INTERNATIONAL STANDARD

ISO/IEC/ IEEE 8802-21

First edition
2018-04

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements —

Part 21: Media independent services framework

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains — Exigences spécifiques —

Partie 21: Cadre des services indépendants des supports

Reference number
ISO/IEC/IEEE 8802-21:2018(E)

© IEEE 2017



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2017

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

© IEEE 2017 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted.

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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

ISO/IEC/IEEE 8802-21 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.21-2017) and drafted in accordance with its editorial rules. It was adopted under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO website.

© IEEE 2017 – All rights reserved

IEEE Std 802.21™-2017
(Revision of IEEE Std 802.21-2008
as amended by IEEE Std 802.21a™-2012,
IEEE Std 802.21b™-2012, IEEE Std 802.21c™-2014,
and IEEE Std 802.21d™-2015)

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Services Framework

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 February 2017

IEEE-SA Standards Board

Abstract: An extensible IEEE 802® media access independent services framework (i.e., function and protocol) is defined that enables the optimization of services including handover and other services when performed between heterogeneous IEEE 802 networks. These services are facilitated by this standard when networking between IEEE 802 networks and cellular networks.

Keywords: broadcast, downlink only, group, group management, group security, IEEE 802.21™, management, media independent handover, media independent service, mobile node, mobility, multicast, point of attachment, point of service, proactive authentication, seamless, security protection, service access authentication

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

Copyright © 2017 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 28 April 2017. Printed in the United States of America.

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

3GPP and UMTS are trademarks of The European Telecommunications Standards Institute (ETSI).

PDF: ISBN 978-1-5044-3806-3 STD22456
Print: ISBN 978-1-5044-3807-0 STDPD22456

IEEE prohibits discrimination, harassment, and bullying.
For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, 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.

Updating of IEEE Standards documents

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

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Xplore at http://ieeexplore.ieee.org/ or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P802.21 Working Group had the following membership:

Subir Das, *Chair*
Hyeong Ho Lee, *Vice Chair*
Yoshikazu Hanatani, *Technical Editor*

H. Anthony Chan
Clint Chaplin
Lidong Chen
Jin Seek Choi
Daniel Corujo
Antonio De la Oliva Delgado
Yong-Geun Hong
Sangkwon Peter Jeong
Farrokh Khatibi
Michael Lynch
Yoichi Masuda
Naoki Ogura
Yoshihiro Ohba
Hyunho Park
Charles E. Perkins
Karen Randall
Yusuke Shimizu
Tomoki Takazoe
Keiichi Teramoto
Yuji Unagami

In addition, the following members have either contributed or participated during the development of this Standard:

Yusuke Doi
Krzysztof Grochla
Changhwa Lyou
Torleiv Masen
Christian Niephaus
Dick Roy
Ruben Salazar
Randy Turner

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

Thomas Alexander
Butch Anton
H. Stephen Berger
Harry Bims
Gennaro Boggia
William Byrd
Juan Carreon
Charles Cook
Daniel Corujo
Subir Das
Sourav Dutta
Richard Edgar
Marc Emmelmann
Avraham Freedman
Joel Goergen
Randall Groves
Yoshikazu Hanatani
Werner Hoelzl
David Howard
Noriyuki Ikeuchi
Atsushi Ito
Raj Jain
Piotr Karocki
Stuart Kerry
Farrokh Khatibi
Yongbum Kim
Hyeong Ho Lee
Jae Seung Lee
Moon-Sik Lee
Michael Lynch
Elvis Maculuba
Stephen McCann
Michael McInnis
Jeffrey Moore
Nick S. A. Nikjoo
Paul Nikolich
Yoshihiro Ohba
Satoshi Oyama
Arumugam Paventhan
Venkatesha Prasad
Karen Randall
Maximilian Riegel
Naotaka Sato
Yusuke Shimizu
Dorothy Stanley
Thomas Starai
Michael Stelts
Walter Struppler
Mark Sturza
Tomoki Takazoe
Patricia Thaler
Mark-Rene Uchida
Dmitri Varsanofiev
Prabodh Varshney
Oren Yuen

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

When the IEEE-SA Standards Board approved this standard on 14 February 2017, it had the following membership:

Jean-Philippe Faure, *Chair*
Vacant Position, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Gary Hoffman
Michael Janezic
Thomas Koshy
Joseph L. Koepfinger*
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Introduction

This introduction is not part of IEEE Std 802.21-2017, IEEE Standard for Local and metropolitan area networks—Part 21: Media Independent Services Framework.

