	PKM-RSP
~~2934~~ -255	<i>Reserved</i>	—

Insert new subclauses 6.3.2.3.9.29 to 6.3.2.3.9.32 as follows:

6.3.2.3.9.29 MIH Initial Request message

The MS sends this message to the BS to deliver an MIH query encapsulated in an MIHF frame.

Code: 31

Attributes are shown in Table 37s.

Table 37s—MIH Initial Request attributes

Attribute	Contents
MIHF frame type	Indicates type of MIHF frame (11.1.9.1).
Delivery Method and Status Code	Indicates the delivery method of query response (11.1.9.4).
MIHF frame	The encapsulated MIHF query (11.1.9.1).

6.3.2.3.9.30 MIH Acknowledge

This message is sent by the BS to the MS to acknowledge a received MIH query encapsulated in an MIHF frame. The response to the query is sent in a later MIH Comeback Response message, and the MS uses a Query ID, received in this MIH Acknowledge message and associated with the MS Initial Request by virtue of the stateful nature of the MIH Acknowledge, to correlate the MIH Initial Request message query with the later response.

Code: 32

Attributes are shown in Table 37t.

Table 37t—MIH Acknowledge attributes

Attribute	Contents
Cycle	Indicates the delivery method of query response (11.1.9.3).
Query ID	Used to map query and query response (11.1.9.5).
Delivery Method and Status Code	Indicates the delivery method and status code (11.1.9.4).

6.3.2.3.9.31 MIH Comeback Response

The BS sends this message to the MS to deliver a query response encapsulated in an MIHF frame.

Code: 33

Attributes are shown in Table 37u.

Table 37u—MIH Comeback Response attributes

Attribute	Contents
MIHF frame type	Indicates the type of the included MIHF frame. Only included when an MIHF frame is present.
Query ID	Used to map query and query response (11.1.9.5).
Delivery Method and Status Code	Indicates the delivery method and status code (11.1.9.4).
MIHF frame	The encapsulated MIH response (11.1.9.1).

6.3.2.3.23 SS Basic Capability Request (SBC-REQ) message

Change the text in 6.3.2.3.23 as follows:

The following parameters may be included:

Capabilities for construction and transmission of MAC PDUs (see 11.8.2)

PKM flow control (see 11.7.8.6)

Authorization policy support (see 11.8.4.2)

Maximum number of supported security association (see 11.7.8.8)

Service Information Query (see 11.8.9)

Visited NSP ID (see 11.8.11)

Auto Type for Single EAP (see 11.8.12)

MIH Capability Supported (see 11.8.10)

6.3.2.3.24 SS Basic Capability Response (SBC-RSP) message

Insert the following paragraph at the end of subclause 6.3.2.3.24:

The following parameters may be included when solicited in the SBC-REQ message, unless there are no NSP IDs to be included in the NSP List TLV. If the BS is configured with a list of NSPs and the SBC-REQ message has included an SIQ TLV (11.8.9), then the NSP List TLV and, if requested, the Verbose NSP Name List TLV shall be included unless the message includes an SII-ADV Message Pointer TLV providing a pointer to an SII-ADV message in which these TLVs are sent.

NSP List (see 11.1.8.1)

Verbose NSP Name List (see 11.1.8.2)

Verbose NSP Name List shall only be included in the message if NSP List TLV is also included in the message.

Visited NSP Realm (see 11.8.13)

SII-ADV Message Pointer (see 11.8.14)

MIH Capability Supported (see 11.8.10)

6.3.2.3.47 Neighbor Advertisement (MOB_NBR-ADV) message

Change Table 109f as follows (beginning at row 4):

Table 109f—MOB_NBR-ADV message format

Syntax	Size	Notes
If (Skip-optional-fields-[0]=0) {	—	—
Operator ID	24 bits	~~Unique ID assigned to the operator~~
}	—	—

Change the second paragraph after Table 109f, as follows:

Operator ID

The network ID shared by an association of BS. The ‘Operator ID’ field is presented only if #0 of Skip-optional-fields bitmap is set to 0. The most significant 24 bits of the BS ID shall be used as the Operator ID. The 24-bit Operator ID shall be assigned as an IEEE 802.16 Operator ID by the IEEE Registration Authority.⁷ The IEEE Registration Authority shall be the sole authorized number space administrator for this function.

