

# 802.16™

IEEE Standard for  
Local and metropolitan area networks

## Part 16: Air Interface for Fixed Broadband Wireless Access Systems

IEEE Computer Society  
and the  
IEEE Microwave Theory and Techniques Society

Sponsored by the  
LAN/MAN Standards Committee



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

8 April 2002

Print: SH94964  
PDF: SS94964

IEEE Standard for  
Local and metropolitan area networks

# Part 16: Air Interface for Fixed Broadband Wireless Access Systems

Sponsor

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

and the

**IEEE Microwave Theory and Techniques Society**

Approved 6 December 2001

**IEEE-SA Standards Board**



**Abstract:** This standard specifies the air interface of fixed (stationary) point-to-multipoint broadband wireless access systems providing multiple services. The medium access control layer is capable of supporting multiple physical layer specifications optimized for the frequency bands of application. The standard includes a particular physical layer specification applicable to systems operating between 10 and 66 GHz.

**Keywords:** fixed broadband wireless access network, metropolitan area network, microwave, millimeter wave, WirelessMAN™ standards

Grateful acknowledgment is made to Cable Television Laboratories for the permission to use the following source material:

Radio Frequency Interface Specification (version 1.1), part of Data-Over-Cable Service Interface Specifications, © Copyright 1999, Cable Television Laboratories.

Baseline Privacy Plus Interface Specification, © Copyright 1999, Cable Television Laboratories.

---

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

Copyright © 2002 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 8 April 2002. Printed in the United States of America.

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

*Print:* ISBN 0-7381-3070-2 SH94964  
*PDF:* ISBN 0-7381-3071-0 SS94964

*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

Note: 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 shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

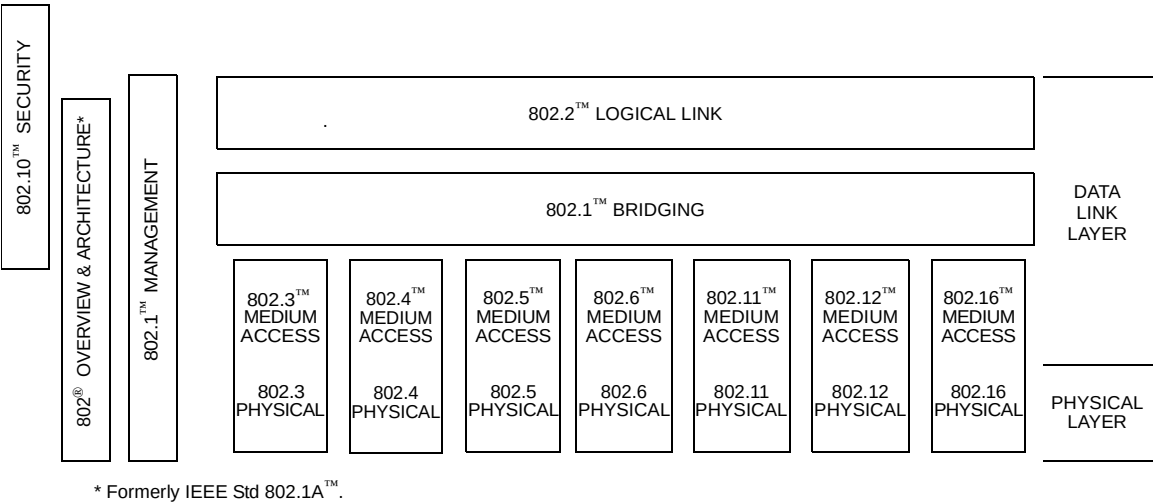
Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright 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 802.16-2001, IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems.)

This standard specifies the air interface of a fixed (stationary) point-to-multipoint broadband wireless access system providing multiple services in a wireless metropolitan area network (MAN). The WirelessMAN™ medium access control layer defined here is capable of supporting multiple physical layer specifications optimized for the frequency bands of application. The standard includes a particular physical layer specification applicable to systems operating between 10 and 66 GHz. This 10-66 GHz air interface, based on single-carrier modulation, is known as the WirelessMAN-SC™ air interface. An amendment to this standard, to support 2-11 GHz using an enhanced version of the same basic medium access control layer along with new physical layer specifications, is in development in IEEE-SA Project 802.16a.

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standards numbers.<sup>1</sup>)



This family of standards deals with the Physical and Data Link Layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection Basic Reference Model (ISO/IEC 7498-1:1994). The access standards define several types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the technologies noted above are as follows:

- IEEE Std 802:<sup>2</sup> *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the IEEE Std 802.1 scope of work.

<sup>1</sup>The IEEE standards referred to in the above figure and list are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

<sup>2</sup>The IEEE 802 Architecture and Overview Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

- IEEE Std 802.1B™ and 802.1K™ [ISO/IEC 15802-2]: *LAN/MAN Management.* Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- IEEE Std 802.1D™ *Media Access Control (MAC) Bridges.* Specifies an architecture and protocol for the [ISO/IEC 15802-3]: interconnection of IEEE 802 LANs below the MAC service boundary.
- IEEE Std 802.1E™ [ISO/IEC 15802-4]: *System Load Protocol.* Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- IEEE Std 802.1F™ *Common Definitions and Procedures for IEEE 802 Management Information.*
- IEEE Std 802.1G™ [ISO/IEC 15802-5]: *Remote Media Access Control (MAC) Bridging.* Specifies extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- IEEE Std 802.1H™ [ISO/IEC TR 11802-5] *Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks.*
- IEEE Std 802.1Q™ *Virtual Bridged Local Area Networks.* Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.
- IEEE Std 802.2 [ISO/IEC 8802-2]: *Logical Link Control.*
- IEEE Std 802.3 [ISO/IEC 8802-3]: *CSMA/CD Access Method and Physical Layer Specifications.*
- IEEE Std 802.4 [ISO/IEC 8802-4]: *Token Bus Access Method and Physical Layer Specifications.*
- IEEE Std 802.5 [ISO/IEC 8802-5]: *Token Ring Access Method and Physical Layer Specifications.*
- IEEE Std 802.6 [ISO/IEC 8802-6]: *Distributed Queue Dual Bus Access Method and Physical Layer Specifications.*
- IEEE Std 802.10: *Interoperable LAN/MAN Security.* Currently approved: Secure Data Exchange (SDE).
- IEEE Std 802.11: [ISO/IEC 8802-11] *Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications.*
- IEEE Std 802.12: [ISO/IEC 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specification.*
- IEEE Std 802.15: *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks.*

- IEEE Std 802.16: *Air Interface for Fixed Broadband Wireless Access Systems.*
- IEEE Std 802.17™: *Resilient Packet Ring Access Method and Physical Layer Specifications.*

In addition to the family of standards, the following is a recommended practice for a common physical layer technology:

- IEEE Std 802.7™: *IEEE Recommended Practice for Broadband Local Area Networks.*

The reader of this standard is urged to become familiar with the complete family of standards.

## Conformance test methodology

An additional standards series, identified by the number 1802™, has been established to identify the conformance test methodology documents for the IEEE 802 family of standards. For example, the conformance test documents for IEEE 802.3 are numbered 1802.3™.

## Interpretations and errata

Interpretations and errata associated with this standard may be found at one of the following Internet locations:

- <http://standards.ieee.org/reading/ieee/interp/>
- <http://standards.ieee.org/reading/ieee/updates/errata/>

One such interpretation exists at the time of publication.

## Participants

This document was developed by the IEEE 802.16 Working Group on Broadband Wireless Access, which is responsible for Wireless Metropolitan Area Network (WirelessMAN™) Standards. The 802.16 Working Group had the following officers:

**Roger B. Marks, Chair**  
**Brian G. Kiernan, Vice Chair**  
**Carl J. Bushue, Secretary**

Louis Olsen served as Working Group Vice Chair during the initial development of this document, until September 2000. J. Scott Marin served as Secretary during the draft's development until December 2000.

Primary development was carried out by the Working Group's Task Group 1. The IEEE 802.16 Task Group 1 had the following officers:

**Roger B. Marks, Chair**  
**Carl Eklund, MAC Chair**  
**Jay Klein, PHY Chair**

The document finalization was overseen by an Editorial Committee. The IEEE 802.16 Task Group 1 Editorial Committee had the following officers:

**Roger B. Marks**, *Technical Editor*  
**Carl Eklund, Ken Stanwood, Stanley Wang**, *Lead MAC Editors*  
**Jay Klein, Lars Lindh**, *Lead PHY Editors*

Phil Guillemette, Wayne Hunter, Sergio Licardie, Ron Meyer, Vicente Quilez, Karl Stambaugh, Vladimir Yanover, and Juan Carlos Zúñiga made significant contributions to the draft as members of the Editorial Committee. Glen Sater served as editor in readying the document for Working Group Letter Ballot, with contributions by Jeffrey Foerster. Earlier, Brian Petry and James Mollenauer served as editors. For a period, Jung Yee served as MAC Chair and John Liebetreu as PHY Vice Chair. Brian Petry served as editor of the Functional Requirements Document on which this standard was developed; George Fishel chaired the development of that document. Juan Carlos Zúñiga, Phil Guillemette, Ron Meyer, and Nico van Waes served as secretaries.

Technical contributions to the document came from many individuals. The Lead Editors were the primary architects of the technical development.

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 approved:

|                        |                    |                    |
|------------------------|--------------------|--------------------|
| Song An                | Baruch Halachmi    | Yunsang Park       |
| Jori Arrakoski         | Michael Hamilton   | Brian Petry        |
| Arun Arunachalam       | Baya Hatim         | Wayne Pleasant     |
| Eli Avivi              | Srinath Hosur      | Moshe Ran          |
| C. R. Baugh            | Coleman Hum        | Stanley Reible     |
| Carlos Belfiore        | Wayne Hunter       | Valentine Rhodes   |
| Anader Benyamin-Seeyar | Eric Jacobsen      | David Ribner       |
| Carl Bushue            | Hamadi Jamali      | Gene Robinson      |
| Baruch Buskila         | Jacob Jorgensen    | Walt Roehr         |
| Dean Chang             | Mika Kasslin       | Durga Satapathy    |
| Naftali Chayat         | Brian Kiernan      | Glen Sater         |
| Rémi Chayer            | John Kim           | Vito Scaringi      |
| Mary Condie            | Itzik Kitroser     | Randall Schwartz   |
| José Costa             | Allan Klein        | Menashe Shahar     |
| Bruce Currivan         | Jay Klein          | Chet Shirali       |
| Amos Dotan             | Demosthenes Kostas | George Stamatelos  |
| Keith Doucet           | Yigal Leiba        | Karl Stambaugh     |
| Roger Durand           | Barry Lewis        | Ken Stanwood       |
| Brian Eidson           | Sergio Licardie    | Michael Stewart    |
| Carl Eklund            | John Liebetreu     | Paul Thompson      |
| David Falconer         | Lars Lindh         | Subir Varma        |
| George Fishel          | Willie Lu          | Nico van Waes      |
| Adrian Florea          | Fred Lucas         | Chao-Chun Wang     |
| Jeff Foerster          | J. Scott Marin     | Bob Ward           |
| Robert Foster          | Roger Marks        | Philip Whitehead   |
| Avi Freedman           | Andy McGregor      | David G. Williams  |
| G. Jack Garrison       | Ronald Meyer       | Vladimir Yanover   |
| Conrad Grell           | Andrew Middleton   | Huanchun Ye        |
| Phil Guillemette       | Apurva Mody        | Chaoming Zeng      |
| Zion Hadad             | Jim Mollenauer     | Juan Carlos Zúñiga |
|                        | William Myers      |                    |
|                        | Lou Olsen          |                    |

The following nonmembers also participated in the Working Group Letter Ballot:

|                      |                  |                |
|----------------------|------------------|----------------|
| Luis Contreras       | Antonis Karvelas | Vicente Quilez |
| Francisco Escrihuela | Tom Kolze        | Andy Schiltz   |
| Moritz Harteneck     | Gregorio Núñez   | Lei Wang       |
| Babis Kalatzis       | Subbu Ponnuswamy | Stanley Wang   |
|                      | Manuel Poza      |                |

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

|                       |                   |                   |
|-----------------------|-------------------|-------------------|
| Larry Arnett          | Stuart Kerry      | Roger Pandanda    |
| Tamer Beser           | Jay Klein         | Ken Peirce        |
| Tracy Black           | Timothy Lee       | Stephan Reis      |
| Wesley Brodsky        | Arthur Light      | Eugene Robinson   |
| James Carlo           | Jenshan Lin       | Walt Roehr        |
| Jose Costa            | David Linton      | Jaideep Roy       |
| Jagadish Kumar Dasari | Ahmad MahinFallah | Hiroyasu Shimizu  |
| Thomas Dineen         | James Scott Marin | Chet Shirali      |
| Vern Dubendorf        | Roger Marks       | Fredrik Tufvesson |
| Peter Ecclesine       | Peter Martini     | Joan Viaplana     |
| Keng Fong             | George May        | Stanley S. Wang   |
| Simon Harrison        | Roderick McMullin | Don Wright        |
| Vic Hayes             | Steve Methley     | Oren Yuen         |
| Hamadi Jamali         | Vlad Mitlin       | Jim Zerbe         |

When the IEEE-SA Standards Board approved this standard on 6 December 2001, it had the following membership:

**Donald N. Heirman**, *Chair*

**James T. Carlo**, *Vice Chair*

**Judith Gorman**, *Secretary*

Satish K. Aggarwal  
Mark D. Bowman  
Gary R. Engmann  
Harold E. Epstein  
H. Landis Floyd  
Jay Forster\*  
Howard M. Frazier  
Ruben D. Garzon

James H. Gurney  
Richard J. Holleman  
Lowell G. Johnson  
Robert J. Kennelly  
Joseph L. Koepfinger\*  
Peter H. Lips  
L. Bruce McClung  
Daleep C. Mohla

James W. Moore  
Robert F. Munzner  
Ronald C. Petersen  
Gerald H. Peterson  
John B. Posey  
Gary S. Robinson  
Akio Tojo  
Donald W. Zipse

\*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Alan Cookson, *NIST Representative*

Donald R. Volzka, *TAB Representative*

Jennifer McClain Longman  
*IEEE Standards Project Editor*

# Contents

|                                                     |    |
|-----------------------------------------------------|----|
| 1. Overview .....                                   | 1  |
| 1.1 Scope .....                                     | 1  |
| 1.2 Purpose .....                                   | 1  |
| 1.2.1 10–66 GHz licensed bands .....                | 1  |
| 1.2.2 2–11 GHz licensed bands .....                 | 1  |
| 1.3 Reference model .....                           | 3  |
| 2. References .....                                 | 5  |
| 3. Definitions .....                                | 8  |
| 4. Abbreviations and acronyms .....                 | 11 |
| 5. Service specific convergence sublayer .....      | 12 |
| 5.1 ATM convergence sublayer .....                  | 12 |
| 5.1.1 Convergence sublayer service definition ..... | 12 |
| 5.1.2 Data/Control plane .....                      | 12 |
| 5.1.2.1 PDU formats .....                           | 12 |
| 5.1.2.2 Classification .....                        | 13 |
| 5.1.2.2.1 VP-switched mode .....                    | 13 |
| 5.1.2.2.2 VC-switched mode .....                    | 13 |
| 5.1.2.3 Payload header suppression .....            | 13 |
| 5.1.2.3.1 PHS for VP-switched ATM connections ..... | 13 |
| 5.1.2.3.2 PHS for VC-switched ATM connections ..... | 14 |
| 5.1.2.4 Signaling procedure .....                   | 14 |
| 5.2 Packet convergence sublayer .....               | 15 |
| 5.2.1 MAC SDU format .....                          | 15 |
| 5.2.2 Classification .....                          | 16 |
| 5.2.3 Classification within the CS .....            | 17 |
| 5.2.4 Payload header suppression .....              | 18 |
| 5.2.4.1 PHS operation .....                         | 19 |
| 5.2.4.2 PHS signaling .....                         | 21 |
| 5.2.5 IEEE 802.3/Ethernet specific part .....       | 22 |
| 5.2.5.1 IEEE 802.3/Ethernet CS PDU format .....     | 22 |
| 5.2.5.2 IEEE 802.3/Ethernet CS classifiers .....    | 22 |
| 5.2.6 IEEE 802.1Q VLAN specific part .....          | 23 |
| 5.2.6.1 802.1Q VLAN CS PDU format .....             | 23 |
| 5.2.6.2 IEEE 802.1Q CS classifiers .....            | 23 |
| 5.2.7 IP specific part .....                        | 23 |
| 5.2.7.1 IP CS PDU format .....                      | 23 |
| 5.2.7.2 IP classifiers .....                        | 24 |
| 6. MAC common part sublayer (CPS) .....             | 24 |
| 6.1 MAC service definition .....                    | 25 |
| 6.1.1 Primitives .....                              | 26 |
| 6.1.1.1 MAC_CREATE_CONNECTION.request .....         | 27 |
| 6.1.1.1.1 Function .....                            | 27 |
| 6.1.1.1.2 Semantics of the service primitive .....  | 27 |
| 6.1.1.1.3 When generated .....                      | 28 |
| 6.1.1.1.4 Effect of receipt .....                   | 28 |
| 6.1.1.2 MAC_CREATE_CONNECTION.indication .....      | 28 |
| 6.1.1.2.1 Function .....                            | 28 |
| 6.1.1.2.2 Semantics of the service primitive .....  | 28 |
| 6.1.1.2.3 When generated .....                      | 28 |
| 6.1.1.2.4 Effect of receipt .....                   | 28 |
| 6.1.1.3 MAC_CREATE_CONNECTION.response .....        | 29 |