This standard defines an extensible IEEE 802® media access independent services framework (i.e., function and protocol) that enables the optimization of services including handover service when performed between heterogeneous IEEE 802 networks. It also facilitates these services when networking between IEEE 802 networks and cellular networks.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Contents

1. Overview 16
1.1 Scope 16
1.2 Purpose 16
1.3 General 16
1.4 Assumptions 18
1.5 Media independence 18

2. Normative references 19

3. Definitions 22

4. Abbreviations and acronyms 26

5. General architecture 31
5.1 Introduction 31
5.2 General design principles 33
5.3 MISF service overview 33
5.4 Media independent service reference framework 36
5.5 MISF reference models for link-layer technologies 38
5.6 Service access points (SAPs) 44
5.7 MIS protocol 46

6. MISF services 48
6.1 General 48
6.2 Service management 48
6.3 Media independent event service 50
6.4 Media independent command service 54
6.5 Media independent information service 58

7. Service access point (SAPs) and primitives 70
7.1 Introduction 70
7.2 SAPs 71
7.3 MIS_LINK_SAP primitives 73
7.4 MIS_SAP primitive 85
7.5 MIS_NET_SAP primitive 136

8. Media independent service protocol 138
8.1 Introduction 138
8.2 MIS protocol description 138
8.3 MIS protocol identifier 150
8.4 MIS protocol frame format 152
8.5 Message parameter TLV encoding 159
8.6 MIS protocol messages 159

9. MIS protocol protection 179
9.1 Protection established through MIS (D)TLS 179
9.2 Key establishment through an MIS service access authentication 180
9.3 MIS message protection mechanisms for EAP-generated SAs 189
9.4 Common procedures 196
9.5 Group manipulation for group addressed messages 197
9.6 Group addressed message protection 223

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

10. Proactive authentication 231
10.1 Media-specific proactive authentication 232
10.2 Bundling media access authentication with MIS service access authentication 233

Annex A (informative) Bibliography 236

Annex B (normative) Quality of service mapping 237
B.1 Generic IEEE 802.21 QoS flow diagram 238
B.2 Generic IEEE 802.21 QoS parameter mappings 239
B.3 Deriving generic IEEE 802.21 QoS parameters 241

Annex C (normative) Mapping media independent service (MIS) messages to reference points 244

Annex D (normative) Media-specific mapping for service access points (SAPs) 245
D.1 MIS_LINK_SAP mapping to specific technologies 245
D.2 Mapping from MIS_LINK_SAP to media-specific SAPs 247

Annex E (normative) Data type definitions 249
E.1 General 249
E.2 Basic data types 249
E.3 Derived data types 251

Annex F (normative) Information element identifiers 282

Annex G (normative) Media independent information service (MIIS) basic schema 283

Annex H (informative) Making user extensions to media independent information service (MIIS) schema 284

Annex I (normative) IEEE 802.21 management information base (MIB) 285
I.1 Parameters requiring MIB definition 285
I.2 IEEE 802.21 MIB definition 286

Annex J (informative) Example media independent service (MIS) message fragmentation 287
J.1 Example of original MIS message fragmentation 287
J.2 Calculation of securityOverhead when there is an MIS security association (SA) 287

Annex K (normative) Media independent service (MIS) protocol message code assignments 290

Annex L (normative) Protocol implementation conformance statement (PICS) proforma 294
L.1 Introduction 294
L.2 Scope 294
L.3 Conformance 294
L.4 Instructions 294
L.5 Identification of the implementation 297
L.6 Identification of the protocol 297
L.7 Identification of corrigenda to the protocol 297
L.8 PICS proforma tables 297

Annex M (informative) Authentication and key distribution procedures 303
M.1 Media independent service (MIS) service access authentication 303
M.2 Push key distribution 305
M.3 Proactive authentication 306
M.4 Optimized pull key distribution 307
M.5 Termination phase 308

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Annex N (informative) Protection through transport protocols....309
N.1 Protection through layer 2....309
N.2 Protection through internet protocol security (IPsec)....309

Annex O (informative) Examples of fragmented group key block (GKB) operation....310

Annex P (normative) Use of Bloom Filter for certificate revocation....312
P.1 Calculating Bloom Filter output for revoked certificates....312
P.2 Certificate revocation check....312
P.3 False positive case....312