Insert new subclause 6.3.2.3.62 as follows:

6.3.2.3.62 MIH Payload Transfer message (MOB_MIH-MSG)

The MOB_MIH-MSG message shall be transmitted on the Primary Management connection. See Table 109ya.

Table 109ya—MOB_MIH-MSG message format

Syntax	Size	Notes
MOB_MIH-MSG_Message_Format() {	—	—
Management Message Type = 67	8 bits	—
TLV Encoded Information	Variable	TLV specific
}	—	—

The MOB_MIH-MSG shall include the following parameters as encoded as TLV tuples:

- MIHF Frame (see 11.1.9)
- HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

⁷The IEEE Registration Authority is a committee of the IEEE Standards Association Board of Governors. General information as well as details on the allocation of IEEE 802.16 Operator ID can be obtained at <http://standards.ieee.org/regauth>.

Insert new subclause 6.3.2.3.63 as follows:

6.3.2.3.63 Service Identity Information (SII-ADV) message

A BS may use the SII-ADV message to broadcast a list of Network Service Provider (NSP) identifiers. The message may be broadcast periodically without solicitation or may be solicited by an SS during network entry by including the SIQ TLV in the SBC-REQ message (see 6.3.2.3.23). This message is sent from the BS to all SSs on the broadcast CID. Assignment method, administration, and usage of NSP IDs are outside the scope of this standard. The list of NSP IDs to be included in this message and the message transmission frequency are programmable. The BS may use the SII-ADV message to deliver the IEEE P802.21 MIHF frame that carries the query response. SII-ADV is broadcast at the identified cycle that was notified to the MS during initial query. (See Table 109yb.)

Table 109yb—Service Identity Information (SII-ADV) message format

Syntax	Size	Notes
SII-ADV () {	—	—
Management message type = 68	8 bits	
TLV Encoded Information	Variable	TLV specific
}	—	—

The following parameters may be included in the SII-ADV message; at least one TLV shall be included in an SII-ADV message:

NSP List TLV (see 11.1.8.1)

The NSP LIST TLV is a TLV that contains one or more Network Service Provider 24-bit identifiers.

Verbose NSP Name List (see 11.1.8.2)

List of the verbose names of the NSPs. Verbose NSP Name List shall only be included in the message if NSP List TLV is also included in the message.

Query ID (11.1.9.4)

The Query ID TLV is used to correlate the response encapsulated in the MIHF frame carried in the MIHF frame TLV with a query previously sent by an MS within the broadcast area of the BS. It may be ignored by all other MSs.

MIHF frame type (11.1.9.2)

The MIHF frame type TLV indicates the service type of the MIHF frame TLV.

MIHF frame (11.1.9.1)

The encapsulated MIH response.

Insert the new subclause 6.3.2.3.64 as follows:

6.3.2.3.64 Location-based services (LBS-ADV) message

A BS may use the LBS-ADV message to broadcast the LBS information. The message may be broadcast periodically without solicitation. This message is sent from the BS to all MSs on a broadcast CID. (See Table 109yc.)

Table 109yc—Location-based services (LBS-ADV) message format

Syntax	Size	Notes
LBS-ADV_Message_Format() {	LBS-ADV	—
Management message type = 69	—	—
Number_of_BS	8 bits	Total number of serving BS and neighbor BSs.
For (j = 0 ; j < Number_of_BS ; j++) {	—	—
Length	8 bits	Length of message information within the iteration of Number_of_BS in bytes.
BSID	24 bits	The least significant 24 bits of the Base Station ID parameter in the DL-MAP message of the Serving BS or Neighbor BS.
TLV encoded information	variable	TLV specific.
}	—	—
}	—	—

The LBS-ADV shall include the following TLV:

Device coordinates (see 11.20)
The BS's coordinates.