|            |                                                           |    |
|------------|-----------------------------------------------------------|----|
| 6.1.1.3.1  | Function .....                                            | 29 |
| 6.1.1.3.2  | Semantics of the service primitive .....                  | 29 |
| 6.1.1.3.3  | When generated .....                                      | 29 |
| 6.1.1.3.4  | Effect of receipt .....                                   | 29 |
| 6.1.1.4    | MAC_CREATE_CONNECTION.confirmation .....                  | 29 |
| 6.1.1.4.1  | Function .....                                            | 29 |
| 6.1.1.4.2  | Semantics of the service primitive .....                  | 30 |
| 6.1.1.4.3  | When generated .....                                      | 30 |
| 6.1.1.4.4  | Effect of receipt .....                                   | 30 |
| 6.1.1.5    | Changing an existing connection .....                     | 30 |
| 6.1.1.6    | MAC_TERMINATE_CONNECTION.request .....                    | 30 |
| 6.1.1.6.1  | Function .....                                            | 30 |
| 6.1.1.6.2  | Semantics of the service primitive .....                  | 30 |
| 6.1.1.6.3  | When generated .....                                      | 31 |
| 6.1.1.6.4  | Effect of receipt .....                                   | 31 |
| 6.1.1.7    | MAC_TERMINATE_CONNECTION.indication .....                 | 31 |
| 6.1.1.7.1  | Function .....                                            | 31 |
| 6.1.1.7.2  | Semantics of the service primitive .....                  | 31 |
| 6.1.1.7.3  | When generated .....                                      | 31 |
| 6.1.1.7.4  | Effect of receipt .....                                   | 31 |
| 6.1.1.8    | MAC_TERMINATE_CONNECTION.response .....                   | 31 |
| 6.1.1.8.1  | Function .....                                            | 31 |
| 6.1.1.8.2  | Semantics of the service primitive .....                  | 32 |
| 6.1.1.8.3  | When generated .....                                      | 32 |
| 6.1.1.8.4  | Effect of receipt .....                                   | 32 |
| 6.1.1.9    | MAC_TERMINATE_CONNECTION.confirmation .....               | 32 |
| 6.1.1.9.1  | Function .....                                            | 32 |
| 6.1.1.9.2  | Semantics of the service primitive .....                  | 32 |
| 6.1.1.9.3  | When generated .....                                      | 32 |
| 6.1.1.9.4  | Effect of receipt .....                                   | 33 |
| 6.1.1.10   | MAC_DATA.request .....                                    | 33 |
| 6.1.1.10.1 | Function .....                                            | 33 |
| 6.1.1.10.2 | Semantics of the service primitive .....                  | 33 |
| 6.1.1.10.3 | When generated .....                                      | 33 |
| 6.1.1.10.4 | Effect of receipt .....                                   | 33 |
| 6.1.1.11   | MAC_DATA.indication .....                                 | 33 |
| 6.1.1.11.1 | Function .....                                            | 33 |
| 6.1.1.11.2 | Semantics of the service primitive .....                  | 34 |
| 6.1.1.11.3 | When generated .....                                      | 34 |
| 6.1.1.11.4 | Effect of receipt .....                                   | 34 |
| 6.1.2      | MAC service stimulation of dynamic service messages ..... | 34 |
| 6.2        | Data/Control plane .....                                  | 36 |
| 6.2.1      | Addressing and connections .....                          | 36 |
| 6.2.2      | MAC PDU formats .....                                     | 37 |
| 6.2.2.1    | MAC header formats .....                                  | 37 |
| 6.2.2.1.1  | Generic MAC header .....                                  | 38 |
| 6.2.2.1.2  | Bandwidth request header .....                            | 40 |
| 6.2.2.2    | MAC subheaders .....                                      | 41 |
| 6.2.2.2.1  | Fragmentation subheader .....                             | 41 |
| 6.2.2.2.2  | Grant Management subheader .....                          | 42 |
| 6.2.2.2.3  | Packing subheader .....                                   | 43 |
| 6.2.2.3    | MAC Management Messages .....                             | 44 |
| 6.2.2.3.1  | Downlink Channel Descriptor (DCD) message .....           | 45 |
| 6.2.2.3.2  | Downlink Map (DL-MAP) message .....                       | 46 |

|            |                                                                 |    |
|------------|-----------------------------------------------------------------|----|
| 6.2.2.3.3  | Uplink Channel Descriptor (UCD) message .....                   | 47 |
| 6.2.2.3.4  | Uplink Map (UL-MAP) message .....                               | 49 |
| 6.2.2.3.5  | Ranging Request (RNG-REQ) message .....                         | 50 |
| 6.2.2.3.6  | Ranging Response (RNG-RSP) message .....                        | 51 |
| 6.2.2.3.7  | Registration Request (REG-REQ) message .....                    | 52 |
| 6.2.2.3.8  | Registration Response (REG-RSP) message .....                   | 52 |
| 6.2.2.3.9  | Privacy Key Management messages (PKM-REQ/PKM-RSP) .....         | 54 |
| 6.2.2.3.10 | Dynamic Service Addition—Request (DSA-REQ) message .....        | 62 |
| 6.2.2.3.11 | Dynamic Service Addition—Response (DSA-RSP) message .....       | 63 |
| 6.2.2.3.12 | Dynamic Service Addition—Acknowledge (DSA-ACK) message .....    | 64 |
| 6.2.2.3.13 | Dynamic Service Change—Request (DSC-REQ) message .....          | 65 |
| 6.2.2.3.14 | Dynamic Service Change—Response (DSC-RSP) message .....         | 66 |
| 6.2.2.3.15 | Dynamic Service Change—Acknowledge (DSC-ACK) message .....      | 67 |
| 6.2.2.3.16 | Dynamic Service Deletion—Request (DSD-REQ) message .....        | 68 |
| 6.2.2.3.17 | Dynamic Service Deletion—Response (DSD-RSP) message .....       | 69 |
| 6.2.2.3.18 | Multicast Polling Assignment Request (MCA-REQ) message .....    | 70 |
| 6.2.2.3.19 | Multicast Polling Assignment Response (MCA-RSP) message .....   | 71 |
| 6.2.2.3.20 | Downlink Burst Profile Change Request (DBPC-REQ) message .....  | 71 |
| 6.2.2.3.21 | Downlink Burst Profile Change Response (DBPC-RSP) message ..... | 72 |
| 6.2.2.3.22 | Reset Command (RES-CMD) message .....                           | 72 |
| 6.2.2.3.23 | SS Basic Capability Request (SBC-REQ) message .....             | 73 |
| 6.2.2.3.24 | SS Basic Capability Response (SBC-RSP) message .....            | 73 |
| 6.2.2.3.25 | Clock Comparison (CLK-CMP) message .....                        | 74 |
| 6.2.2.3.26 | De/Re-register Command (DREG-CMD) message .....                 | 75 |
| 6.2.2.3.27 | DSx Received (DSX-RVD) message .....                            | 76 |
| 6.2.2.3.28 | Config File TFTP Complete (TFTP-CPLT) message .....             | 77 |
| 6.2.2.3.29 | Config File TFTP Complete Response (TFTP-RSP) message .....     | 78 |
| 6.2.3      | Construction and transmission of MAC PDUs .....                 | 78 |
| 6.2.3.1    | Conventions .....                                               | 78 |
| 6.2.3.2    | Concatenation .....                                             | 79 |
| 6.2.3.3    | Fragmentation .....                                             | 80 |
| 6.2.3.4    | Packing .....                                                   | 80 |
| 6.2.3.4.1  | Packing fixed-length MAC SDUs .....                             | 80 |
| 6.2.3.4.2  | Packing variable-length MAC SDUs .....                          | 81 |
| 6.2.3.5    | CRC calculation .....                                           | 82 |
| 6.2.3.6    | Encryption of MAC PDUs .....                                    | 83 |
| 6.2.4      | ARQ mechanism .....                                             | 83 |
| 6.2.5      | Uplink scheduling service .....                                 | 83 |
| 6.2.5.1    | Unsolicited Grant Service .....                                 | 84 |
| 6.2.5.2    | Real-Time Polling Service .....                                 | 84 |
| 6.2.5.3    | Non-Real-Time Polling Service .....                             | 85 |
| 6.2.5.4    | Best Effort Service .....                                       | 85 |
| 6.2.6      | Bandwidth allocation and request mechanisms .....               | 85 |
| 6.2.6.1    | Requests .....                                                  | 86 |
| 6.2.6.2    | Grants per connection (GPC) mode .....                          | 86 |
| 6.2.6.3    | Grants per subscriber station (GPSS) mode .....                 | 87 |
| 6.2.6.4    | Polling .....                                                   | 88 |
| 6.2.6.4.1  | Unicast .....                                                   | 88 |
| 6.2.6.4.2  | Multicast and broadcast .....                                   | 90 |
| 6.2.6.4.3  | Poll-me bit .....                                               | 92 |
| 6.2.7      | MAC support of PHY .....                                        | 93 |
| 6.2.7.1    | Unframed Frequency Division Duplexing (FDD) .....               | 93 |
| 6.2.7.2    | Framed (burst) FDD .....                                        | 93 |
| 6.2.7.3    | Time Division Duplexing (TDD) .....                             | 94 |

|            |                                                                      |     |
|------------|----------------------------------------------------------------------|-----|
| 6.2.7.4    | Downlink Map .....                                                   | 95  |
| 6.2.7.5    | Uplink Map .....                                                     | 95  |
| 6.2.7.5.1  | Uplink timing .....                                                  | 95  |
| 6.2.7.5.2  | Uplink minislot definition .....                                     | 96  |
| 6.2.7.5.3  | Uplink interval definition .....                                     | 96  |
| 6.2.7.6    | Map relevance and synchronization .....                              | 97  |
| 6.2.7.6.1  | Map relevance for framed PHY systems .....                           | 97  |
| 6.2.7.6.2  | Map relevance for unframed PHY systems .....                         | 98  |
| 6.2.8      | Contention resolution .....                                          | 99  |
| 6.2.8.1    | Transmission opportunities .....                                     | 100 |
| 6.2.9      | Network entry and initialization .....                               | 100 |
| 6.2.9.1    | Scanning and synchronization to the downlink .....                   | 102 |
| 6.2.9.2    | Obtain downlink parameters .....                                     | 102 |
| 6.2.9.3    | Obtain uplink parameters .....                                       | 104 |
| 6.2.9.4    | Message flows during scanning and uplink parameter acquisition ..... | 106 |
| 6.2.9.5    | Initial ranging and automatic adjustments .....                      | 107 |
| 6.2.9.6    | Ranging parameter adjustment .....                                   | 109 |
| 6.2.9.7    | Negotiate basic capabilities .....                                   | 112 |
| 6.2.9.8    | SS authorization and key exchange .....                              | 112 |
| 6.2.9.9    | Registration .....                                                   | 112 |
| 6.2.9.9.1  | IP version negotiation .....                                         | 113 |
| 6.2.9.10   | Establish IP connectivity .....                                      | 114 |
| 6.2.9.11   | Establish time of day .....                                          | 114 |
| 6.2.9.12   | Transfer operational parameters .....                                | 115 |
| 6.2.9.13   | Establish provisioned connections .....                              | 115 |
| 6.2.10     | Ranging .....                                                        | 115 |
| 6.2.10.1   | Downlink burst profile management in framed operation .....          | 115 |
| 6.2.11     | Update of channel descriptors .....                                  | 120 |
| 6.2.12     | Assigning SSs to multicast groups .....                              | 122 |
| 6.2.13     | Quality of Service .....                                             | 125 |
| 6.2.13.1   | Theory of operation .....                                            | 125 |
| 6.2.13.2   | Service flows .....                                                  | 125 |
| 6.2.13.3   | Object model .....                                                   | 128 |
| 6.2.13.4   | Service classes .....                                                | 128 |
| 6.2.13.5   | Authorization .....                                                  | 129 |
| 6.2.13.6   | Types of service flows .....                                         | 130 |
| 6.2.13.6.1 | Provisioned service flows .....                                      | 130 |
| 6.2.13.6.2 | Admitted service flows .....                                         | 130 |
| 6.2.13.6.3 | Active service flows .....                                           | 131 |
| 6.2.13.7   | Preprovisioned service flow creation .....                           | 131 |
| 6.2.13.7.1 | Static operation .....                                               | 131 |
| 6.2.13.7.2 | Dynamic service flow creation .....                                  | 132 |
| 6.2.13.8   | Dynamic service .....                                                | 133 |
| 6.2.13.8.1 | Connection establishment .....                                       | 133 |
| 6.2.13.8.2 | Dynamic service flow state transitions .....                         | 134 |
| 6.2.13.8.3 | Dynamic Service Addition .....                                       | 143 |
| 6.2.13.8.4 | Dynamic Service Change (DSC) .....                                   | 154 |
| 6.2.13.8.5 | Connection release .....                                             | 165 |
| 7.         | Privacy Sublayer .....                                               | 169 |
| 7.1        | Architecture .....                                                   | 170 |
| 7.1.1      | Packet data encryption .....                                         | 170 |
| 7.1.2      | Key management protocol .....                                        | 170 |
| 7.1.3      | Security Associations .....                                          | 171 |
| 7.1.4      | Mapping of connections to Security Associations .....                | 171 |

|           |                                                                              |     |
|-----------|------------------------------------------------------------------------------|-----|
| 7.1.5     | Cryptographic Suite .....                                                    | 172 |
| 7.2       | PKM protocol .....                                                           | 172 |
| 7.2.1     | SS authorization and AK exchange overview .....                              | 172 |
| 7.2.2     | TEK exchange overview .....                                                  | 173 |
| 7.2.3     | Security capabilities selection .....                                        | 174 |
| 7.2.4     | Authorization state machine .....                                            | 174 |
| 7.2.4.1   | States .....                                                                 | 176 |
| 7.2.4.2   | Messages .....                                                               | 176 |
| 7.2.4.3   | Events .....                                                                 | 177 |
| 7.2.4.4   | Parameters .....                                                             | 178 |
| 7.2.4.5   | Actions .....                                                                | 178 |
| 7.2.5     | TEK state machine .....                                                      | 180 |
| 7.2.5.1   | States .....                                                                 | 182 |
| 7.2.5.2   | Messages .....                                                               | 183 |
| 7.2.5.3   | Events .....                                                                 | 183 |
| 7.2.5.4   | Parameters .....                                                             | 184 |
| 7.2.5.5   | Actions .....                                                                | 184 |
| 7.3       | Dynamic SA creation and mapping .....                                        | 186 |
| 7.3.1     | Dynamic SA creation .....                                                    | 186 |
| 7.3.2     | Dynamic mapping of SA .....                                                  | 186 |
| 7.4       | Key usage .....                                                              | 187 |
| 7.4.1     | BS key usage .....                                                           | 187 |
| 7.4.1.1   | AK key lifetime .....                                                        | 187 |
| 7.4.1.2   | AK transition period on BS side .....                                        | 187 |
| 7.4.1.3   | BS usage of AK .....                                                         | 189 |
| 7.4.1.4   | TEK lifetime .....                                                           | 189 |
| 7.4.1.5   | BS usage of TEK .....                                                        | 190 |
| 7.4.2     | SS key usage .....                                                           | 190 |
| 7.4.2.1   | SS reauthorization .....                                                     | 190 |
| 7.4.2.2   | SS usage of AK .....                                                         | 192 |
| 7.4.2.3   | SS usage of TEK .....                                                        | 192 |
| 7.5       | Cryptographic methods .....                                                  | 192 |
| 7.5.1     | Data encryption with DES .....                                               | 192 |
| 7.5.2     | Encryption of TEK with 3-DES .....                                           | 193 |
| 7.5.3     | Calculation of HMAC digests .....                                            | 193 |
| 7.5.4     | Derivation of TEKs, KEKs, and message authentication Keys .....              | 193 |
| 7.5.4.1   | DES Keys .....                                                               | 194 |
| 7.5.4.2   | 3-DES KEKs .....                                                             | 194 |
| 7.5.4.3   | HMAC authentication keys .....                                               | 194 |
| 7.5.5     | Public-Key encryption of authorization key .....                             | 194 |
| 7.5.6     | Digital signatures .....                                                     | 195 |
| 7.6       | Certificate profile .....                                                    | 195 |
| 7.6.1     | Certificate format .....                                                     | 195 |
| 7.6.1.1   | tbsCertificate.validity.notBefore and tbsCertificate.validity.notAfter ..... | 196 |
| 7.6.1.2   | tbsCertificate.serialNumber .....                                            | 196 |
| 7.6.1.3   | tbsCertificate.signature and signatureAlgorithm .....                        | 196 |
| 7.6.1.4   | tbsCertificate.issuer and tbsCertificate.subject .....                       | 196 |
| 7.6.1.4.1 | Manufacturer certificate .....                                               | 197 |
| 7.6.1.4.2 | SS certificate .....                                                         | 197 |
| 7.6.1.5   | tbsCertificate.subjectPublicKeyInfo .....                                    | 198 |
| 7.6.1.6   | tbsCertificate.issuerUniqueID and tbsCertificate.subjectUniqueID .....       | 198 |
| 7.6.1.7   | tbsCertificate.extensions .....                                              | 198 |
| 7.6.1.7.1 | SS certificates .....                                                        | 198 |
| 7.6.1.7.2 | Manufacturer certificates .....                                              | 198 |