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

List of Figures

Figure 1—MIS services and their initiations 18
Figure 2—Group communication functional entities 32
Figure 3—MISF communication model 37
Figure 4—General MISF reference model and SAPs 39
Figure 5—Types of MISF relationships 40
Figure 6—MIS reference model for IEEE 802.3 41
Figure 7—MIS reference model for IEEE 802.11 42
Figure 8—MIS reference model for IEEE 802.16 42
Figure 9—MIS reference model for 3GPP systems 43
Figure 10—MIS reference model for 3GPP2 systems 44
Figure 11—Relationship between different MISF SAPs 45
Figure 12—Link events and MIS events 51
Figure 13—Remote MIS events 51
Figure 14—MIS events subscription and flow 52
Figure 15—Link commands and MIS commands 55
Figure 16—Remote MIS command 56
Figure 17—Command service flow 57
Figure 18—Depicting a list of neighboring networks with information elements 63
Figure 19—TLV representation of information elements 64
Figure 20—MIIS information flow 70
Figure 21—State machines interactions 140
Figure 22—Transaction timers state machine 145
Figure 23—Transaction source state machine 146
Figure 24—Transaction destination state machine 147
Figure 25—ACK requestor state machine 148
Figure 26—ACK responder state machine 149
Figure 27—MIS protocol general frame format 152
Figure 28—MIS protocol header format 152
Figure 29—Protected MIS frame format 154
Figure 30—MIS PDU during TLS handshake 155
Figure 31—MIS PDU in existence of MIS SA by TLS 155
Figure 32—MIS PDU protected by an EAP-generated MIS SA 156
Figure 33—MIS PDU upon Transport Address Change 156
Figure 34—MIS PDU protected by a GKB-generated MIS SA with a signature TLV 156
Figure 35—MIS PDU protected by digital signature only 157
Figure 36—Fragmented MIS protocol frame format 157
Figure 37—Protected fragmented MIS protocol frame format 158
Figure 38—Message parameter TLV encoding 159
Figure 39—The TLV encoding for the vendor-specific TLV (Type = 111) 159
Figure 40—Protocol stack of service access authentication (with an EAP server) 180
Figure 41—Main stages with MN initiated EAP execution 182
Figure 42—Main stages with PoS initiated EAP execution 183
Figure 43—Main stages with MN initiated ERP execution 184
Figure 44—Main stages with PoS initiated ERP execution (1) 185
Figure 45—Main stages with PoS initiated ERP execution (2) 186
Figure 46—MIS Key Hierarchy 188
Figure 47—MIS PDU protection procedure 191
Figure 48—AES-CCM nonce construction 192
Figure 49—Format of *B0* 192
Figure 50—Format of counter *Ctr(i)* 193
Figure 51—Security TLV for AES-CCM 193
Figure 52—Security TLV for AES CBC and HMAC-SHA1-96 195
Figure 53—Security TLV for HMAC-SHA1-96 195
Figure 54—Security TLV for AES-CMAC 196

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Figure 55—Sending and receiving protected MIS PDU 197
Figure 56—A group of management tree of depth 3 199
Figure 57—Three complete subtrees for the group with nodes 000, 001, 010, 011, 101, and 111 200
Figure 58—GKB for the group with nodes 000, 001, 010, 011, 101, and 111 202
Figure 59—Flow diagram of the verify group code generation 203
Figure 60—Flow diagram of the group key wrapping 204
Figure 61—Selection of *master group key unwrapping* or *no group key procedures* 205
Figure 62—Flow diagram of the group key unwrapping 205
Figure 63—Flow diagram of *no group key data procedure* 206
Figure 64—Flow diagram of the *master group key unwrapping procedure 1* 207
Figure 65—Flow diagram of the *master group key unwrapping procedure 2* 209
Figure 66—Flow diagram of the *master group key unwrapping procedure 3* 210
Figure 67—Example of group manipulation distribution using multicast mechanisms 213
Figure 68—Summary of steps performed by MIS user of PoS with group manager 215
Figure 69—Summary of steps performed by MIS user of PoS with group manager (continued from Figure 68) 216
Figure 70—Flow diagram of CreateCompleteSubtree and CreateCompleteSubtreeFragments procedure .217
Figure 71—Summary of steps performed by MISF of PoS with group manager 219
Figure 72—Summary of steps performed by the recipient MISF 222
Figure 73—Key derivation example 223
Figure 74—MIS PDU protection procedure with the GKB-generated MIS SA 225
Figure 75—Format of *B0* with associated data 226
Figure 76—Signing with confidentiality 228
Figure 77—Signing without confidentiality 228
Figure 78—Signature verification with confidentiality 229
Figure 79—Signature verification without confidentiality 229
Figure 80—Protocol stack for MIS supported proactive authentication 232
Figure 81—Protocol stack for MIS supported optimized pull key distribution with two points of service 232
Figure 82—Key hierarchy for bundle case 235
Figure B.1—An example flow for setting application QoS requirements 239
Figure E.1—Encoding example of a LIST with two LINK_ID elements 250
Figure J.1—MIS fragmentation example for Maximum Transmission Unit (MTU) of 1500 octets 287
Figure J.2—Example of protected MIS fragment message 289
Figure M.1—Mobile initiated access authentication phase 303
Figure M.2—Network initiated access authentication phase 304
Figure M.3—Push key distribution 305
Figure M.4—Proactive authentication 306
Figure M.5—Optimized pull key distribution 307
Figure M.6—Mobile node (MN) initiated termination phase 308
Figure O.1—Example of fragmented complete subtrees with Subgroup Ranges 311
Figure P.1—Bloom Filter example (k = 3, m = 32) 312