In 6.3.9.2, change the first paragraph as follows:

6.3.9.2 Obtain downlink parameters

The MAC shall search for the DL-MAP MAC management messages. The SS achieves MAC synchronization once it has received at least one DL-MAP message and is able to decode the DL-Burst Profiles contained therein. An SS MAC remains in synchronization as long as it continues to successfully receive the DL-MAP and DCD messages for its Channel. An MS may use information received in the DCD or MOB_NBR-ADV messages, such as the available DL radio resources and cell type (see 11.4.1), to determine whether the channel is suitable for its intended use and whether it should continue scanning for other channels. If the Lost DL-MAP Interval (Table 342) has elapsed without a valid DL-MAP message or the timing adjustment interval (Table 342) has elapsed without a valid DCD message, an SS shall try to reestablish synchronization. The process of acquiring synchronization is illustrated in Figure 56. The process of maintaining synchronization is illustrated in Figure 57.

In 6.3.9.3, change the text as follows:

6.3.9.3 Obtain uplink parameters

After synchronization, the SS shall wait for a UCD message from the BS in order to retrieve a set of transmission parameters for a possible uplink channel. These messages are transmitted periodically from the BS for all available uplink channels and are addressed to the MAC broadcast address.

If no uplink channel can be found after a suitable timeout period, then the SS shall continue scanning to find another downlink channel. An MS may use information received in the UCD or MOB_NBR-ADV messages, such as the available UL radio resources or cell type (see 11.4.1), to determine whether the channel is suitable for its intended use and whether it should continue scanning for other channels. The process of obtaining uplink parameters is illustrated in Figure 58.

The SS shall determine from the channel description parameters whether it may use the uplink channel. If the channel is not suitable, then the SS shall continue scanning to find another downlink channel until all channels are exhausted. If the channel is suitable, the SS shall extract the parameters for this uplink from the UCD. Then, the SS shall wait for a bandwidth allocation map for the selected channel. It may begin transmitting uplink in accordance with the MAC operation and the bandwidth allocation mechanism.

If, after scanning all channels, the SS does not find a suitable channel, the SS may choose the most appropriate channel based on conditions that include RSSI, CINR, cell type, and the available radio resources of all channels to perform initial ranging according to 6.3.9.5.

The SS shall perform initial ranging at least once, per Figure 60 and Figure 61. If initial ranging is not successful, the procedure is restarted from scanning to find another downlink channel.

The SS MAC is considered to have valid uplink parameters as long as it continues to successfully receive the UL-MAP and UCD messages. If at least one of these messages is not received within the time intervals specified in Table 342, the SS shall not use the uplink. This is illustrated in Figure 59.

In 6.3.9.5.1, change the text below Table 115 as follows:

6.3.9.5.1 Contention-based initial ranging and automatic adjustments

NOTES

1—The BS shall allow the SS sufficient time to have processed the previous RNG-RSP (i.e., to modify the transmitter parameters) before sending the SS a specific ranging opportunity. This is defined as SS Ranging Response Processing Time in Table 342.

2—For multichannel support, the SS shall attempt initial ranging on every suitable uplink channel before moving to the next available downlink channel. Suitability of a channel is determined by conditions that include RSSI, CINR, cell type, available DL radio resources, and available UL radio resources.

During initial Network Entry, a BS may decide to redirect the ranging SS to another channel by sending the RNG-RSP with an Offset Frequency Adjustment pointing to the other channel. If the Offset Frequency Adjustment value is less than half of the channel bandwidth, this is fine-frequency adjustment within the ranged channel; otherwise, the value is a reassignment to a different channel.

On receiving a RNG-RSP instruction to move to a new downlink frequency and/or uplink channel ID, the SS shall consider any previously assigned Basic, Primary Management, and Secondary Management CIDs to be deassigned, and shall obtain new Basic, Primary Management, and Secondary Management CIDs via initial ranging and registration.

Change 6.3.9.8 as follows:

6.3.9.8 SS authorization and key exchange

If PKM is enabled (see 11.7.8.7), the BS and SS shall perform authorization and key exchange as described in 7.2.

If MIH query capability during network entry is enabled (refer to 11.4.1 and 11.8.10), the BS and MS may perform MIH query using PKM messages before authorization and key exchange.