|            |                                                       |     |
|------------|-------------------------------------------------------|-----|
| 7.6.1.8    | signatureValue .....                                  | 198 |
| 7.6.2      | SS certificate storage and management in the SS ..... | 198 |
| 7.6.3      | Certificate processing and management in the BS ..... | 199 |
| 8.         | Physical Layer.....                                   | 199 |
| 8.1        | Physical layer (PHY) service specification .....      | 199 |
| 8.1.1      | Scope.....                                            | 199 |
| 8.1.2      | PHY functions.....                                    | 199 |
| 8.1.3      | PHY SAP management.....                               | 200 |
| 8.1.3.1    | PHY MIB and generic SET/GET primitives .....          | 200 |
| 8.1.3.2    | Parameter sets (vectors) .....                        | 200 |
| 8.1.3.3    | PHY_SCHEDPARAM.request.....                           | 201 |
| 8.1.3.3.1  | Function .....                                        | 201 |
| 8.1.3.3.2  | Semantics of the service primitive.....               | 201 |
| 8.1.3.3.3  | When generated .....                                  | 201 |
| 8.1.3.3.4  | Effect of receipt .....                               | 201 |
| 8.1.3.4    | PHY_SCHEDPARAM.response .....                         | 201 |
| 8.1.3.4.1  | Function .....                                        | 201 |
| 8.1.3.4.2  | Semantics of the service primitive.....               | 202 |
| 8.1.3.4.3  | When generated .....                                  | 202 |
| 8.1.3.4.4  | Effect of receipt .....                               | 202 |
| 8.1.3.5    | PHY_DCD.indication .....                              | 202 |
| 8.1.3.5.1  | Function .....                                        | 202 |
| 8.1.3.5.2  | Semantics of the service primitive.....               | 202 |
| 8.1.3.5.3  | When generated .....                                  | 202 |
| 8.1.3.5.4  | Effect of receipt .....                               | 202 |
| 8.1.3.6    | PHY_DCD.request .....                                 | 202 |
| 8.1.3.7    | Function .....                                        | 202 |
| 8.1.3.7.1  | Semantics of the service primitive.....               | 202 |
| 8.1.3.7.2  | When generated .....                                  | 203 |
| 8.1.3.7.3  | Effect of receipt .....                               | 203 |
| 8.1.3.8    | PHY_DCD.confirmation .....                            | 203 |
| 8.1.3.8.1  | Function .....                                        | 203 |
| 8.1.3.8.2  | Semantics of the service primitive.....               | 203 |
| 8.1.3.8.3  | When generated .....                                  | 203 |
| 8.1.3.8.4  | Effect of receipt .....                               | 203 |
| 8.1.3.9    | PHY_DCD Primitives Example .....                      | 203 |
| 8.1.3.10   | PHY_UCD.indication .....                              | 203 |
| 8.1.3.10.1 | Function .....                                        | 204 |
| 8.1.3.10.2 | Semantics of the service primitive.....               | 204 |
| 8.1.3.10.3 | When generated .....                                  | 204 |
| 8.1.3.10.4 | Effect of receipt .....                               | 204 |
| 8.1.3.11   | PHY_UCD.request .....                                 | 204 |
| 8.1.3.11.1 | Function .....                                        | 204 |
| 8.1.3.11.2 | Semantics of the service primitive.....               | 204 |
| 8.1.3.11.3 | When generated .....                                  | 204 |
| 8.1.3.11.4 | Effect of receipt .....                               | 204 |
| 8.1.3.12   | PHY_UCD.confirmation .....                            | 204 |
| 8.1.3.12.1 | Function .....                                        | 204 |
| 8.1.3.12.2 | Semantics of the service primitive.....               | 205 |
| 8.1.3.12.3 | When generated .....                                  | 205 |
| 8.1.3.12.4 | Effect of receipt .....                               | 205 |
| 8.1.3.13   | UCD primitives example .....                          | 205 |
| 8.1.3.14   | PHY_RNG.request .....                                 | 205 |
| 8.1.3.14.1 | Function .....                                        | 205 |

|            |                                         |     |
|------------|-----------------------------------------|-----|
| 8.1.3.14.2 | Semantics of the service primitive..... | 205 |
| 8.1.3.14.3 | When generated .....                    | 205 |
| 8.1.3.14.4 | Effect of receipt .....                 | 206 |
| 8.1.3.15   | PHY_RNG.confirmation .....              | 206 |
| 8.1.3.15.1 | Function .....                          | 206 |
| 8.1.3.15.2 | Semantics of the service primitive..... | 206 |
| 8.1.3.15.3 | When generated .....                    | 206 |
| 8.1.3.15.4 | Effect of receipt .....                 | 206 |
| 8.1.3.16   | PHY_RNG.indication .....                | 206 |
| 8.1.3.16.1 | Function .....                          | 206 |
| 8.1.3.16.2 | Semantics of the service primitive..... | 206 |
| 8.1.3.16.3 | When generated .....                    | 206 |
| 8.1.3.16.4 | Effect of receipt .....                 | 206 |
| 8.1.3.16.5 | Ranging primitives examples.....        | 206 |
| 8.1.3.17   | PHY_TXSTART.request.....                | 207 |
| 8.1.3.17.1 | Function .....                          | 207 |
| 8.1.3.17.2 | Semantics of the service primitive..... | 207 |
| 8.1.3.17.3 | When generated .....                    | 207 |
| 8.1.3.17.4 | Effect of receipt .....                 | 208 |
| 8.1.3.18   | PHY_TXSTART.confirmation.....           | 208 |
| 8.1.3.18.1 | Function .....                          | 208 |
| 8.1.3.18.2 | Semantics of the service primitive..... | 208 |
| 8.1.3.18.3 | When generated .....                    | 208 |
| 8.1.3.18.4 | Effect of receipt .....                 | 208 |
| 8.1.3.19   | PHY_TXSTART.indication .....            | 208 |
| 8.1.3.19.1 | Function .....                          | 208 |
| 8.1.3.19.2 | Semantics of the service primitive..... | 208 |
| 8.1.3.19.3 | When generated .....                    | 208 |
| 8.1.3.19.4 | Effect of receipt .....                 | 208 |
| 8.1.3.20   | PHY_MACPDU.request.....                 | 208 |
| 8.1.3.20.1 | Function .....                          | 208 |
| 8.1.3.20.2 | Semantics of the service primitive..... | 209 |
| 8.1.3.20.3 | When generated .....                    | 209 |
| 8.1.3.20.4 | Effect of receipt .....                 | 209 |
| 8.1.3.21   | PHY_MACPDU.confirmation.....            | 209 |
| 8.1.3.21.1 | Function .....                          | 209 |
| 8.1.3.21.2 | Semantics of the service primitive..... | 209 |
| 8.1.3.21.3 | When generated .....                    | 209 |
| 8.1.3.21.4 | Effect of receipt .....                 | 209 |
| 8.1.3.22   | PHY_TXEND.indication.....               | 209 |
| 8.1.3.22.1 | Function .....                          | 209 |
| 8.1.3.22.2 | Semantics of the service primitive..... | 209 |
| 8.1.3.22.3 | When generated .....                    | 210 |
| 8.1.3.22.4 | Effect of receipt .....                 | 210 |
| 8.1.3.23   | PHY_RXSTART.request.....                | 210 |
| 8.1.3.23.1 | Function .....                          | 210 |
| 8.1.3.23.2 | Semantics of the service primitive..... | 210 |
| 8.1.3.23.3 | When generated .....                    | 210 |
| 8.1.3.23.4 | Effect of receipt .....                 | 210 |
| 8.1.3.24   | PHY_RXSTART.confirmation.....           | 210 |
| 8.1.3.24.1 | Function .....                          | 210 |
| 8.1.3.24.2 | Semantics of the service primitive..... | 210 |
| 8.1.3.24.3 | When generated .....                    | 210 |
| 8.1.3.24.4 | Effect of receipt .....                 | 210 |

|            |                                                             |     |
|------------|-------------------------------------------------------------|-----|
| 8.1.3.25   | PHY_RXSTART.indication .....                                | 211 |
| 8.1.3.25.1 | Function .....                                              | 211 |
| 8.1.3.25.2 | Semantics of the service primitive .....                    | 211 |
| 8.1.3.25.3 | When generated .....                                        | 211 |
| 8.1.3.25.4 | Effect of receipt .....                                     | 211 |
| 8.1.3.26   | PHY_MACPDU.indication .....                                 | 211 |
| 8.1.3.26.1 | Function .....                                              | 211 |
| 8.1.3.26.2 | Semantics of the service primitive .....                    | 211 |
| 8.1.3.26.3 | When generated .....                                        | 211 |
| 8.1.3.26.4 | Effect of receipt .....                                     | 211 |
| 8.1.3.27   | PHY_RXEND.indication .....                                  | 211 |
| 8.1.3.27.1 | Function .....                                              | 211 |
| 8.1.3.27.2 | Semantics of the service primitive .....                    | 211 |
| 8.1.3.27.3 | When generated .....                                        | 212 |
| 8.1.3.27.4 | Effect of receipt .....                                     | 212 |
| 8.1.3.28   | Data transfer related primitives example .....              | 212 |
| 8.2        | Physical layer for 10–66 GHz .....                          | 213 |
| 8.2.1      | Overview .....                                              | 213 |
| 8.2.2      | PHY SAP parameter definitions .....                         | 214 |
| 8.2.2.1    | SCHED_PARAM_VECTOR .....                                    | 214 |
| 8.2.2.2    | DCD_PARAM_VECTOR .....                                      | 214 |
| 8.2.2.3    | UCD_PARAM_VEC .....                                         | 215 |
| 8.2.2.4    | RNG_REQ_VECTOR .....                                        | 215 |
| 8.2.2.5    | RNG_IND_VECTOR .....                                        | 215 |
| 8.2.2.6    | TXVECTOR .....                                              | 216 |
| 8.2.2.7    | TXSTATUS .....                                              | 216 |
| 8.2.2.8    | RXVECTOR .....                                              | 216 |
| 8.2.2.9    | RXSTATUS .....                                              | 216 |
| 8.2.3      | Framing .....                                               | 217 |
| 8.2.3.1    | Supported frame durations .....                             | 217 |
| 8.2.4      | Duplexing techniques and PHY Type parameter encodings ..... | 218 |
| 8.2.4.1    | FDD operation .....                                         | 218 |
| 8.2.4.2    | TDD operation .....                                         | 218 |
| 8.2.4.2.1  | Tx/Rx Transition Gap .....                                  | 219 |
| 8.2.4.2.2  | Rx/Tx Transition Gap .....                                  | 219 |
| 8.2.5      | Downlink PHY .....                                          | 219 |
| 8.2.5.1    | Downlink subframe .....                                     | 219 |
| 8.2.5.1.1  | Downlink burst preambles .....                              | 221 |
| 8.2.5.1.2  | Frame control section .....                                 | 223 |
| 8.2.5.2    | Downlink burst allocation .....                             | 226 |
| 8.2.5.3    | Downlink transmission CS .....                              | 228 |
| 8.2.5.4    | Downlink physical medium dependent (PMD) sublayer .....     | 229 |
| 8.2.5.4.1  | Burst profile definitions .....                             | 229 |
| 8.2.5.4.2  | Downlink PHY SS capability set parameters .....             | 230 |
| 8.2.5.4.3  | Randomization .....                                         | 230 |
| 8.2.5.4.4  | Downlink forward error correction .....                     | 231 |
| 8.2.5.4.5  | Definition of parameters for burst profile (DIUC=0) .....   | 239 |
| 8.2.5.4.6  | Coding of the control portion of the frame .....            | 239 |
| 8.2.5.4.7  | Downlink modulation .....                                   | 240 |
| 8.2.5.4.8  | Baseband pulse shaping .....                                | 245 |
| 8.2.5.4.9  | Transmitted waveform .....                                  | 245 |
| 8.2.5.4.10 | Summary of downlink physical layer parameters .....         | 246 |
| 8.2.6      | Uplink physical layer .....                                 | 246 |
| 8.2.6.1    | Uplink subframe .....                                       | 246 |

|            |                                                                        |     |
|------------|------------------------------------------------------------------------|-----|
| 8.2.6.1.1  | Uplink burst preamble .....                                            | 247 |
| 8.2.6.1.2  | UL_MAP_Information_Element definition .....                            | 248 |
| 8.2.6.1.3  | Required UCD parameters .....                                          | 250 |
| 8.2.6.1.4  | Uplink channel .....                                                   | 250 |
| 8.2.6.1.5  | Uplink_Burst_Profile .....                                             | 250 |
| 8.2.6.2    | Uplink transmission CS .....                                           | 251 |
| 8.2.6.3    | Uplink PHY1 medium dependent sublayer .....                            | 251 |
| 8.2.6.3.1  | Randomization for spectrum shaping .....                               | 251 |
| 8.2.6.3.2  | Uplink Forward Error Correction .....                                  | 252 |
| 8.2.6.3.3  | Shortening of FEC blocks in uplink .....                               | 253 |
| 8.2.6.3.4  | Number of scheduled uplink bursts per frame .....                      | 254 |
| 8.2.6.3.5  | Coding of the Request IE Uplink_Burst_Profile .....                    | 254 |
| 8.2.6.3.6  | Coding of the Initial Maintenance Uplink_Burst_Profile .....           | 254 |
| 8.2.6.3.7  | Uplink Modulation .....                                                | 254 |
| 8.2.6.3.8  | Baseband pulse shaping .....                                           | 254 |
| 8.2.6.3.9  | Transmitted waveform .....                                             | 254 |
| 8.2.6.3.10 | Summary of uplink PHY parameters .....                                 | 255 |
| 8.2.7      | Baud rates and channel bandwidths .....                                | 255 |
| 8.2.8      | Radio subsystem control .....                                          | 256 |
| 8.2.8.1    | Synchronization technique .....                                        | 256 |
| 8.2.8.2    | Frequency control .....                                                | 256 |
| 8.2.8.3    | Power control .....                                                    | 256 |
| 8.2.9      | Minimum performance .....                                              | 256 |
| 8.2.9.1    | Propagation conditions .....                                           | 259 |
| 8.2.9.1.1  | Propagation models .....                                               | 260 |
| 8.2.9.1.2  | Rain fades .....                                                       | 260 |
| 8.2.9.2    | Transmitter characteristics .....                                      | 261 |
| 8.2.9.2.1  | Output power .....                                                     | 261 |
| 8.2.9.2.2  | Emission mask .....                                                    | 261 |
| 8.2.9.2.3  | Modulation accuracy and error vector magnitude .....                   | 263 |
| 9.         | Configuration file .....                                               | 264 |
| 9.1        | SS IP addressing .....                                                 | 264 |
| 9.1.1      | Dynamic Host Configuration Protocol (DHCP) fields used by the SS ..... | 264 |
| 9.2        | SS Configuration .....                                                 | 265 |
| 9.2.1      | SS binary configuration file format .....                              | 265 |
| 9.2.2      | Configuration file settings .....                                      | 266 |
| 9.2.3      | Configuration file creation .....                                      | 266 |
| 9.2.3.1    | SS MIC calculation .....                                               | 267 |
| 10.        | Parameters and Constants .....                                         | 267 |
| 10.1       | Global values .....                                                    | 267 |
| 10.2       | PKM parameter values .....                                             | 271 |
| 10.3       | PHY-specific values .....                                              | 272 |
| 10.3.1     | 10–66 GHz parameter and constant definitions .....                     | 272 |
| 10.3.1.1   | Physical Slot (PS) .....                                               | 272 |
| 10.3.1.2   | Symbol rate .....                                                      | 272 |
| 10.3.1.3   | Uplink center frequency .....                                          | 272 |
| 10.3.1.4   | Downlink center frequency .....                                        | 272 |
| 10.3.1.5   | Tolerated poll jitter .....                                            | 272 |
| 10.4       | Well-known addresses and identifiers .....                             | 272 |
| 11.        | TLV encodings .....                                                    | 272 |
| 11.1       | MAC management message encodings .....                                 | 273 |
| 11.1.1     | UCD message encodings .....                                            | 273 |
| 11.1.1.1   | UCD channel encodings .....                                            | 273 |
| 11.1.1.2   | Uplink burst profile encodings for 10–66 GHz systems .....             | 274 |

|            |                                                              |     |
|------------|--------------------------------------------------------------|-----|
| 11.1.2     | DCD message encodings .....                                  | 275 |
| 11.1.2.1   | DCD channel encodings .....                                  | 275 |
| 11.1.2.2   | Downlink burst profile encodings for 10–66 GHz systems ..... | 276 |
| 11.1.3     | RNG-REQ message encodings .....                              | 277 |
| 11.1.4     | RNG-RSP message encodings .....                              | 278 |
| 11.1.5     | MCA-REQ and MCA-RSP TLV encodings .....                      | 279 |
| 11.2       | PKM message encodings .....                                  | 279 |
| 11.2.1     | Display-string .....                                         | 281 |
| 11.2.2     | AUTH-Key .....                                               | 281 |
| 11.2.3     | TEK .....                                                    | 281 |
| 11.2.4     | Key lifetime .....                                           | 281 |
| 11.2.5     | Key-Sequence-Number .....                                    | 282 |
| 11.2.6     | HMAC digest .....                                            | 282 |
| 11.2.7     | SAID .....                                                   | 282 |
| 11.2.8     | TEK parameters .....                                         | 282 |
| 11.2.9     | CBC-IV .....                                                 | 283 |
| 11.2.10    | Error Code .....                                             | 283 |
| 11.2.11    | CA certificate .....                                         | 284 |
| 11.2.12    | SS certificate .....                                         | 285 |
| 11.2.13    | Security capabilities .....                                  | 285 |
| 11.2.14    | Cryptographic suite .....                                    | 285 |
| 11.2.15    | Cryptographic-Suite-List .....                               | 286 |
| 11.2.16    | Version .....                                                | 287 |
| 11.2.17    | SA descriptor .....                                          | 287 |
| 11.2.18    | SA type .....                                                | 287 |
| 11.2.19    | PKM configuration settings .....                             | 288 |
| 11.2.19.1  | Authorize wait timeout .....                                 | 288 |
| 11.2.19.2  | Reauthorize wait timeout .....                               | 288 |
| 11.2.19.3  | Authorization grace time .....                               | 289 |
| 11.2.19.4  | Operational wait timeout .....                               | 289 |
| 11.2.19.5  | Rekey wait timeout .....                                     | 289 |
| 11.2.19.6  | TEK grace time .....                                         | 289 |
| 11.2.19.7  | Authorize reject wait timeout .....                          | 289 |
| 11.3       | Configuration file encodings .....                           | 290 |
| 11.3.1     | End-of-data marker .....                                     | 290 |
| 11.3.2     | Pad configuration setting .....                              | 290 |
| 11.3.3     | Software upgraded filename .....                             | 290 |
| 11.3.4     | SNMP write-access control .....                              | 290 |
| 11.3.5     | SNMP MIB Object .....                                        | 291 |
| 11.3.6     | Software upgrade TFTP server .....                           | 291 |
| 11.4       | Common encodings .....                                       | 292 |
| 11.4.1     | SS Capabilities encoding .....                               | 292 |
| 11.4.1.1   | Uplink CID support .....                                     | 292 |
| 11.4.1.2   | Physical parameters supported .....                          | 292 |
| 11.4.1.2.1 | 10–66 GHz PHY SS demodulator types .....                     | 292 |
| 11.4.1.2.2 | 10–66 GHz PHY SS modulator types .....                       | 293 |
| 11.4.1.2.3 | 10–66 GHz PHY SS downlink FEC types .....                    | 293 |
| 11.4.1.2.4 | 10–66 GHz PHY SS uplink FEC types .....                      | 293 |
| 11.4.1.3   | PKM flow control .....                                       | 294 |
| 11.4.1.4   | DSx flow control .....                                       | 294 |
| 11.4.1.5   | MCA flow control .....                                       | 294 |
| 11.4.1.6   | Bandwidth allocation support .....                           | 294 |
| 11.4.1.7   | IP Version .....                                             | 294 |
| 11.4.1.8   | MAC CRC support .....                                        | 294 |