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

List of Tables

Table 1—Summary of reference points 38
Table 2—MIS protocol Ethernet type 47
Table 3—Service management primitives 49
Table 4—Link events 53
Table 5—MIS events 54
Table 6—Link commands 58
Table 7—MIS commands 58
Table 8—Information element containers 60
Table 9—Information elements 61
Table 10—Information element namespace 64
Table 11—IE_CONTAINER_LIST_OF_NETWORKS definition 65
Table 12—IE_CONTAINER_NETWORKS definition 66
Table 13—IE_CONTAINER_POA definition 67
Table 14—MIS_LINK_SAP primitives 71
Table 15—MIS_NET_SAP primitive 71
Table 16—MIS_SAP primitives 72
Table 17—State machine symbols 141
Table 18—Inter-state-machine variables 142
Table 19—Exported state machine variables 142
Table 20—State Machines to be searched for incoming message 143
Table 21—State Machines to be searched for outgoing message 143
Table 22—Description of MIS protocol header fields 153
Table 23—Valid combination of S-bit and security-related TLVs 154
Table 24—Cryptographic algorithms 188
Table 25—Ciphersuites 189
Table 26—Device key assignments for recipients through a depth-3 group management tree 199
Table 27—Group ciphersuites 230
Table 28—Group key distribution ciphersuites 231
Table B.1—QoS parameter mapping for IEEE 802.11 240
Table B.2—QoS parameter mapping for IEEE 802.16 and 3GPP2 241
Table B.3—QoS parameter mapping for 3GPP 241
Table C.1—Mapping MIS messages to reference points 244
Table D.1—MIS_Link_SAP/IEEE 802.16 primitives mapping 245
Table D.2—MIS_LINK_SAP/IEEE 802.11/IEEE 802.3/IEEE 802.1Q primitives mapping 246
Table D.3—MIS_LINK_SAP/3GPP/3GPP2 primitives mapping 247
Table E.1—Basic data types 249
Table E.2—General data types 251
Table E.3—Data types for address 252
Table E.4—Data types for links 253
Table E.5—Link actions 261
Table E.6—Link action attributes 261
Table E.7—Link down reason code 262
Table E.8—Link going down reason code 262
Table E.9—Data types for QoS 263
Table E.10—Data types for location 263
Table E.11—Value field format of PoA location information (geospatial location) 264
Table E.12—Data types for IP configuration 265
Table E.13—Data types for information elements 265
Table E.14—Network type and subtype representation 270
Table E.15—Data types for binary query 272
Table E.16—Data type for RDF query 273
Table E.17—Data type for binary information query response 273
Table E.18—Data type for RDF information query response 273
Table E.19—Data type for MISF identification 274

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Table E.20—Data type for MIS capabilities 274
Table E.21—Data type for MIS registration 276
Table E.22—Data type for handover operations 277
Table E.23—Data type for MIS_NET_SAP primitives 277
Table E.24—Data type for security 277
Table E.25—Delivery types for delivery of control messages 281
Table F.1—Information element identifier values 282
Table J.1—Protection overhead for EAP-generated SAs 288
Table K.1—AID assignments 290
Table K.2—Type values for TLV encoding 291

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Services Framework

1. Overview

1.1 Scope

This standard defines an extensible IEEE 802® media access independent services framework (i.e., function and protocol) that enables the optimization of services including handover service when performed between heterogeneous IEEE 802 networks. It also facilitates these services when networking between IEEE 802 networks and cellular networks.