6.3.10.3 OFDMA-based ranging

Change 6.3.10.3.1 as follows:

6.3.10.3.1 Contention-based initial ranging and automatic adjustments

- The SS, after acquiring downlink synchronization and uplink transmission parameters, shall choose randomly a Ranging Slot (with the use of a binary truncated exponent algorithm to avoid possible re-collisions) at the time to perform the ranging, then it chooses randomly a Ranging Code (from the Initial Ranging domain) and sends it to the BS (as a CDMA code).
- The BS cannot tell which SS sent the CDMA ranging request; therefore, upon successfully receiving a CDMA Ranging Code, the BS broadcasts a Ranging Response message that advertises the received Ranging Code as well as the ranging slot (OFDMA symbol number, subchannel, etc.) where the CDMA Ranging code has been identified. This information is used by the SS that sent the CDMA ranging code to identify the Ranging Response message that corresponds to its ranging request. The Ranging Response message contains all the needed adjustment (e.g., time, power, and possibly frequency corrections) and a status notification.
- Upon receiving a Ranging Response message with continue status, the SS shall continue the ranging process as done on the first entry with ranging codes randomly chosen from the Initial Ranging domain sent on the Periodic Ranging region.
- When the BS receives an initial-ranging CDMA code that results in sending an RNG-RSP message with success status, the BS shall provide BW allocation for the SS using the CDMA_Allocation_IE to send an RNG-REQ message.
- Initial ranging process is over after receiving RNG-RSP message, which includes a valid basic CID (following a RNG-REQ transmission on a CDMA_Allocation_IE). If this RNG-RSP message includes 'continue' indication, the ranging process should be continued using the periodic ranging mechanisms.
- If the RNG-RSP includes an Offset Frequency Adjustment pointing to another channel and it is larger than the value required for a channel bandwidth offset, the SS should synchronize with the new channel indicated in the RNG-RSP.
- The timeout required for SS to wait for RNG-RSP, following or not following CDMA Allocation IE, is defined by T3.
- Using the OFDMA ranging mechanism, the periodic ranging timer is controlled by the SS, not the BS.

Insert new subclause 6.3.10.3.4 as follows:

6.3.10.3.4 Dedicated ranging and automatic adjustments

A dedicated ranging is an optional initial ranging that can be used to expedite the ranging process when the ranging is performed as an initial step of a certain procedure such as location determination, coordinated association during scanning, location update in idle mode, etc. For a dedicated ranging, BS will provide

dedicated ranging information and allocate the dedicated ranging region at a pre-defined *rendezvous time*, in terms of relative frame number. The BS will also assign the following:

- A unique code number (from within the initial ranging code set)
- A transmission opportunity within the allocated region (in terms of offset from the start of the region)

The BS may assign the same code or transmission opportunity to more than one MS, but not both. In case all allocated transmission opportunities in the current region are different, there is no potential for collision of transmissions from different MSs. In case the BS allocates the same transmission opportunity to several MSs, there is some probability of collision and then the BS may fail to identify transmitted codes.

The BS will provide the dedicated ranging information via MAC management messages, which are different according to the procedures for which the dedicated ranging is used.

When the *dedicated ranging indicator* is set to 1, the ranging region will be allocated via UIUC=12 in the UL-MAP.

When the *dedicated ranging indicator* is set to 1, then the ranging region and ranging method defined could be used for the purpose of ranging using dedicated CDMA code and transmit opportunity assigned in the unsolicited RNG-RSP message (for location determination of MS) or in the MOB_SCN-RSP message (for coordinated association).

MSs registered to this BS are prohibited from use of the named ranging region.