|                                          |                                                                     |     |
|------------------------------------------|---------------------------------------------------------------------|-----|
| 11.4.1.9                                 | Multicast polling group CID support.....                            | 295 |
| 11.4.2                                   | SS Message integrity check (MIC) configuration setting.....         | 295 |
| 11.4.3                                   | Vendor ID encoding.....                                             | 295 |
| 11.4.4                                   | MAC version encodings .....                                         | 296 |
| 11.4.5                                   | Convergence sublayer capabilities.....                              | 296 |
| 11.4.5.1                                 | Convergence sublayer support.....                                   | 296 |
| 11.4.5.2                                 | Maximum number of classifiers .....                                 | 297 |
| 11.4.5.3                                 | Payload header suppression support.....                             | 297 |
| 11.4.6                                   | Trivial File Transfer Protocol (TFTP) Server Timestamp.....         | 297 |
| 11.4.7                                   | TFTP Server Provisioned SS Address .....                            | 297 |
| 11.4.8                                   | Service flow encodings .....                                        | 298 |
| 11.4.8.1                                 | Service flow identifier .....                                       | 298 |
| 11.4.8.2                                 | Connection identifier .....                                         | 298 |
| 11.4.8.3                                 | Service Class Name .....                                            | 299 |
| 11.4.8.4                                 | Service Flow Error Parameter Set .....                              | 299 |
| 11.4.8.4.1                               | Errored parameter .....                                             | 300 |
| 11.4.8.4.2                               | Error code .....                                                    | 300 |
| 11.4.8.4.3                               | Error message .....                                                 | 300 |
| 11.4.8.5                                 | QoS parameter set type .....                                        | 300 |
| 11.4.8.6                                 | Traffic priority .....                                              | 301 |
| 11.4.8.7                                 | Maximum sustained traffic rate .....                                | 302 |
| 11.4.8.8                                 | Maximum traffic burst.....                                          | 303 |
| 11.4.8.9                                 | Minimum reserved traffic rate .....                                 | 303 |
| 11.4.8.10                                | Vendor specific QoS parameters .....                                | 303 |
| 11.4.8.11                                | Service flow scheduling type.....                                   | 304 |
| 11.4.8.12                                | Request/transmission policy .....                                   | 304 |
| 11.4.8.13                                | Tolerated jitter.....                                               | 304 |
| 11.4.8.14                                | Maximum latency .....                                               | 305 |
| 11.4.8.15                                | Fixed-length versus variable-length SDU indicator .....             | 305 |
| 11.4.8.16                                | SDU size .....                                                      | 305 |
| 11.4.8.17                                | Target SAID.....                                                    | 306 |
| 11.4.9                                   | CS specific service flow encodings .....                            | 306 |
| 11.4.9.1                                 | CS specification .....                                              | 306 |
| 11.4.9.2                                 | Convergence Sublayer Parameter Encoding Rules .....                 | 306 |
| 11.4.9.3                                 | Packet CS encodings for configuration and MAC-layer messaging ..... | 307 |
| 11.4.9.3.1                               | Configuration-file-specific settings .....                          | 307 |
| 11.4.9.3.2                               | REG-REQ/REG-RSP specific encodings.....                             | 307 |
| 11.4.9.3.3                               | QoS-related encodings.....                                          | 307 |
| 11.4.9.3.4                               | Dynamic service change action .....                                 | 307 |
| 11.4.9.3.5                               | Classifier error parameter set.....                                 | 307 |
| 11.4.9.3.6                               | Packet classification rule .....                                    | 309 |
| 11.4.9.3.7                               | PHS Rule.....                                                       | 315 |
| 11.4.9.4                                 | ATM CS Encodings for Configuration and MAC-Layer Messaging.....     | 317 |
| 11.4.9.4.1                               | ATM switching encoding .....                                        | 317 |
| 11.4.9.4.2                               | VPI classifier.....                                                 | 318 |
| 11.4.9.4.3                               | VCI classification .....                                            | 318 |
| 11.4.10                                  | HMAC Tuple .....                                                    | 318 |
| 11.4.11                                  | Vendor-specific information.....                                    | 319 |
| 11.4.12                                  | Confirmation code .....                                             | 320 |
| 12.                                      | System profiles .....                                               | 320 |
| 12.1                                     | Basic ATM system profile.....                                       | 320 |
| Annex A (informative) Bibliography ..... |                                                                     | 322 |

## List of Figures

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| Figure 1—IEEE Std 802.16-2001 protocol layering, showing service access points (SAPs).....                         | 2   |
| Figure 2—PDU and SDU in a protocol stack.....                                                                      | 7   |
| Figure 3—ATM CS PDU format.....                                                                                    | 12  |
| Figure 4—CS PDU format for VP-switched ATM connections.....                                                        | 14  |
| Figure 5—CS PDU format for VC-switched ATM connections.....                                                        | 14  |
| Figure 6—MAC SDU Format .....                                                                                      | 16  |
| Figure 7—Classification and CID Mapping (BS to SS).....                                                            | 17  |
| Figure 8—Classification and CID Mapping (SS to BS).....                                                            | 17  |
| Figure 9—Payload header suppression operation .....                                                                | 20  |
| Figure 10—Payload header suppression with masking.....                                                             | 21  |
| Figure 11—Payload header suppression signaling example .....                                                       | 22  |
| Figure 12—IEEE 802.3/Ethernet CS PDU format without header suppression .....                                       | 22  |
| Figure 13—IEEE 802.3/Ethernet CS PDU format with header suppression .....                                          | 22  |
| Figure 14—IEEE 802.1Q VLAN CS PDU format.....                                                                      | 23  |
| Figure 15—IP CS PDU format IEEE 802.3/Ethernet CS PDU format without header suppression .....                      | 24  |
| Figure 16—IP CS PDU format IEEE 802.3/Ethernet CS PDU format with header suppression .....                         | 24  |
| Figure 17—Use of primitives to request service of MAC sublayer and generate response.....                          | 26  |
| Figure 18—MAC SAP event and MAC event sequence for connection creation stimulated by<br>convergence sublayer.....  | 35  |
| Figure 19—MAC SAP event and MAC event sequence for connection change stimulated by<br>convergence sublayer.....    | 35  |
| Figure 20—MAC SAP event and MAC event sequence for connection deletion stimulated by<br>convergence sublayer ..... | 36  |
| Figure 21—MAC PDU formats.....                                                                                     | 37  |
| Figure 22—Generic MAC header format.....                                                                           | 38  |
| Figure 23—Bandwidth request header format.....                                                                     | 40  |
| Figure 24—MAC Management Message Format .....                                                                      | 44  |
| Figure 25—Construction of a MAC PDU .....                                                                          | 79  |
| Figure 26—MAC PDU concatenation showing example CIDs .....                                                         | 80  |
| Figure 27—Packing fixed-length MAC SDUs into a single MAC PDU .....                                                | 81  |
| Figure 28—Packing variable-length MAC SDUs into a single MAC PDU.....                                              | 81  |
| Figure 29—Packing a single variable-length MAC SDU into a single MAC PDU .....                                     | 81  |
| Figure 30—Packing with fragmentation.....                                                                          | 82  |
| Figure 31—MAC PDU encryption.....                                                                                  | 83  |
| Figure 32—SS GPC mode flow chart.....                                                                              | 87  |
| Figure 33—SS GPSS mode flow chart.....                                                                             | 89  |
| Figure 34—Unicast polling .....                                                                                    | 90  |
| Figure 35—Multicast and broadcast polling .....                                                                    | 92  |
| Figure 36—Poll-Me bit usage.....                                                                                   | 93  |
| Figure 37—Example of Burst FDD bandwidth allocation .....                                                          | 94  |
| Figure 38—TDD frame structure .....                                                                                | 95  |
| Figure 39—Maximum time relevance of PHY and MAC control information (TDD).....                                     | 97  |
| Figure 40—Minimum time relevance of PHY and MAC control information (TDD) .....                                    | 97  |
| Figure 41—Maximum time relevance of PHY and MAC control information (FDD).....                                     | 98  |
| Figure 42—Minimum time relevance of PHY and MAC control information (FDD) .....                                    | 98  |
| Figure 43—Time relevance of UL-Map information (unframed FDD).....                                                 | 99  |
| Figure 44—Example of Request IE containing multiple transmission opportunities .....                               | 100 |
| Figure 45—SS Initialization overview .....                                                                         | 101 |
| Figure 46—Obtaining downlink synchronization .....                                                                 | 103 |
| Figure 47—Maintaining downlink synchronization.....                                                                | 103 |
| Figure 48—Obtaining uplink parameters .....                                                                        | 105 |

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| Figure 49—Maintain uplink parameters, single uplink case, ChID=i .....                      | 106 |
| Figure 50—Initial Ranging—SS .....                                                          | 110 |
| Figure 51—Initial Ranging—BS .....                                                          | 111 |
| Figure 52—Registration—SS .....                                                             | 112 |
| Figure 53—Wait for registration response—SS .....                                           | 112 |
| Figure 54—Registration—BS .....                                                             | 113 |
| Figure 55—Periodic Ranging—BS .....                                                         | 116 |
| Figure 56—Periodic Ranging—SS .....                                                         | 117 |
| Figure 57—Transition to a more robust burst profile .....                                   | 118 |
| Figure 58—Transition to a less robust burst profile .....                                   | 119 |
| Figure 59—Burst profile threshold usage .....                                               | 120 |
| Figure 60—Multicast polling assignment—SS .....                                             | 123 |
| Figure 61—Multicast polling assignment—BS .....                                             | 124 |
| Figure 62—Provisioned authorization model “envelopes” .....                                 | 127 |
| Figure 63—Dynamic authorization model “envelopes” .....                                     | 127 |
| Figure 64—Theory of Operation Object Model .....                                            | 128 |
| Figure 65—DSA message flow—SS-initiated .....                                               | 132 |
| Figure 66—DSA message flow—BS-initiated .....                                               | 133 |
| Figure 67—Dynamic service flow overview .....                                               | 134 |
| Figure 68—Dynamic service flow state transition diagram .....                               | 137 |
| Figure 69—DSA—Locally initiated transaction state transition diagram .....                  | 138 |
| Figure 70—DSA—Remotely initiated transaction state transition diagram .....                 | 139 |
| Figure 71—DSC—Locally initiated transaction state transition diagram .....                  | 140 |
| Figure 72—DSC—Remotely initiated transaction state transition diagram .....                 | 141 |
| Figure 73—DSD—Locally initiated transaction state transition diagram .....                  | 142 |
| Figure 74—DSD—Remotely initiated transaction state transition diagram .....                 | 143 |
| Figure 75—DSA—Locally initiated transaction begin state flow diagram .....                  | 146 |
| Figure 76—DSA—Locally initiated transaction DSA-RSP pending state flow diagram .....        | 147 |
| Figure 77—DSA—Locally initiated transaction holding state flow diagram .....                | 148 |
| Figure 78—DSA—Locally initiated transaction retries exhausted state flow diagram .....      | 149 |
| Figure 79—DSA—Locally initiated transaction deleting service flow state flow diagram .....  | 150 |
| Figure 80—DSA—Remotely initiated transaction begin state flow diagram .....                 | 151 |
| Figure 81—DSA—Remotely initiated transaction DSA-ACK pending state flow diagram .....       | 152 |
| Figure 82—DSA—Remotely initiated transaction holding down state flow diagram .....          | 153 |
| Figure 83—DSA—Remotely initiated transaction deleting service state flow diagram .....      | 153 |
| Figure 84—DSC—Locally initiated transaction begin state flow diagram .....                  | 157 |
| Figure 85—DSC—Locally initiated transaction DSC-RSP pending state flow diagram .....        | 158 |
| Figure 86—DSC—Locally initiated transaction holding down state flow diagram .....           | 159 |
| Figure 87—DSC—Locally initiated transaction retries exhausted state flow diagram .....      | 160 |
| Figure 88—DSC—Locally initiated transaction deleting service flow state flow diagram .....  | 161 |
| Figure 89—DSC—Remotely initiated transaction begin state flow diagram .....                 | 162 |
| Figure 90—DSC—Remotely initiated transaction DSC-ACK pending state flow diagram .....       | 163 |
| Figure 91—DSC—Remotely initiated transaction holding down state flow diagram .....          | 164 |
| Figure 92—DSC—Remotely initiated transaction deleting service flow state flow diagram ..... | 164 |
| Figure 93—DSD—Locally initiated transaction begin state flow diagram .....                  | 166 |
| Figure 94—DSD—Locally initiated transaction DSD-RSP pending state flow diagram .....        | 167 |
| Figure 95—DSD—Locally initiated transaction holding down state flow diagram .....           | 168 |
| Figure 96—DSD—Remotely initiated transaction begin state flow diagram .....                 | 169 |
| Figure 97—Authorization state machine flow diagram .....                                    | 175 |
| Figure 98—TEK state machine flow diagram .....                                              | 181 |
| Figure 99—AK management in BS and SS .....                                                  | 188 |
| Figure 100—TEK management in BS and SS .....                                                | 191 |
| Figure 101—Example of usage of PHY_DCD primitives .....                                     | 203 |
| Figure 102—Example of usage of PHY_UCD primitives .....                                     | 205 |

|                                                                                              |     |
|----------------------------------------------------------------------------------------------|-----|
| Figure 103—Example of usage of the PHY_RNG primitives with unsolicited RNG-RSP message ..... | 207 |
| Figure 104—Example of usage of the PHY_RNG primitives: RNG-REQ and RNG-RSP messages .....    | 207 |
| Figure 105—Example of usage of primitives during downlink PHY PDU transfer .....             | 212 |
| Figure 106—Example of usage of primitives during uplink PHY PDU transfer .....               | 213 |
| Figure 107—Example of FDD bandwidth allocation .....                                         | 218 |
| Figure 108—TDD frame structure .....                                                         | 219 |
| Figure 109—TDD downlink subframe structure .....                                             | 220 |
| Figure 110—FDD downlink subframe structure .....                                             | 221 |
| Figure 111—Downlink map usage with shortened FEC blocks—TDM case .....                       | 227 |
| Figure 112—Downlink map usage with shortened FEC blocks—TDMA case .....                      | 228 |
| Figure 113—Format of the downlink transmission convergence sublayer PDU .....                | 228 |
| Figure 114—Conceptual block diagram of the downlink PMD sublayer .....                       | 229 |
| Figure 115—Randomizer logic diagram .....                                                    | 230 |
| Figure 116—Inner code for Code Type 2 in the downlink .....                                  | 234 |
| Figure 117—Two-dimensional product code matrix .....                                         | 235 |
| Figure 118—Example encoder for a (16,11) extended Hamming Code .....                         | 236 |
| Figure 119—Structure of shortened 2 D block .....                                            | 238 |
| Figure 120—QPSK constellation .....                                                          | 240 |
| Figure 121—16-QAM constellation (gray-coded) .....                                           | 241 |
| Figure 122—64-QAM Constellation (gray-coded) .....                                           | 243 |
| Figure 123—Uplink subframe structure .....                                                   | 247 |
| Figure 124—Conceptual block diagram of the uplink PHY .....                                  | 251 |
| Figure 125—Structure of shortened 2 D block .....                                            | 253 |
| Figure 126—ETSI Type A spectrum mask .....                                                   | 262 |
| Figure 127—ETSI Type B spectrum mask .....                                                   | 262 |
| Figure 128—ETSI Type C spectrum mask .....                                                   | 263 |
| Figure 129—Illustration of EVM .....                                                         | 264 |
| Figure 130—Configuration file structure .....                                                | 266 |
| Figure 131—Create TLV entries for parameters required by the SS .....                        | 266 |
| Figure 132—Add SS MIC .....                                                                  | 267 |
| Figure 133—Add end of data marker .....                                                      | 267 |

## List of Tables

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Table 1—ATM CS PDU Header .....                                         | 12 |
| Table 2—MAC Header format .....                                         | 38 |
| Table 3—Generic MAC header fields .....                                 | 39 |
| Table 4—Downlink type encoding .....                                    | 39 |
| Table 5—Uplink type encoding .....                                      | 40 |
| Table 6—Bandwidth request header fields .....                           | 41 |
| Table 7—Fragmentation subheader format .....                            | 41 |
| Table 8—Fragmentation subheader fields .....                            | 42 |
| Table 9—Grant Management subheader format .....                         | 42 |
| Table 10—Grant Management subheader fields .....                        | 43 |
| Table 11—Packing subheader format .....                                 | 43 |
| Table 12—Packing subheader fields .....                                 | 43 |
| Table 13—MAC Management Messages .....                                  | 44 |
| Table 14—DCD message format .....                                       | 45 |
| Table 15—DL-MAP message format .....                                    | 47 |
| Table 16—UCD message format .....                                       | 48 |
| Table 17—UL-MAP message format .....                                    | 49 |
| Table 18—RNG-REQ message format .....                                   | 50 |
| Table 19—RNG-RSP message format .....                                   | 51 |
| Table 20—REG-REQ message format .....                                   | 52 |
| Table 21—REG-RSP message format .....                                   | 53 |
| Table 22—PKM MAC messages .....                                         | 54 |
| Table 23—PKM-REQ message format .....                                   | 54 |
| Table 24—PKM response (PKM-RSP) message format .....                    | 55 |
| Table 25—PKM message codes .....                                        | 56 |
| Table 26—SA Add attributes .....                                        | 56 |
| Table 27—Auth Request attributes .....                                  | 57 |
| Table 28—Auth Reply attributes .....                                    | 58 |
| Table 29—Auth Reject attributes .....                                   | 58 |
| Table 30—Key Request attributes .....                                   | 58 |
| Table 31—Key Reply attributes .....                                     | 59 |
| Table 32—Key Reject attributes .....                                    | 60 |
| Table 33—Authorization Invalid attributes .....                         | 60 |
| Table 34—TEK Invalid attributes .....                                   | 61 |
| Table 35—Authent Info attributes .....                                  | 61 |
| Table 36—DSA-REQ message format .....                                   | 62 |
| Table 37—DSA-RSP message format .....                                   | 63 |
| Table 38—DSA-ACK message format .....                                   | 64 |
| Table 39—DSC-REQ message format .....                                   | 65 |
| Table 40—Dynamic Service Change Response (DSC-RSP) message format ..... | 66 |
| Table 41—DSC-ACK message format .....                                   | 67 |
| Table 42—DSD-REQ message format .....                                   | 68 |
| Table 43—DSD-RSP message format .....                                   | 69 |
| Table 44—MCA-REQ message format .....                                   | 70 |
| Table 45—MCA-RSP message format .....                                   | 71 |
| Table 46—DBPC-REQ message format .....                                  | 71 |
| Table 47—DBPC-REQ message format .....                                  | 72 |
| Table 48—RES-CMD message format .....                                   | 72 |
| Table 49—SS SBC-REQ message format .....                                | 73 |
| Table 50—SS SBC-RSP message format .....                                | 74 |
| Table 51—CLK-CMP message format .....                                   | 75 |

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| Table 52—DREG-CMD) message format .....                                         | 76  |
| Table 53—Action Codes and Actions .....                                         | 76  |
| Table 54—DSX-RVD message format .....                                           | 77  |
| Table 55—TFTP-CPLT message format .....                                         | 77  |
| Table 56—Config File TFTP-RSP message format .....                              | 78  |
| Table 57—Fragmentation rules .....                                              | 80  |
| Table 58—Scheduling services and usage rules .....                              | 84  |
| Table 59—Sample uplink map with multicast and broadcast IE .....                | 91  |
| Table 60—Message flows during scanning and uplink parameter acquisition .....   | 106 |
| Table 61—Ranging and automatic adjustments procedure .....                      | 108 |
| Table 62—Establishing IP connectivity .....                                     | 114 |
| Table 63—Establishing time of day .....                                         | 114 |
| Table 64—UCD update .....                                                       | 121 |
| Table 65—DCD update .....                                                       | 122 |
| Table 66—DSA initiated from SS .....                                            | 144 |
| Table 67—DSA initiated from BS .....                                            | 145 |
| Table 68—SS-initiated DSC .....                                                 | 155 |
| Table 69—BS-initiated DSC .....                                                 | 156 |
| Table 70—DSD-initiated from SS .....                                            | 165 |
| Table 71—DSD-initiated from BS .....                                            | 165 |
| Table 72—Authorization FSM state transition matrix .....                        | 175 |
| Table 73—TEK FSM state transition matrix .....                                  | 182 |
| Table 74—Basic fields of an X.509 Version 3 certificate .....                   | 195 |
| Table 75—SCHED_PARAM_VECTOR for 10–66 GHz PHY .....                             | 214 |
| Table 76—DCD_PARAM_VECTOR for 10–66 GHz PHY .....                               | 214 |
| Table 77—UCD_PARAM_VEC for 10–66 GHz PHY .....                                  | 215 |
| Table 78—RNG_REQ_VECTOR for 10–66 GHz PHY .....                                 | 215 |
| Table 79—RNG_IND_VECTOR for 10–66 GHz PHY .....                                 | 215 |
| Table 80—TXVECTOR for 10–66 GHz PHY .....                                       | 216 |
| Table 81—TXSTATUS for 10–66 GHz PHY .....                                       | 216 |
| Table 82—RXVECTOR for 10–66 GHz PHY .....                                       | 216 |
| Table 83—RXSTATUS for 10–66 GHz PHY .....                                       | 217 |
| Table 84—Frame durations and frame duration codes .....                         | 217 |
| Table 85—PHY Type parameter encoding .....                                      | 218 |
| Table 86—Downlink burst preambles .....                                         | 221 |
| Table 87—Frame start preamble .....                                             | 222 |
| Table 88—Downlink TDMA burst preamble .....                                     | 222 |
| Table 89—DL_MAP_Information_Element .....                                       | 223 |
| Table 90—PHY synchronization field .....                                        | 223 |
| Table 91—Mapping of burst profile to DIUC .....                                 | 225 |
| Table 92—Downlink_Burst_Profile format .....                                    | 225 |
| Table 93—DIUC allocation .....                                                  | 230 |
| Table 94—FEC Code Types .....                                                   | 231 |
| Table 95—Parameters of the inner codes for the BCC .....                        | 233 |
| Table 96—Hamming code generator polynomials .....                               | 235 |
| Table 97—Original data for encoding .....                                       | 236 |
| Table 98—Encoded block .....                                                    | 237 |
| Table 99—Required block codes for the BTC option for the downlink channel ..... | 238 |
| Table 100—Parameters for burst profile (DIUC=0) .....                           | 239 |
| Table 101—QPSK bits to symbol mapping .....                                     | 241 |
| Table 102—16-QAM bits to symbol mapping .....                                   | 242 |
| Table 103—64-QAM bits to symbol mapping .....                                   | 243 |
| Table 104—Summary of downlink PHY Parameters .....                              | 246 |
| Table 105—16-symbol uplink preamble sequence .....                              | 247 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Table 106—32-symbol uplink preamble sequence .....                             | 248 |
| Table 107—UL_MAP_Information_Element .....                                     | 249 |
| Table 108—Uplink map IE.....                                                   | 249 |
| Table 109—Uplink_Burst_Profile format .....                                    | 251 |
| Table 110—Required block codes for the BTC option for the uplink channel ..... | 253 |
| Table 111—Summary of uplink PHY parameters .....                               | 255 |
| Table 112—Baud rates and channel sizes for a roll-off factor of 0.25 .....     | 255 |
| Table 113—Minimum BS transmitter performance .....                             | 257 |
| Table 114—Minimum SS transmitter performance .....                             | 258 |
| Table 115—Minimum SS receiver performance .....                                | 259 |
| Table 116—Propagation models .....                                             | 260 |
| Table 117—Configuration setting format in SS binary configuration file .....   | 265 |
| Table 118—Parameters and constants .....                                       | 268 |
| Table 119—Operational ranges for privacy configuration settings.....           | 271 |
| Table 120—Values for privacy configuration setting for protocol testing.....   | 271 |
| Table 121—CIDs .....                                                           | 272 |
| Table 122—UCD channel encodings .....                                          | 273 |
| Table 123—Uplink_Burst_Profile encodings .....                                 | 274 |
| Table 124—DCD channel encodings .....                                          | 275 |
| Table 125—Downlink_Burst_Profile encodings.....                                | 276 |
| Table 126—RNG-REQ message encodings.....                                       | 277 |
| Table 127—RNG-RSP message encodings.....                                       | 278 |
| Table 128—Multicast assignment request message encodings .....                 | 279 |
| Table 129—PKM attribute types .....                                            | 280 |
| Table 130—Attribute value data types .....                                     | 280 |
| Table 131—TEK-parameters subattributes .....                                   | 283 |
| Table 132—Error-code attribute code values .....                               | 284 |
| Table 133—Security-capabilities subattributes .....                            | 285 |
| Table 134—Data encryption algorithm identifiers .....                          | 286 |
| Table 135—Data authentication algorithm identifiers .....                      | 286 |
| Table 136—TEK encryption algorithm identifier .....                            | 286 |
| Table 137—Allowed cryptographic suites .....                                   | 286 |
| Table 138—Version attribute values .....                                       | 287 |
| Table 139—SA-descriptor subattributes .....                                    | 287 |
| Table 140—SA-type attribute values .....                                       | 288 |
| Table 141—Values used in Dynamic Service Messages.....                         | 301 |
| Table 142—HMAC Tuple definition .....                                          | 318 |
| Table 143—HMAC Tuple value field .....                                         | 318 |
| Table 144—Confirmation code .....                                              | 320 |

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

# **Part 16: Air Interface for Fixed Broadband Wireless Access Systems**

## **1. Overview**

### **1.1 Scope**

This standard specifies the air interface, including the medium access control layer (MAC) and physical layer (PHY), of fixed point-to-multipoint broadband wireless access (BWA) systems providing multiple services. The MAC is structured to support multiple PHY specifications, each suited to a particular operational environment.

For the purposes of this document, a “system” consists of an IEEE Std 802.16™-2001 MAC and PHY implementation with at least one subscriber station communicating with a base station via a point-to-multipoint air interface, along with the interfaces to external networks and services transported by the MAC and PHY.

### **1.2 Purpose**

This standard is intended to enable rapid worldwide deployment of innovative, cost-effective, and interoperable multivendor broadband wireless access products, to facilitate competition in broadband access by providing alternatives to wireline broadband access, to facilitate coexistence studies, to encourage consistent worldwide allocation, and to accelerate the commercialization of broadband wireless access spectrum.

The applications depend on the spectrum to be used. The primary bands of interest are as follows:

#### **1.2.1 10–66 GHz licensed bands**

The 10–66 GHz bands provide a physical environment where, due to the short wavelength, line of sight is required and multipath is negligible. The channels used in this physical environment are typically large. For example, channels 25 or 28 MHz wide are typical. With raw data rates in excess of 120 Mbit/s, this environment is well suited for point-to-multipoint access serving applications from small office/home office (SOHO) through medium to large office applications.

#### **1.2.2 2–11 GHz**

This work is in development under IEEE Standards Association Project P802.16a™.

### 1.3 Reference model

Figure 1 illustrates the reference model and scope of this standard.

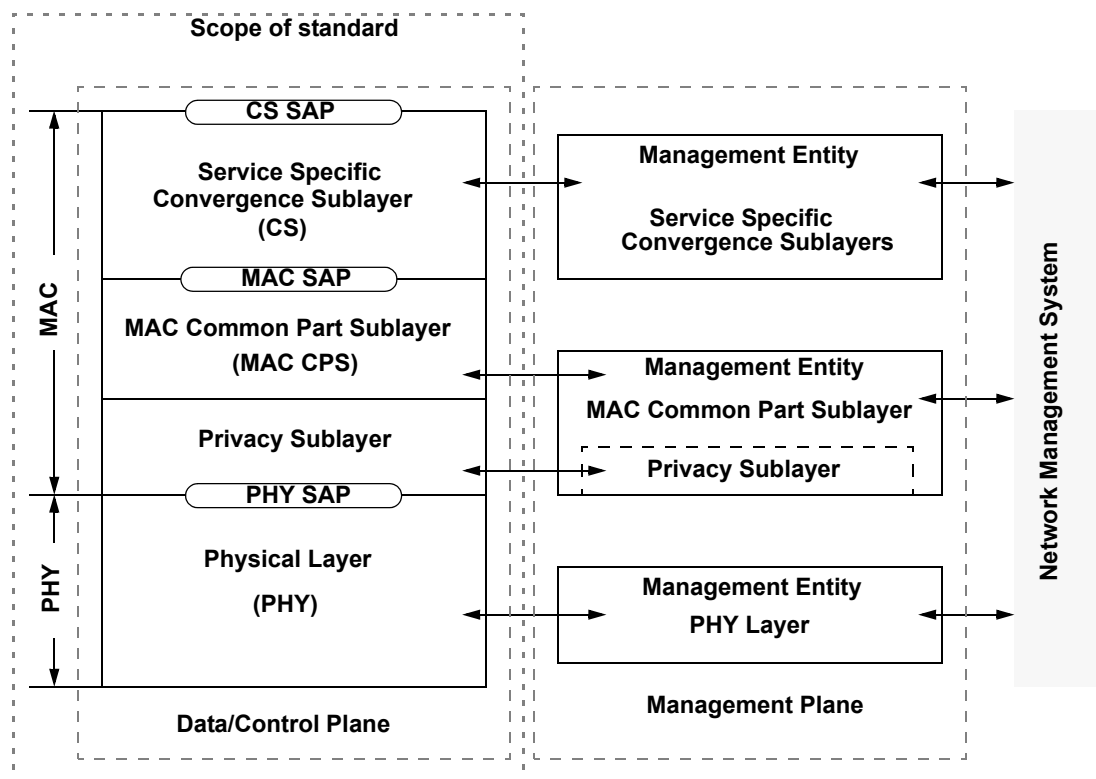


**Figure 1—IEEE Std 802.16-2001 protocol layering, showing service access points (SAPs)**

The MAC comprises three sublayers. The Service Specific Convergence Sublayer (CS) provides any transformation or mapping of external network data, received through the CS service access point (SAP), into MAC SDUs received by the MAC Common Part Sublayer (MAC CPS) through the MAC SAP. This includes classifying external network Service Data Units (SDUs) and associating them to the proper MAC service flow and Connection Identifier (CID). It may also include such functions as payload header suppression. Multiple CS specifications are provided for interfacing with various protocols. The internal format of the CS payload is unique to the CS, and the MAC CPS is not required to understand the format of or parse any information from the CS payload.

The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. It receives data from the various CSs, through the MAC SAP, classified to particular MAC connections. Quality of Service (QoS) is applied to the transmission and scheduling of data over the PHY.

The MAC also contains a separate Privacy Sublayer providing authentication, secure key exchange, and encryption.

Data, PHY control, and statistics are transferred between the MAC CPS and the PHY via the PHY SAP.

The PHY may include multiple specifications, each appropriate to a particular frequency range and application. The various physical layer specifications supported are discussed in Clause 8.

## 2. References

This standard shall be used in conjunction with the following publications. When the following specifications are superseded by an approved revision, the revision shall apply.

ATM Forum Specification af-uni-0010.002, ATM User-Network Interface Specification, Version 3.1, September 1994.<sup>1</sup>

ATM Forum Specification af-sig-0061.000, ATM User-Network Interface (UNI) Signalling Specification, Version 4.0, July 1996.

ETSI EN 301 213-3, Fixed Radio Systems; Point-to-multipoint equipment; Point-to-multipoint digital radio systems in frequency bands in the range 24,25 GHz to 29,5 GHz using different access methods; Part 3: Time Division Multiple Access (TDMA) methods, Version 1.3.1, September 2001.<sup>2</sup>

FIPS 46-3, Data Encryption Standard (DES), October, 1999.<sup>3</sup>

FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, April 1981.

FIPS 81, DES Modes of Operation, December 1980.

FIPS 180-1, Secure Hash Standard (SHS), April 1995.

FIPS 186-2, Digital Signature Standard (DSS), January 2000.

IEEE Std 802<sup>®</sup>-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.<sup>4, 5</sup>

IEEE Std 802.1D<sup>™</sup>-1998, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges.<sup>6</sup>

IEEE Std 802.1Q<sup>™</sup>-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.2<sup>™</sup>-1998 (ISO/IEC 8802-2: 1998), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical Link Control.

IEEE Std 802.3<sup>™</sup>-2000 (ISO 8802-3), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

<sup>1</sup>ATM Forum publications are available from the ATM Forum at <http://www.atmforum.com/>.

<sup>2</sup>ETSI publications are available from the European Telecommunications Standards Institute at <http://www.etsi.org/>.

<sup>3</sup>FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Road, Springfield, VA 22161 (<http://www.ntis.gov/>).

<sup>4</sup>IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

<sup>5</sup>IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://standards.ieee.org/>).

<sup>6</sup>IEEE standards referred to in Clause 2 are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

IEEE Std 802.16.2™-2001, IEEE Recommended Practice for Local and metropolitan area networks—Coexistence of Fixed Broadband Wireless Access Systems.

IETF RFC 791, “Internet Protocol,” J. Postel, September 1981.<sup>7</sup>

IETF RFC 868, “Time Protocol,” J. Postel, K. Harrenstien, May 1983.

IETF RFC 1042, “A Standard for the Transmission of IP Datagrams over IEEE 802 Networks,” J. Postel, J. Reynolds, February 1988.

IETF RFC 1123, “Requirements for Internet Hosts—Application and Support,” R. Braden, October 1989.

IETF RFC 1157, “A Simple Network Management Protocol (SNMP),” M. Schoffstall, M. Fedor, J. Davin, and J. Case, May 1990.

IETF RFC 2104, “HMAC: Keyed-Hashing for Message Authentication,” H. Krawczyk, M. Bellare, R. Canetti, February 1997.

IETF RFC 2131, “Dynamic Host Configuration Protocol,” R. Droms, March 1997.

IETF RFC 2132, “DHCP Options and BOOTP Vendor Extensions,” S. Alexander, and R. Droms, March 1997.

IETF RFC 2349, “TFTP Timeout Interval and Transfer Size Options,” G. Malkin and A. Harkin, May 1998.

IETF RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” R. Housley, W. Ford, W. Polk, D. Solo, January 1999.

IETF RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification,” S. Deering, R. Hinden, December 1998.

IETF RFC 2474, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” K. Nichols, S. Blake, F. Baker, D. Black, December 1998.

Internet Assigned Numbers Authority (IANA), “Protocol Numbers,” <<http://www.iana.org/assignments/protocol-numbers>>, June 2001.

ISO/IEC 8825, Information technology—Open Systems Interconnection—Specification of the Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), May 1999.<sup>8</sup>

ITU-T Recommendation X.690, Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER), December 1997.<sup>9</sup>

PKCS #1 v2.0, RSA Cryptography Standard, RSA Laboratories, October 1998 <<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1>>.

<sup>7</sup>IETF publications are available from the Internet Engineering Task Force at <http://www.ietf.org/>.

<sup>8</sup>ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Geneva 20, Switzerland/Suisse or the IEC Sales Department, Case Postale 131, 3, rue de Varembe, CH-1211, Geneva 20, Switzerland/Suisse. They are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42<sup>nd</sup> Street, 13<sup>th</sup> floor, New York, NY 10036, USA.

<sup>9</sup>ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (<http://www.itu.int/>).