Upon receiving one of aforementioned messages, which include the dedicated ranging information, the MS should interpret the provided rendezvous time, dedicated code, and transmission opportunity as follows:

- Rendezvous time specifies the frame in which the BS will transmit a UL-MAP containing the definition of the dedicated ranging region where the MS can use the assigned CDMA ranging code. Rendezvous time is provided in units of frames, beginning at the frame where the MAC management message that includes the dedicated ranging information is transmitted.
- The MS shall read the UL-MAP transmitted at the first frame immediately following the rendezvous time and extract the description of the dedicated ranging region (ranging region with dedicated ranging indicator bit set to 1). The MS shall determine the specific region it should use for transmission of the dedicated CDMA code by applying the offset defined by the *transmission opportunity offset* field in the management message, which was received from the BS, to the dedicated ranging region definition in the UL-MAP of the BS. In case the BS decides to provide a regular (non-dedicated) ranging region with dedicated ranging indicator set to 0, the MS may transmit the allocated CDMA code in the regular ranging region.
- If the MS could not obtain UL-MAP at the first frame immediately following the rendezvous time, it shall abort the dedicated ranging process. The MS may perform a contention-based ranging process as described in 6.3.10.3.1.

In subclause 6.3.22.2.2, change the text in the fourth paragraph as follows:

6.3.22.2.2 HO decision and initiation

Serving BS criteria for recommendation of target BS may include factors such as expected MS performance at potential target BS, BS and network loading conditions, and MS QoS requirements. Serving BS may obtain expected MS performance and BS and network loading conditions at a potential target BS through the exchange of backbone messages with that BS. Serving BS may negotiate location of common time interval

where dedicated initial ranging transmission opportunity for the MS will be provided by all potential target BSs. This information may be included into MOB_BSHO-RSP message.

Change 6.2.24.2 as follows:

6.3.24.2 Cell selection

At MS Idle Mode Initiation, an MS may engage in cell selection to obtain a new Preferred BS. A Preferred BS is a Neighbor BS that the MS evaluates and selects as the BS with the best air interface DL properties, which may include the RSSI, CINR, cell type, the available radio resources, etc. The Preferred BS may be the MS's previous Serving BS. In all other respects, cell selection is similar to 6.3.22.2.1.

Insert new subclause 6.3.25 as follows:

6.3.25 MIHF support

MIHF support is the support of IEEE P802.21 specific features and functions. The IEEE 802.16 entity may send or receive the MOB_MIH-MSG message to or from the peer IEEE 802.16 entity in order to convey MIHF frames carrying the IEEE P802.21 MIH protocol messages.

When MIH query capability during network entry is enabled (refer to 11.4.1 and 11.8.10), PKM messages may be used to exchange MIH frames for MIH queries.

The MS may submit an MIH query by sending a PKM-REQ message with code 31 (MIH Initial Request) containing an MIHF frame encapsulating the query. Upon receiving this message, the BS acknowledges the request by sending a PKM-RSP message with code 32 (MIH Acknowledge). This message does not contain the response to the MIH query, but contains a Cycle TLV (11.1.9.3), which indicates when the response is expected to be ready for delivery to the MS. This message also contains a Query ID that the MS may use to correlate the query with the response, and the delivery method (unicast or broadcast) that the BS will use.

When a unicast delivery method has been negotiated, then if the BS is ready to transmit the MIH response, the BS shall allocate bandwidth for the MS in the UL-MAP in the MAC frame indicated by the Cycle TLV. Upon receiving this UL allocation, the MS shall transmit at least a Bandwidth request PDU. If the MS has no data to transmit, the BR field of the Bandwidth request PDU shall be set to 0. The BS may use the receipt of the Bandwidth request PDU to assert the continued presence of the MS. If the MS does not send at least a Bandwidth Request PDU, the BS shall abort the network entry procedure for the MS; otherwise, it shall send a PKM-RSP message with code 33 (MIH Comeback Response) containing the encapsulated MIH response. The MIH Comeback Response message shall also contain the Query ID previously sent in the MIH Acknowledge message, which the MS may use to correlate the MIH response with the MIH query. When a broadcast delivery method has been negotiated, and if the BS is ready to transmit the MIH response, the BS shall transmit an SII-ADV message containing the MIH response in the MAC frame indicated by the Cycle TLV.

If the BS is not ready to transmit the MIH response at the time indicated by the Cycle TLV, the MS and BS shall wait for another cycle and repeat the procedures specified in the preceding paragraph. The maximum number of times the MS and BS shall perform those procedures is determined by the MIH max cycles system parameter (10.1, Table 342).

Insert new subclause 6.3.26 as follows:

6.3.26 Location-based services

This subclause provides mechanisms to coordinate the collection, generation, and reporting of information used to determine MS location [e.g., RSSI, CINR, Time Difference of Arrival (TDOA), Time of Arrival (TOA)]. Reporting of the BS location information is also described.

6.3.26.1 Time Difference of Arrival (TDOA)

TDOA is a location determination scheme that measures the difference of time arrival for packet transmission between a MS and multiple BSs. There are two types of TDOA—Downlink TDOA (D-TDOA) and Uplink TDOA (U-TDOA) based on whether the measurements are performed in the MS and the BS, respectively.

- *D-TDOA*: The MS may report D-TDOA data in the Relative Delay parameter in MOB_SCN-REP message that indicates the delay of DL signals from a neighbor BS relative to the serving BS. MOB_SCN-REP also reports RSSI and CINR of DL signals from the neighbor BS that can be used for MS location estimation. During SBC-REQ/RSP based capability negotiation, HO Trigger metric support (see 11.8.7) indicates which trigger metric the MS supports.
- *U-TDOA*: As opposed to D-TDOA that is reported each time MS scanning is completed, U-TDOA enables BS to initiate U-TDOA measurement when it is needed. Annex J describes two algorithms to show the U-TDOA measurement through the coordination of MS, serving BS, and one or more neighbor BS for wireless broadband networks: the General U-TDOA Method, for any FRF (Frequency Reuse Factor); and the Special U-TDOA Method, for FRF = 1.

8. PHY

8.4.4.5 Uplink transmission allocations

Change the fourth paragraph in this subclause as follows:

The BS shall not allocate more than three ranging allocation IEs (UIUC 12) per frame, one for initial ranging/handover ranging (Dedicated ranging indicator bit in UL-MAP IE is set to 0 and Ranging Method is set to 0b00 or 0b01), one for bandwidth request/periodic ranging (Dedicated ranging indicator bit in UL-MAP IE is set to 0 and Ranging Method is set to 0b10 or 0b11), and one for initial ranging for the paged MS, location measurement, and/or coordinated association (Dedicated ranging indicator bit in UL-MAP IE is set to 1).

8.4.5.4 UL-MAP IE format

In Table 287, change the “Dedicated ranging indicator” row as follows:

Table 287—OFDMA UL-MAP IE format

Syntax	Size	Notes
Dedicated ranging indicator	1 bit	0: the OFDMA region and Ranging Method defined are used for the purpose of normal ranging. 1: the OFDMA region and Ranging Method defined are used for the purpose of ranging using dedicated CDMA code and transmission opportunities assigned in the MOB_PAG-ADV message, <u>in the RNG-RSP message</u> , or in the MOB_SCN-RSP message.

9. Configuration

Change subclause 9.1.2 as follows:

9.1.2 Mobile IP v4 fields used by the MS

If Mobile IP v4 is used to obtain an address for the secondary management connection, the following fields shall be present in the Mobile IP registration request sent from the MIP client residing in the MS and shall be set as described below and encoded according to IETF RFC 3344.

- a) When the MS (or Mobile Node) attempts to obtain an IP address dynamically, the home address field shall be set to “0.0.0.0”.
- b) When the MS attempts to obtain an IP address in the visited network, the home agent address field shall be set to “0.0.0.0”. On the other hand, when the MS attempts to obtain an IP address in the home network, the home agent address field shall be set to “255.255.255.255”.
- c) The Network Access identifier (NAI) extension [IETF RFC 2789] shall be included for identifying the Mobile IP user.
- d) The Challenge extension shall be included [IETF RFC 3012], if the Challenge extension is included in the Agent Advertisement message.
- e) A 128-bit key may be shared between an MS and an ASA server during the initial Mobile IP registration, and the MS-ASA Authentication extension may be generated based on the shared key [IETF RFC 3012].