### 3. Definitions

For the purposes of this standard, the following terms and definitions apply. The *IEEE 100, The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B4]<sup>10</sup>, should be referenced for terms not defined in this clause.

**3.1 bandwidth stealing:** The use, by a subscriber station operating on a *grant per subscriber station* basis, of a portion of the bandwidth allocated in response to a bandwidth request for a connection to send another bandwidth request rather than sending data. *See also: grant per subscriber station.*

**3.2 base station (BS):** A generalized equipment set providing connectivity, management, and control of the subscriber station.

**3.3 Basic Connection:** Connection that is established during initial subscriber station registration and that which is used to transport delay-intolerant MAC management messages.

**3.4 broadband:** Having instantaneous bandwidths greater than around 1 MHz and supporting data rates greater than about 1.5 Mbit/s.

**3.5 broadband wireless access (BWA):** Wireless access in which the connection(s) capabilities are broadband.

**3.6 burst profile:** Set of parameters that describe the uplink or downlink transmission properties associated with an interval usage code. Each profile contains parameters such as modulation type, forward error correction type, preamble length, guard times, etc. *See also: interval usage code.*

**3.7 byte:** Throughout this standard, one byte is 8 bits.

**3.8 Channel Identifier (ChID):** An identifier used to distinguish between multiple uplink channels, all of which are associated with the same downlink channel.

**3.9 concatenation:** The act of combining multiple medium access control (MAC) protocol data units (PDUs) into a single time division multiplex (TDM) or time division multiple access (TDMA) burst.

**3.10 connection:** A unidirectional mapping between base station and subscriber station medium access control (MAC) peers for the purpose of transporting a service flow's traffic. Connections are identified by a connection identifier (CID). All traffic is carried on a connection, even for service flows that implement connectionless protocols, such as internet protocol (IP). *See also: connection identifier.*

**3.11 Connection Identifier (CID):** A unidirectional, medium access control layer address that identifies a connection to equivalent peers in the medium access control layer of the base station and subscriber station. It maps to a *service flow identifier* (SFID), which defines the quality of service (QoS) parameters of the service flow associated with that connection. Security associations also exist between keying material and CIDs. *See also: service flow identifier.*

**3.12 downlink:** The direction from the base station to the subscriber station.

**3.13 Downlink Channel Descriptor (DCD):** A medium access control layer message that describes the physical layer characteristics of a downlink channel.

**3.14 Downlink Interval Usage Code (DIUC):** An interval usage code (IUC) specific to a downlink. *See also: interval usage code.*

<sup>10</sup>The numbers in brackets correspond to those of the bibliography in Annex A.

**3.15 downlink map (DL-MAP):** A medium access control layer message that defines burst start times for both time division multiplex and time division multiple access by a subscriber station on the downlink.

**3.16 dynamic service:** The set of messages and protocols that allow the base station and subscriber station to add, modify, or delete the characteristics of a service flow.

**3.17 fixed wireless access:** Wireless access application in which the location of the base station and subscriber station are fixed in location during operation.

**3.18 frame:** A structured data sequence of fixed duration used by some physical layer specifications. A frame may contain both an uplink subframe and a downlink subframe.

**3.19 frequency division duplex (FDD):** A duplex scheme in which uplink and downlink transmissions use different frequencies but are typically simultaneous.

**3.20 grant per connection (GPC):** A bandwidth allocation method in which grants are allocated to a specific connection within a subscriber station. Note that bandwidth requests are always made for a connection.

**3.21 grant per subscriber station (GPSS):** A bandwidth allocation method in which grants are aggregated for all connections within a subscriber station and are allocated to the subscriber station as that aggregate. Note that bandwidth requests are always made for a connection.

**3.22 information element (IE):** A component of the downlink or uplink map that defines the starting address associated with an interval usage code (IUC). *See also:* **interval usage code**.

**3.23 Initial Ranging Connection Identifier:** A well-defined connection identifier that is used by a subscriber station during the initial ranging process. This Connection Identifier (CID) is defined as constant value within the protocol since a subscriber station has no addressing information available until the initial ranging process is complete.

**3.24 Interval Usage Code (IUC):** A code identifying a particular burst profile that can be used by a downlink or uplink transmission interval.

**3.25 management connection:** A connection that is established during initial subscriber station registration that is used to transport delay-tolerant medium access control management messages.

**3.26 minislot:** A unit of uplink bandwidth allocation equivalent to  $n$  physical slots, where  $n = 2^m$  and  $m$  is an integer ranging from 0 through 7.

**3.27 multicast polling group:** A group of zero or more subscriber stations that are assigned a multicast address for the purposes of polling.

**3.28 packing:** The act of combining multiple service data units from a higher layer into a single medium access control protocol data unit.

**3.29 payload header suppression (PHS):** The process of suppressing the repetitive portion of payload headers at the sender and restoring the headers at the receiver.

**3.30 Payload Header Suppression Field (PHSF):** A string of bytes representing the header portion of a protocol data unit in which one or more bytes are to be suppressed (i.e., a snapshot of the uncompressed protocol data unit header inclusive of suppressed and unsuppressed bytes).

**3.31 Payload Header Suppression Index (PHSI):** An 8-bit mask that indicates which bytes in the payload header suppression field to suppress and which bytes to not suppress.

**3.32 Payload Header Suppression Size (PHSS):** The length of the suppressed field in bytes. This value is equivalent to the number of bytes in the payload header suppression field and also the number of valid bits in the payload header suppression mask.

**3.33 Payload Header Suppression Valid (PHSV):** A flag that tells the sending entity to verify all bytes that are to be suppressed.

**3.34 physical slot (PS):** A unit of time, dependent on the physical layer specification, for allocating bandwidth

**3.35 privacy key management protocol (PKM):** A client/server model between the base station and subscriber station that is used to secure distribution of keying material.

**3.36 protocol data unit (PDU):** The data unit exchanged between peer entities of the same protocol layer. On the downward direction, it is the data unit generated for the next lower layer. On the upward direction, it is the data unit received from the previous lower layer (see Figure 2).

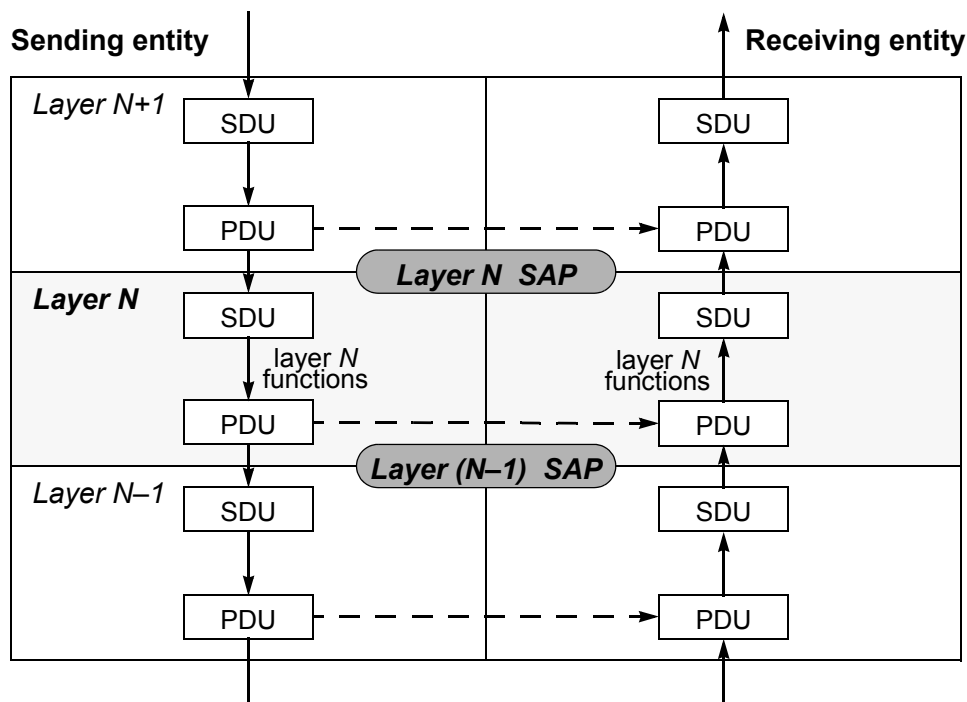


Figure 2—PDU and SDU in a protocol stack

**3.37 security association (SA):** The set of security information a base station and one or more of its client subscriber stations share in order to support secure communications. This shared information includes traffic encryption keys and cipher block chaining initialization vectors.

**3.38 Security Association Identifier (SAID):** An identifier shared between the base station and subscriber station that uniquely identifies a security association.

**3.39 service access point (SAP):** The point in a protocol stack where the services of a lower layer are available to its next higher layer.

**3.40 service data unit (SDU):** The data unit exchanged between two adjacent protocol layers. On the downward direction, it is the data unit received from the previous higher layer. On the upward direction, it is the data unit sent to the next higher layer (see Figure 2).

**3.41 service flow (SF):** A unidirectional flow of medium access control service data units on a connection that is provided a particular quality of service.

**3.42 service flow class:** A grouping of service flow properties to allow higher layer entities and external applications to request service flows with desired quality of service (QoS) parameters in a globally consistent way.

**3.43 Service Flow Identifier (SFID):** A 32-bit quantity that uniquely identifies a service flow to both the subscriber station and base station.

**3.44 service flow name:** An ASCII string that is used to reference a set of quality of service (QoS) parameters that (partially) define a service flow.

**3.45 subscriber station (SS):** A generalized equipment set providing connectivity between subscriber equipment and a base station.

**3.46 time division duplex (TDD):** A duplex scheme where uplink and downlink transmissions occur at different times but may share the same frequency.

**3.47 time division multiple access (TDMA) burst:** A contiguous portion of the uplink or downlink using physical layer parameters, determined by the downlink or uplink interval usage code, that remain constant for the duration of the burst. TDMA bursts are separated by preambles and are separated by gaps in transmission if subsequent bursts are from different transmitters.

**3.48 time division multiplex (TDM) burst:** A contiguous portion of a time division multiplex (TDM) data stream using physical layer parameters, determined by the downlink interval usage code, that remain constant for the duration of the burst. TDM bursts are not separated by gaps or preambles.

**3.49 Transport Connection Identifier:** A unique identifier taken from the connection identifier address space that uniquely identifies the transport connection.

**3.50 transport connection:** A connection used to transport user data.

**3.51 type/length/value (TLV):** A formatting scheme that adds a tag to each transmitted parameter containing the parameter type (and implicitly its encoding rules) and the length of the encoded parameter.

**3.52 uplink:** The direction from a subscriber station to the base station.

**3.53 Uplink Channel Descriptor (UCD):** A medium access control message that describes the physical layer characteristics of an uplink.

**3.54 Uplink Interval Usage Code (UIUC):** An interval usage code specific to an uplink.

**3.55 uplink map (UL-MAP):** A set of information that defines the entire access for a scheduling interval.

**3.56 wireless access:** End-user radio connection(s) to core networks.

## 4. Abbreviations and acronyms

|       |                                  |
|-------|----------------------------------|
| 3-DES | triple data encryption standard  |
| AK    | authorization key                |
| ARP   | address resolution protocol      |
| ARQ   | automatic repeat request         |
| ATDD  | adaptive time division duplexing |
| ATM   | asynchronous transfer mode       |

|         |                                                                      |
|---------|----------------------------------------------------------------------|
| BCC     | block convolutional code                                             |
| BE      | best effort                                                          |
| BNI     | base station network interface                                       |
| BR      | bandwidth request                                                    |
| BS      | base station                                                         |
| BTC     | block turbo code                                                     |
| BWA     | broadband wireless access                                            |
| C/(I+N) | carrier-to/(interference plus noise) ratio                           |
| C/I     | carrier-to-interference ratio                                        |
| C/N     | carrier-to-noise ratio                                               |
| CA      | certification authority                                              |
| CBC     | cipher block chaining                                                |
| CC      | confirmation code                                                    |
| CCS     | common channel signaling                                             |
| CCV     | clock comparison value                                               |
| CEPT    | European Conference of Postal and Telecommunications Administrations |
| CG      | continuous grant                                                     |
| ChID    | Channel Identifier                                                   |
| CID     | Connection Identifier                                                |
| CLP     | Cell Loss Priority                                                   |
| CPS     | common part sublayer                                                 |
| CRC     | cyclic redundancy check                                              |
| CS      | convergence sublayer                                                 |
| DAMA    | demand assigned multiple access                                      |
| DCD     | Downlink Channel Descriptor                                          |
| DES     | data encryption standard                                             |
| DHCP    | dynamic host configuration protocol                                  |
| DIUC    | Downlink Interval Usage Code                                         |
| DL      | downlink                                                             |
| DSA     | dynamic service addition                                             |
| DSC     | dynamic service change                                               |
| DSCP    | differentiated services codepoint                                    |
| DSD     | dynamic service deletion                                             |
| DSx     | dynamic service addition, change, or deletion                        |
| EC      | encryption control                                                   |
| ECB     | electronic code book                                                 |
| EDE     | encrypt-decrypt-encrypt                                              |
| EIRP    | effective isotropic radiated power                                   |
| EKS     | encryption key sequence                                              |
| ETSI    | European Telecommunications Standards Institute                      |
| EUI     | extended unique identifier                                           |
| EVM     | error vector magnitude                                               |
| FC      | fragmentation control                                                |
| FDD     | frequency division duplex                                            |
| FEC     | forward error correction                                             |
| FIPS    | Federal Information Processing Standard                              |
| FSH     | fragmentation subheader                                              |
| FSN     | fragment sequence number                                             |
| GF      | Galois field                                                         |
| GM      | grant management                                                     |
| GPC     | grant per connection                                                 |
| GPSS    | grant per subscriber station                                         |
| HCS     | header check sequence                                                |
| HEC     | header error check                                                   |

|       |                                                          |
|-------|----------------------------------------------------------|
| HMAC  | Hashed Message Authentication Code                       |
| HT    | header type                                              |
| IANA  | Internet Assigned Numbers Authority                      |
| IE    | information element                                      |
| IETF  | Internet Engineering Task Force                          |
| IGMP  | Internet Group Management Protocol                       |
| IP    | Internet Protocol                                        |
| ITU   | International Telecommunications Union                   |
| IUC   | Interval Usage Code                                      |
| IWF   | interworking function                                    |
| KEK   | key encryption key                                       |
| LAN   | local area network                                       |
| LFSR  | linear feedback shift registers                          |
| LLC   | logical link control                                     |
| LMDS  | local multipoint distribution service                    |
| lsb   | least significant bit                                    |
| LSB   | least significant byte                                   |
| MAC   | medium access control layer                              |
| MAN   | metropolitan area network                                |
| MIB   | management information base                              |
| MIC   | message integrity check                                  |
| MMDS  | multichannel multipoint distribution service             |
| MPEG  | Moving Pictures Experts Group                            |
| MPLS  | multiprotocol label switching                            |
| msb   | most significant bit                                     |
| MSB   | most significant byte                                    |
| NNI   | network-to-network interface (or network node interface) |
| nrtPS | non-real-time polling service                            |
| OID   | object identifier                                        |
| PBR   | piggyback request                                        |
| PDH   | plesiochronous digital hierarchy                         |
| PDU   | protocol data unit                                       |
| PHS   | Payload Header Suppression                               |
| PHSF  | Payload Header Suppression Field                         |
| PHSI  | Payload Header Suppression Index                         |
| PHSM  | Payload Header Suppression Mask                          |
| PHSS  | Payload Header Suppression Size                          |
| PHSV  | Payload Header Suppression Valid                         |
| PHY   | physical layer                                           |
| PKM   | privacy key management                                   |
| PM    | poll-me bit                                              |
| PMD   | physical medium dependent                                |
| ppm   | parts per million                                        |
| PPP   | Point-to-Point Protocol                                  |
| PS    | physical slot                                            |
| PSH   | Packing Subheader                                        |
| PTI   | Payload Type Indicator                                   |
| PVC   | Permanent Virtual Circuit                                |
| QAM   | quadrature amplitude modulation                          |
| QoS   | Quality of Service                                       |
| QPSK  | quadrature phase-shift keying                            |
| RS    | Reed–Solomon                                             |
| RSSI  | receive signal strength indicator                        |
| rtPS  | real-time polling service                                |

|      |                                               |
|------|-----------------------------------------------|
| Rx   | reception                                     |
| SA   | security association                          |
| SAID | security association identifier               |
| SAP  | service access point                          |
| SCTE | Society of Cable Telecommunications Engineers |
| SDH  | Synchronous Digital Hierarchy                 |
| SDU  | service data unit                             |
| SF   | service flow                                  |
| SFID | Service Flow Identifier                       |
| SHA  | secure hash algorithm                         |
| SI   | slip indicator                                |
| SNMP | Simple Network Management Protocol            |
| SS   | subscriber station                            |
| SVC  | Switched Virtual Circuit                      |
| TC   | transmission convergence sublayer             |
| TCP  | Transmission Control Protocol                 |
| TDD  | time division duplex                          |
| TDM  | time division multiplex                       |
| TDMA | time division multiple access                 |
| TEK  | traffic encryption key                        |
| TFTP | Trivial File Transfer Protocol                |
| TLV  | type-length-value                             |
| Tx   | transmission                                  |
| UCD  | Uplink Channel Descriptor                     |
| UDP  | User Datagram Protocol                        |
| UGS  | unsolicited grant service                     |
| UIUC | Uplink Interval Usage Code                    |
| UL   | uplink                                        |
| UNI  | user-to-network interface                     |
| UTC  | Coordinated Universal Time                    |
| VC   | virtual channel                               |
| VCI  | virtual channel identifier                    |
| VLAN | virtual local area network                    |
| VP   | virtual path                                  |
| VPI  | Virtual Path Identifier                       |
| XOR  | exclusive or                                  |

## 5. Service specific convergence sublayer

The service specific convergence sublayer (CS) resides on top of the MAC CPS and utilizes, via the MAC SAP, the services provided by the MAC CPS (see Figure 1). The CS performs the following functions:

- accepting higher-layer PDUs from the higher layer
- performing classification of higher-layer PDUs
- processing (if required) the higher-layer PDUs based on the classification
- delivering CS PDUs to the appropriate MAC SAP
- receiving CS PDUs from the peer entity

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

5.1 ATM convergence sublayer

The ATM CS is a logical interface that associates different ATM services with the MAC CPS SAP. The ATM CS accepts ATM cells from the ATM layer, performs *classification* and, if provisioned, *payload header suppression* (PHS), and delivers CS PDUs to the appropriate MAC SAP.

5.1.1 Convergence sublayer service definition

The ATM CS is specifically defined to support the convergence of PDUs generated by the ATM layer protocol of an ATM network. Since ATM cell streams are generated according to the ATM standards, no ATM CS service primitive is required.

5.1.2 Data/Control plane

5.1.2.1 PDU formats

The ATM CS PDU shall consist of an ATM CS PDU Header, defined in Table 1, and the ATM CS PDU payload. The ATM CS PDU payload shall be equal to the ATM cell payload. The ATM CS PDU is illustrated in Figure 3.

Table 1—ATM CS PDU Header

| Syntax                  | Size    | Notes                    |
|-------------------------|---------|--------------------------|
| ATM_CS_PDU_Header () {  |         |                          |
| if (no PHS) {           |         |                          |
| <b>ATM_Header</b>       | 40 bits | The full ATM cell header |
| }                       |         |                          |
| else if (VP switched) { |         |                          |
| <b>PTI</b>              | 3 bits  | From the ATM cell header |
| <b>CLP</b>              | 1 bit   | From the ATM cell header |
| <i>reserved</i>         | 4 bits  |                          |
| <b>VCI</b>              | 16 bits | From the ATM cell header |
| }                       |         |                          |
| else (VC switched) {    |         |                          |
| <b>PTI</b>              | 3 bits  | From the ATM cell header |
| <b>CLP</b>              | 1 bit   | From the ATM cell header |
| <i>reserved</i>         | 4 bits  |                          |
| }                       |         |                          |
| }                       |         |                          |



Figure 3—ATM CS PDU format

### 5.1.2.2 Classification

An ATM connection, which is uniquely identified by a pair of values of Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI), is either Virtual Path (VP) switched or Virtual Channel (VC) switched. In VP-switched mode, all VCIs within one single incoming VPI are automatically mapped to that of an outgoing VPI. In VC-switched mode, input VPI/VCI values are individually mapped to output VPI/VCI values. Thus, when performing PHS, the ATM CS differentiates these two types of connections and performs the suppression accordingly.

A classifier is a set of matching criteria applied to each ATM cell entering the ATM CS. It consists of some ATM cell matching criteria, such as VPI and VCI, and a reference to a CID. If an ATM cell matches the specified matching criteria, it is delivered to the MAC SAP for delivery on the connection identified by the CID.

#### 5.1.2.2.1 VP-switched mode

For VP-switched mode, the VPI field, 12 bits for a network-to-network interface (NNI) and 8 bits for a user-to-network interface (UNI), is mapped to the 16-bit CID for the MAC connection on which it is transported. Since the QoS and category of service parameters for the connection are set at connection establishment, this mapping of VPI to CID guarantees the correct handling of the traffic by the MAC sublayer.

#### 5.1.2.2.2 VC-switched mode

For VC switched mode, the VPI and VCI fields, 28 bits total for an NNI and 24 bits total for a UNI, are mapped to the 16-bit CID for the MAC connection on which it is transported. Since the QoS and category of service parameters for the connection are set at connection establishment, this mapping of VPI and VCI to CID guarantees the correct handling of the traffic by the MAC sublayer. Note that the full range of VPI/VCI combinations (up to  $2^{28}$  for NNI and  $2^{24}$  for UNI) cannot be simultaneously supported in this mode.

### 5.1.2.3 Payload header suppression

In payload header suppression (PHS), a repetitive portion of the payload headers of the CS SDUs is suppressed by the sending entity and restored by the receiving entity. On the downlink, the sending entity is the ATM CS on the base station (BS) and the receiving entity is the ATM CS on the SS. On the uplink, the sending entity is the ATM CS on the SS, and the receiving entity is the ATM CS on the BS. To further save bandwidth, multiple ATM cells (with or without PHS) that share the same CID may be packed and carried by a single MAC CPS PDU. Note that when PHS is turned off, no part of any ATM cell header including Header Error Check (HEC) field shall be suppressed. This provides an option for protecting the integrity of the cell header. Whether or not PHS is applied to an ATM connection is signaled in the DSA-REQ message at the connection's creation. Similarly, the VPI (for VP-switched connections) or the VPI/VCI (for VC-switched connections) is also signaled in the classifier settings of the DSA-REQ message at connection creation.

#### 5.1.2.3.1 PHS for VP-switched ATM connections

In VP switched mode, the VPI is mapped to a CID. This allows the disposal of the remainder of the ATM cell header except for the VCI, payload type indicator (PTI), and cell loss priority (CLP) fields. These fields shall be encapsulated in the CS PDU header.

Figure 4 shows a CS PDU containing a single VP-switched ATM cell with the cell header suppressed and the format of the ATM CS PDU Header for VP-switched ATM connections.

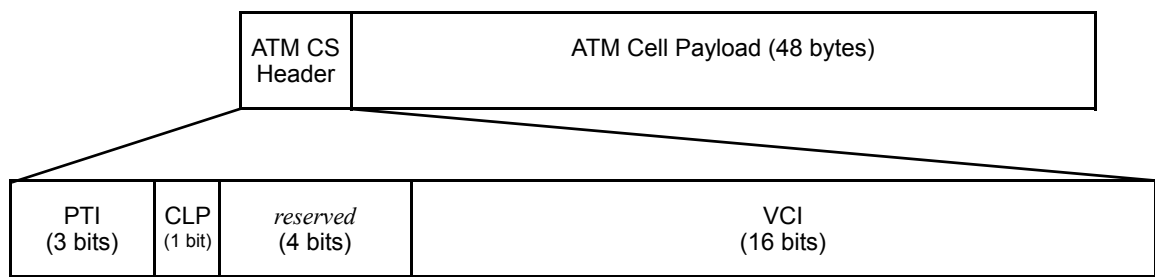


Figure 4—CS PDU format for VP-switched ATM connections

5.1.2.3.2 PHS for VC-switched ATM connections

In VC-switched mode, the VPI/VCI combination is mapped to a CID. This allows the disposal of the remainder of the ATM cell header except for the PTI and CLP fields. These fields shall be encapsulated in the CS PDU Header.

Figure 5 shows a CS PDU containing a single VC-switched ATM cell with the cell header suppressed and the format of the ATM CS PDU header for VC-switched ATM connections.

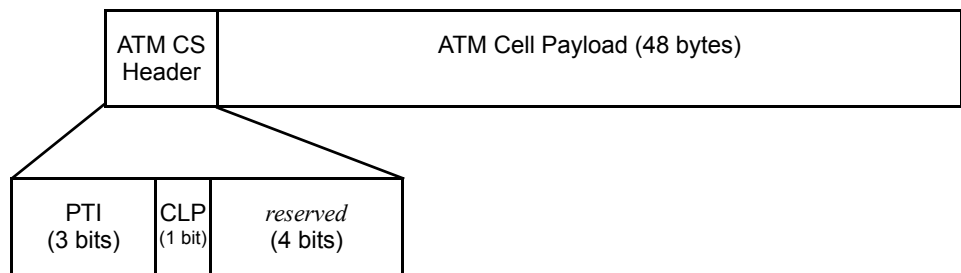


Figure 5—CS PDU format for VC-switched ATM connections

5.1.2.4 Signaling procedure

ATM interfaces support three types of connections, switched virtual circuit (SVC), permanent virtual circuit (PVC), and soft permanent virtual circuit (soft PVC). SVCs are established and terminated dynamically on demand by the use of signaling. The word “permanent” signifies that the circuit is established administratively. Although both PVC and soft PVC are established administratively, PVCs are established by provisioning process, and soft PVCs are established by the use of signaling.

ATM networks use common channel signaling (CCS), where signaling messages are carried over a connection completely independent of user connections and where one signaling channel can carry signaling messages for a number of user connections. Per nonassociated signaling (ATM as-sig-0061.000), by default, the signaling channel on VPI=0 controls all VPs on the same physical interface. In other words, except when the optional proxy signaling capability (Annex 2 of ATM as-sig-0061.000) or when the optional Virtual UNI capability (Annex 8 of ATM as-sig-0061.000) is used, the signaling channel is identified by VPI=0 and VCI=5. Note that this specification does not support associated signaling (ATM af-uni-0010.002), where VCI=5 of each VP is used as the signaling channel for all VCs on the same VP. In addition, this specification does not support either proxy signaling or virtual UNI.

To establish an SVC, it is the responsibility of the calling party to initiate the signaling procedure by issuing the appropriate signaling messages. Either end can establish or release the SVC. Details on how to use these

signaling messages are available in ATM as-sig-0061.000. It shall be the responsibility of the implementation of the BS to map ATM signaling messages to corresponding MAC CPS service primitives.

To establish a soft PVC, the network management system provisions one end of the soft PVC with the address identifying the egress ATM interface of the ATM network. The calling end has the responsibility for establishing and releasing the connection. It is also the responsibility of the calling party (if necessary) to reestablish the connection in case of switching system or link failure. It shall be the responsibility of the implementation of the BS to map ATM signaling messages to corresponding MAC CPS service primitives.

On the downlink direction, the signaling starts at an “end user” of the ATM backhaul network that implements an ATM UNI and terminates at the BS that shall implement either an ATM UNI or an ATM NNI. The signaling may be mapped by an interworking function (IWF) and extended to some user network on the SS-side. On the uplink direction, the signaling starts at the ATM interface of the BS and ends at the ATM UNI of an “end user.” In addition, the signaling may be originated by an “end user” of some user network and mapped by the IWF. Note that mapping of data units carried by the air link shall be limited to only cell-level convergence (5.1.2.2). If required by a user network, other levels of mappings (e.g., the convergence of, say, an Ethernet packet to ATM cells) shall be handled by the user network’s IWF exclusively.

During the provisioning process, each SS joining the IEEE Std 802.16-2001 system shall request a dedicated CID as the signaling connection corresponding to the CCS connection used by ATM networks. Any CID provisioned for this purpose shall not be dynamically changed or terminated. Each IEEE Std 802.16-2001 system shall provision a set of CIDs for this purpose.

## 5.2 Packet convergence sublayer

The packet CS resides on top of the IEEE Std 802.16-2001 MAC CPS layer. The CS performs the following functions, utilizing the services of the MAC sublayer:

- a) Classification of the higher-layer protocol PDU into the appropriate connection
- b) Suppression of payload header information (optional)
- c) Delivery of the resulting CS PDU to the MAC SAP associated with the service flow for transport to the peer MAC SAP
- d) Receipt of the CS PDU from the peer MAC SAP
- e) Rebuilding of any suppressed payload header information (optional)

The sending CS is responsible for delivering the MAC SDU to the MAC SAP. The MAC is responsible for delivery of the MAC SDU to peer MAC SAP in accordance with the QoS, fragmentation, concatenation and other transport functions associated with a particular connection’s service flow characteristics. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity.

The packet CS is used for transport for all packet-based protocols such as internet protocol (IP), point-to-point protocol (PPP), and IEEE Std 802.3 (Ethernet).

### 5.2.1 MAC SDU format

Higher-layer PDUs shall be encapsulated in the MAC SDU format as illustrated in Figure 6. For some payload protocols, each payload consists of an 8-bit payload header suppression index (PHSI) field followed by the actual payload. Other protocols map the higher layer PDU directly to the MAC SDU. A value of zero in the PHSI indicates no payload header suppression has been applied to the PDU. Otherwise, the value in

the index identifies the rules for suppression. This index is mapped to equivalent rules at BS and SS peers to allow for reconstruction of suppressed information.

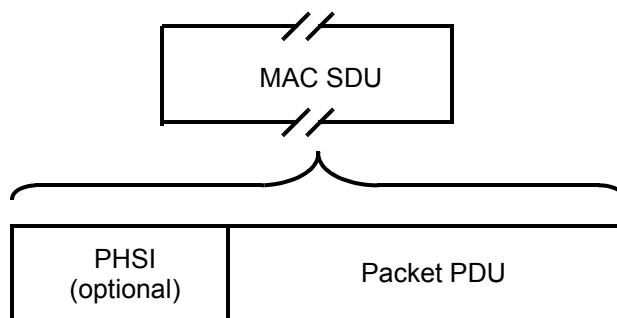


**Figure 6—MAC SDU Format**

### 5.2.2 Classification

Classification is the process by which a MAC SDU is mapped onto a particular connection for transmission between MAC peers. The mapping process associates a MAC SDU with a connection, which also creates an association with the service flow characteristics of that connection. This process facilitates the delivery of MAC SDUs with the appropriate QoS constraints.

A classifier is a set of matching criteria applied to each packet entering the IEEE Std 802.16-2001 network. It consists of some protocol-specific packet matching criteria (destination IP address, for example), a classifier priority, and a reference to a CID. If a packet matches the specified packet matching criteria, it is then delivered to the SAP for delivery on the connection defined by the CID. The service flow characteristics of the connection provide the QoS for that packet.

Several classifiers may each refer to the same service flow. The classifier priority is used for ordering the application of classifiers to packets. Explicit ordering is necessary because the patterns used by classifiers may overlap. The priority need not be unique, but care shall be taken within a classifier priority to prevent ambiguity in classification. Downlink classifiers are applied by the BS to packets it is transmitting and uplink classifiers are applied at the SS. Figure 7 and Figure 8 illustrate the mappings discussed above.

It is possible for a packet to fail to match the set of defined classifiers. In this case, the CS may either associate the packet with a default CID or discard the packet. The action taken is vendor specific.

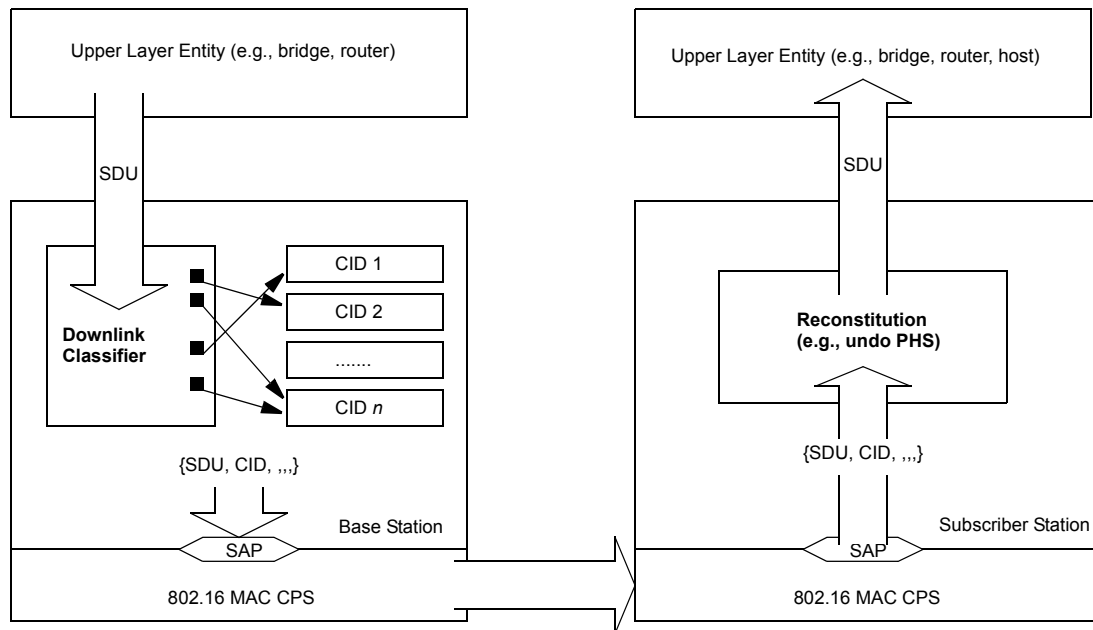


Figure 7—Classification and CID mapping (BS to SS)

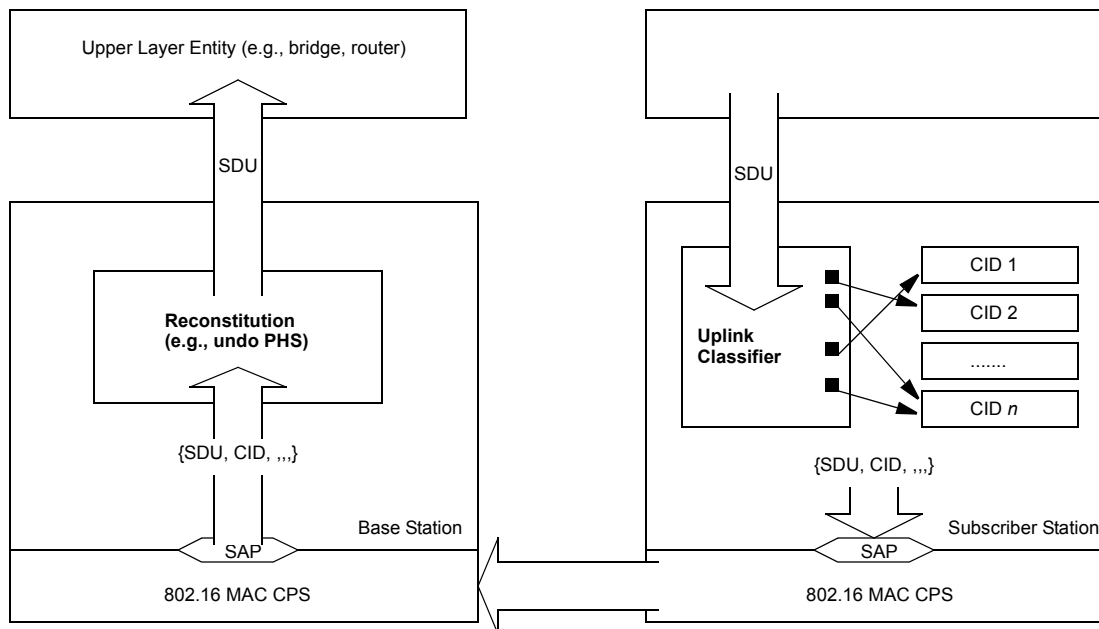


Figure 8—Classification and CID mapping (SS to BS)

### 5.2.3 Classification within the CS

SS and BS packet classification consists of multiple classifiers. Each classifier contains a priority field which determines the search order for the classifier. The highest priority classifier shall be applied first. If a classifier is found in which all parameters match the packet, the classifier shall forward the packet to the

corresponding connection(s). If no classifier is found in which all parameters match the packet then the packet is delivered under vendor or operator specific conditions. Two actions may be performed: the packet may be delivered using a “default” connection, or the packet may be discarded.