The following fields are expected in the Mobile IP registration response returned to the MIP Client residing in the MS. The MS shall configure itself based on the Mobile IP registration response

- The home address to be used by the MS.
- The MS’s NAI extension to identify a Mobile IP user [IETF RFC 2789].
- The challenge extension if the foreign agent supports more strong security.
- The MS and home agent authentication extension for authenticating the home agent.
- The key reply extensions for security between the MS and the home agent, and between the MS and foreign agent, if the MS requests keys between the MS and the home agent, and between the MS and the foreign agent.

10. Parameters and constants

10.1 Global values

Insert the following new entries to Table 342:

Table 342—Parameters and constants

System	Name	Time reference	Minimum value	Default value	Maximum value
BS	LBS-ADV interval	Nominal time between transmission of LBS-ADV messages.	2 s	10 s	1800 s
BS	SII-ADV interval	Nominal time between transmission of SII-ADV messages.		10 s	30 s
BS	T48	The time allowed between the SBC response and PKM-REQ.			
BS	T49	The time allowed between the PKM-REQ (Code=31) and PKM-REQ for security procedure initiation.			
BS	DL_radio_resources_window_size	The number of frames over which the available DL radio resources are calculated.		200	
BS	UL_radio_resources_window_size	The number of frames over which the available UL radio resources are calculated.		200	
MS, BS	MIH max cycles	The maximum number of cycles that an MS waits for an MIH response during initial entry. Refer to 6.3.25.	3	3	

11. TLV encodings

11.1 Common encodings

Insert the following entries into Table 346

Table 346—Type values for common TLV encodings

Type	Name
140	NSP List
139	NSP Change Count

11.1.2.1 HMAC Tuple

Change Table 347 as follows:

Table 347—HMAC Tuple definition

Type	Length	Value	Scope
149	21	See Table 348	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-REQ, DREG-CMD, TFTP-CPLT, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND, DREG-REQ, <u>MOB_MIH-MSG</u>

Change Table 348a as follows:

Table 348a—CMAC Tuple definition

Type	Length	Value	Scope
150	13 or 19	See Table 348b	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT, PKM-REQ, PKM-RSP, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND, DREG-REQ, <u>MOB_MIH-MSG</u>

11.1.3 MAC version encoding

Change the TLV definition for MAC version encoding as follows:

Type	Length	Value	Scope
148	1	Version number of IEEE 802.16 supported on this channel. 1: Indicates conformance with IEEE Std 802.16-2001 2: Indicates conformance with IEEE Std 802.16c-2002 and its predecessors 3: Indicates conformance with IEEE Std 802.16a-2003 and its predecessors 4: Indicates conformance with IEEE Std 802.16-2004 5: Indicates conformance with IEEE Std 802.16-2004 and IEEE Std 802.16e-2005 <u>6: Indicates conformance with IEEE Std 802.16-2004, IEEE Std 802.16e-2005 and IEEE Std 802.16f-2005</u> <u>7: Indicates conformance with IEEE Std 802.16-2004, IEEE Std 802.16e-2005, IEEE Std 802.16f-2005 and IEEE Std 802.16g-2007</u> ~~68–255~~ : Reserved	PMP: DCD, RNG-REQ MESH: REG-REQ, REG-RSP

Insert new subclause 11.1.8 as follows:

11.1.8 NSP List encodings

11.1.8.1 NSP List

The NSP LIST TLV contains one or more 24-bit Network Service Provider identifiers.

Name	Type	Length	Value	Scope
NSP List TLV	140	3n	Including n, 24 bit Network Service Provider IDs, n is greater than or equal to 1.	SBC-RSP, SII-ADV

11.1.8.2 Verbose NSP Name List

The Verbose NSP Name List is a compound list of the verbose names of the Network Service Providers as indicated by the NSP List.

Name	Type	Length	Value	Scope
Verbose NSP Name List	139	variable	List of verbose names of the Network Service Provider(s). The value of Verbose NSP Name List is a compound list of verbose NSP name lengths and verbose NSP names. The order of the Verbose NSP Name Lengths and Verbose NSP Names presented in the Verbose NSP Name List TLV shall be in the same order as the NSP IDs presented in the NSP List TLV.	SBC-RSP, SII-ADV