Classifiers can be added to the table either via network management operations or via dynamic operations (dynamic signaling, IEEE Std 802.16-2001 MAC sublayer service interface). Simple Network Management Protocol (SNMP)-based operations can view classifiers that are added via dynamic operations, but they shall not modify or delete classifiers that are created by dynamic operations. The format for classification table parameters defined in the configuration file or dynamic signaling message is contained in 11.4.9.3.

Typically, an outgoing user data packet is submitted by an upper-layer protocol (such as the forwarding bridge of an SS) for transmission on the MAC interface. The packet is compared against a set of classifiers. The matching classifier for the packet identifies the corresponding service flow via the service flow ID (SFID). In the case where more than one classifier matches the packet, the highest priority classifier is chosen.

The classifier matching a packet may be associated with a payload header suppression rule. A PHS rule provides details on how header bytes of a packet PDU may be omitted, replaced with a PHSI for transmission, and subsequently regenerated at the receiving end. PHS rules are indexed by the combination of {SFID, PHSI}. When a service flow is deleted, all classifiers and any associated PHS rules referencing it shall also be deleted.

#### 5.2.4 Payload header suppression

In payload header suppression (PHS), a repetitive portion of the payload headers of the higher layer is suppressed in the MAC SDU by the sending entity and restored by the receiving entity. On the uplink, the sending entity is the SS and the receiving entity is the BS. On the downlink, the sending entity is the BS and the receiving entity is the SS. Each MAC SDU is prefixed with a PHSI, which references the payload header suppression field (PHSF).

The sending entity uses classifiers to map packets into a service flow. The classifier uniquely maps packets to its associated PHS Rule. The receiving entity uses the CID and the PHSI to restore the PHSF. Once a PHSF has been assigned to a PHSI, it shall not be changed. To change the value of a PHSF on a service flow, a new PHS rule shall be defined, the old rule is removed from the service flow, and the new rule is added. When a classifier is deleted, any associated PHS rule shall also be deleted.

PHS has a payload header suppression valid (PHSV) option to verify or not verify the payload header before suppressing it. PHS has also a payload header suppression mask (PHSM) option to allow select bytes not to be suppressed. This is used for sending bytes that change, such as IP sequence numbers, while still suppressing bytes that do not change.

The BS shall assign all PHSI values just as it assigns all CID values. Either the sending or the receiving entity shall specify the PHSF and the payload header suppression size (PHSS). This provision allows for preconfigured headers or for higher-level signaling protocols outside the scope of this specification to establish cache entries. PHS is intended for unicast service and is not defined for multicast service.

It is the responsibility of the higher-layer service entity to generate a PHS Rule which uniquely identifies the suppressed header within the service flow. It is also the responsibility of the higher-layer service entity to guarantee that the byte strings being suppressed are constant from packet to packet for the duration of the active service flow.

#### 5.2.4.1 PHS operation

SS and BS implementations are free to implement PHS in any manner as long as the protocol specified in this subclause is followed. Figure 9 illustrates the following procedure.

A packet is submitted to the packet CS. The SS applies its list of Classifier rules. A match of the rule shall result in an Uplink Service Flow, CID, and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the SS shall compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM. If they match, the SS shall suppress all the bytes in the Uplink PHSF except the bytes masked by PHSM. The SS shall then prefix the PDU with the PHSI and present the entire MAC SDU to the MAC SAP for transport on the uplink.

When the packet is received by the BS, the BS shall determine the associated CID by examination of the generic MAC header. The BS sends the PDU to the MAC SAP associated with that CID. The receiving packet CS uses the CID and the PHSI to look up PHSF, PHSM, and PHSS. The BS reassembles the packet and then proceeds with normal packet processing. The reassembled packet contains bytes from the PHSF. If verification was enabled, then the PHSF bytes equal the original header bytes. If verification was not enabled, then there is no guarantee that the PHSF bytes match the original header bytes.

A similar operation occurs on the downlink. The BS applies its list of Classifiers. A match of the Classifier shall result in a Downlink Service Flow and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the BS shall verify the Downlink Suppression Field in the packet with the PHSF. If they match, the BS shall suppress all the bytes in the Downlink Suppression Field except the bytes masked by PHSM. The BS shall then prefix the PDU with the PHSI and present the entire MAC SDU to the MAC SAP for transport on the downlink.

The SS shall receive the packet based upon the CID Address filtering within the MAC. The SS receives the PDU and then sends it to the CS. The CS then uses the PHSI to lookup PHSF, PHSM, and PHSS. The SS reassembles the packet and then proceeds with normal packet processing.

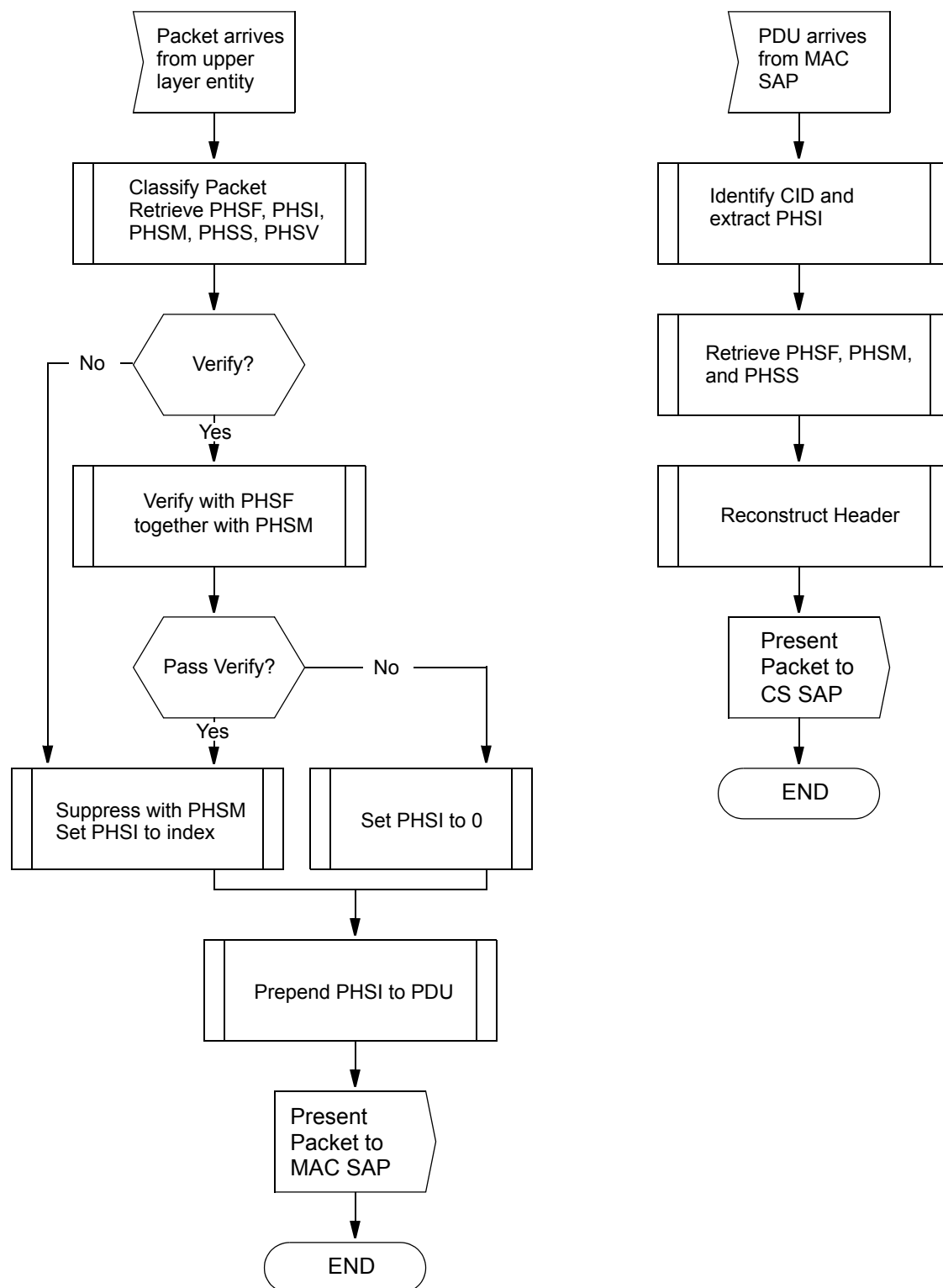


Figure 9—Payload header suppression operation

Figure 10 demonstrates packet suppression and restoration when using PHS masking. Masking allows only bytes that do not change to be suppressed. Note that the PHSF and PHSS span the entire suppression field, included suppressed and unsuppressed bytes.

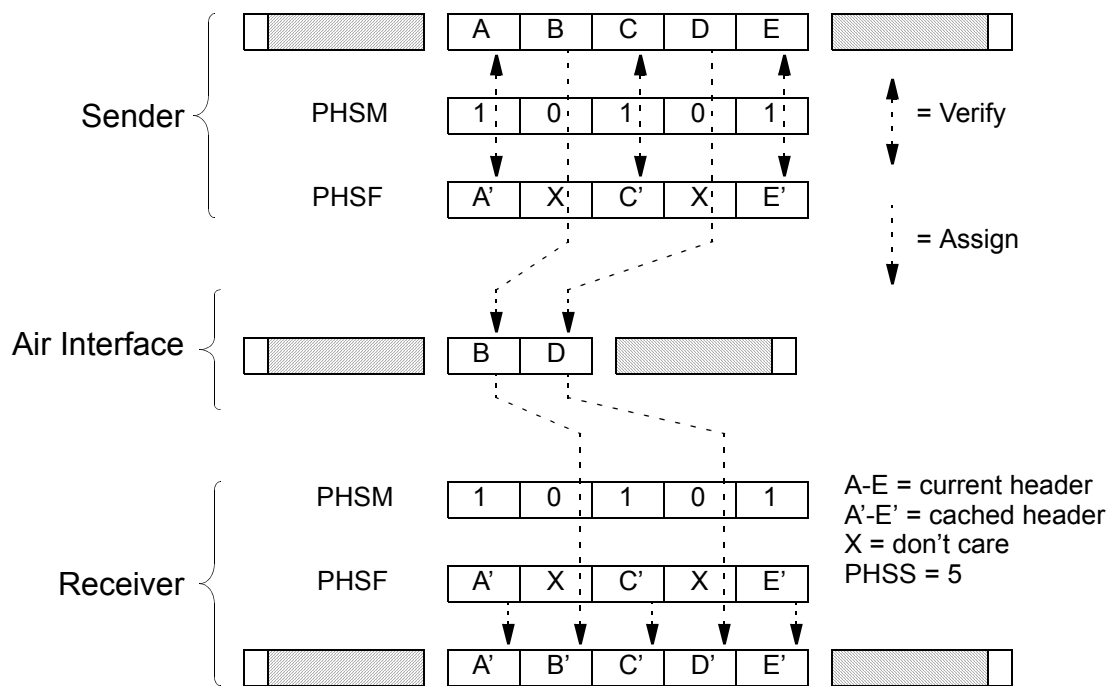


Figure 10—Payload header suppression with masking

#### 5.2.4.2 PHS signaling

PHS requires the creation of the following three objects:

- Service flow
- Classifier
- PHS rule

These three objects may be created either simultaneously or in separate message flows.

PHS Rules are created with dynamic service addition (DSA), or dynamic service change (DSC) messages. The BS shall define the PHSI when the PHS Rule is created. PHS rules are deleted with the DSC or dynamic service deletion (DSD) messages. The SS or BS may define the PHSS and PHSF. To change the value of a PHSF on a service flow, a new PHS rule shall be defined, the old rule is removed from the service flow, and the new rule is added.

Figure 11 shows the two ways to signal the creation of a PHS rule.

It is possible to partially specify a PHS rule (in particular the size of the rule) at the time a service flow is created. As an example, it is likely that, when a service flow is first provisioned, the header fields to be suppressed will be known. The values of some of the fields [e.g., IP addresses, user datagram protocol (UDP) port numbers, etc.] may be unknown and would be provided in a subsequent DSC as part of the activation of the service flow (using the "Set PHS Rule" DSC Action). If the PHS rule is being defined in more than one step, each step, whether it is a DSA or DSC message, shall contain both the service flow ID (or reference) and a PHS index to uniquely identify the PHS rule being defined.

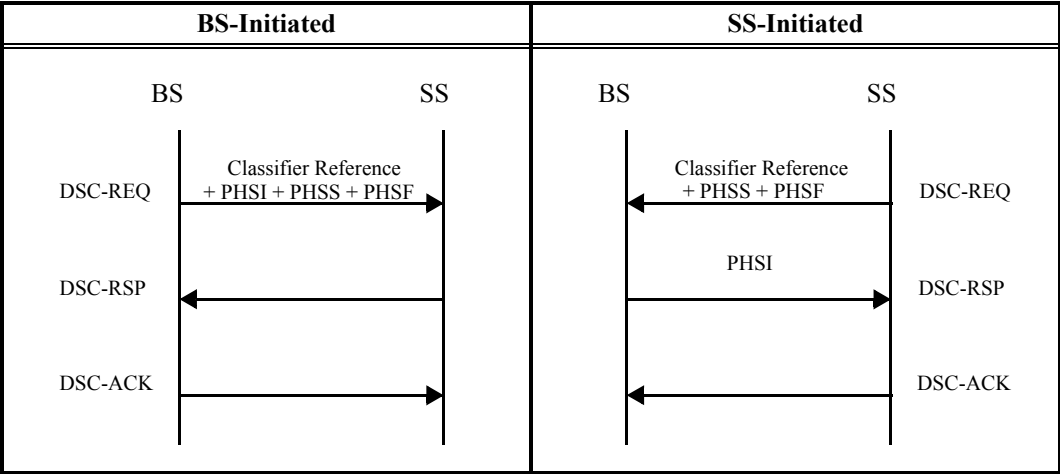


Figure 11—Payload header suppression signaling example

5.2.5 IEEE Std 802.3/Ethernet specific part

5.2.5.1 IEEE Std 802.3/Ethernet CS PDU format

The IEEE Std 802.3/Ethernet PDUs are mapped to MAC SDUs according to Figure 12 (when header suppression is not applied) or Figure 13 (with header suppression).

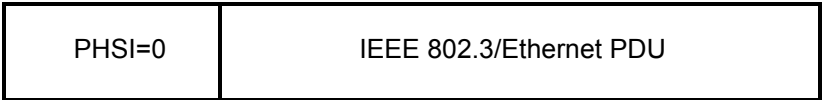


Figure 12—IEEE 802.3/Ethernet CS PDU format without header suppression

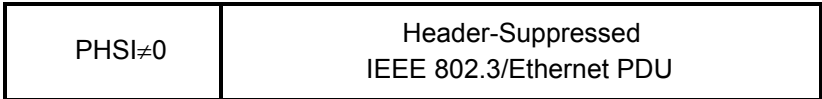


Figure 13—IEEE 802.3/Ethernet CS PDU format with header suppression

5.2.5.2 IEEE Std 802.3/Ethernet CS classifiers

The following parameters are relevant for IEEE Std 802.3/Ethernet CS classifiers:

Logical link control (LLC) classification parameters—zero or more of the LLC classification parameters (destination MAC address, source MAC address, Ethertype/SAP).

For IP over IEEE 802.3/Ethernet, IP headers may be included in classification. In this case, the IP classification parameters (11.4.9.3.6.2—11.4.9.3.6.7) are allowed.

5.2.6 IEEE Std 802.1Q-1998 VLAN specific part

This CS shall be employed when IEEE Std 802.1Q-1998 tagged VLAN frames are to be carried over the IEEE Std 802.16-2001 network.

5.2.6.1 IEEE Std 802.1Q-1998 VLAN CS PDU format

The format of the IEEE Std 802.1Q-1998 VLAN CS PDU shall be as shown in Figure 14.

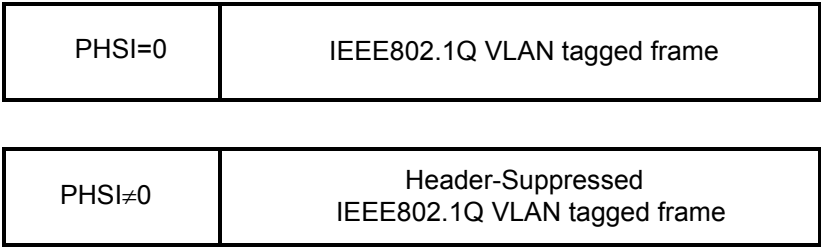


Figure 14—IEEE 802.1Q VLAN CS PDU format

5.2.6.2 IEEE Std 802.1Q-1998 CS classifiers

The following parameters are relevant for IEEE Std 802.1Q-1998 CS classifiers:

LC classification parameters—zero or more of the LLC classification parameters (Destination MAC address, source MAC address, Ethertype/SAP).

IEEE Std 802.1D-1998 Parameters—zero or more of the IEEE classification parameters (IEEE Std 802.1D-1998 Priority Range, IEEE Std 802.1Q-1998 VLAN ID).

For IP over IEEE Std 802.1Q-1998 VLAN, IP headers may be included in classification. In this case, the IP classification parameters (11.4.9.3.6.2—11.4.9.3.6.7) are allowed.

5.2.7 IP specific part

This subclause applies when IP (IETF RFC 791, IETF RFC 2460) is carried over the IEEE Std 802.16-2001 network.

5.2.7.1 IP CS PDU format

The format of the IP CS PDU shall be as shown in Figure 15 (when header suppression is not applied) or Figure 16 (with header suppression).