1.2 Purpose

The purpose of this standard is to improve the user experience of mobile devices by describing a framework and knobs that several services can utilize in a media independent manner, including the handover service between heterogeneous IEEE 802 networks. This framework is also applicable for interworking between IEEE 802 networks and cellular networks.

1.3 General

This standard provides link-layer intelligence and other related network information to upper layers of a mobile device or a network element to support several use cases, such as handovers between heterogeneous networks, radio resource management, home energy management, software-defined radio access networks, and device-to-device (D2D) communication as described in IEEE Std 802.21.1™-2017. In this standard, unless otherwise noted, *media* refers to the method/mode of accessing a telecommunication system (e.g., cable, radio, satellite), as opposed to sensory aspects of communication (e.g., audio, video).

The following items are not within the scope of this standard:

- Enhancements specific to particular link-layer technologies that are required to support this standard (they should be carried out by those respective link-layer technology standards)
- Media-specific protection mechanisms
- Higher layer (layer 3 and above) enhancements that are required to support this standard

The purpose of this standard is to provide a framework with several knobs so that they can be utilized to enhance the experience of mobile users while they are performing functions, such as handovers between heterogeneous networks when mobile, managing link-layer radio resources with or without presence of

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

software-defined networking, and obtaining group keys for home energy-management systems via multicast group management.

This standard supports another important aspect of optimized performance enhancement through link adaptation. For example, a user chooses an application that requires a higher data rate than available on the current link, necessitating a link adaptation to provide the higher rate, or necessitating an action if the higher rate is unavailable on the current link. In all such cases, service continuity and/or user experience should be maintained to the extent possible during this action. As an example, when making a network transition during a phone call, the handover procedures should be executed in such a way that any perceptible interruption to the conversation should be minimized.

This standard supports cooperative use of information available at the mobile node and within the network infrastructure. The mobile node is well-placed to detect available network resources based on the use cases that they are performing. The network infrastructure is well-suited to store the necessary information that is required to provide either a better user experience or managing the mobile devices better. The information could be related to handover and radio-resource management, such as neighborhood cell lists, location of mobile nodes, available link-layer radio resources and higher layer service availability, home energy-management system such as multicast group information with their keys, and certificates.

The overall network includes a mixture of cells of drastically different sizes, such as those from IEEE Std 802.15™, IEEE Std 802.11™, IEEE Std 802.16™, 3GPP™[1], and 3GPP2, with overlapping coverage. The specific use case is initiated either by the mobile node or by a network node. They could be specific measurement reports, triggers supplied by the link layers, unavailability of a key or a certificate. Specifically the standard consists of the following elements:

a) A framework that enables the optimization of handover and other services supporting several use cases described in IEEE Std 802.21.1-2017. The framework relies on the presence of a higher layer applications such as mobility-management protocol stack within the network elements that supports the handover, and a group manager function that manages groups of mobile nodes and distributes the keys and certificates. The framework presents media independent service (MIS) reference models for different link-layer technologies so that all actions from the higher layer can be performed with minimum or no modifications of link-layer technologies.

b) A set of media independent functions within the protocol stacks of the network elements and a new entity created therein called the MIS function (MISF).

c) A media independent service access point (called the MIS_SAP) and associated primitives are defined to provide MIS users with access to the services of the MISF. The MISF provides the following services:

    1) The media independent event service that detects changes in link-layer properties and initiates appropriate events (triggers) from both local and remote interfaces.

    2) The media independent command service provides a set of commands for the MIS users to control link properties that are relevant to handover and other services.

    3) The media independent information service provides the information about different networks and their services, thus enabling more effective handover and other management decisions to be made across heterogeneous networks.

d) Media independent protocol messages and their protection mechanisms using both unicast and multicast modes of transmission.

e) The definition of new link-layer service access points (SAPs) and associated primitives for each link-layer technology as applicable to handover and other use cases described in IEEE Std 802.21.1-2017. The new primitives help the MISF collect link information and control link behavior during handovers.

[1] 3GPP is a trademark of The European Telecommunications Standards Institute (ETSI).

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Figure 1 shows the placement of the MISF within the protocol stack of a multiple interfaced mobile node (MN) or network entity. The MISF provides services to the MIS users through a single media independent interface (the MIS service access point) and obtains services from the lower layers through a variety of media dependent interfaces (media-specific SAPs).

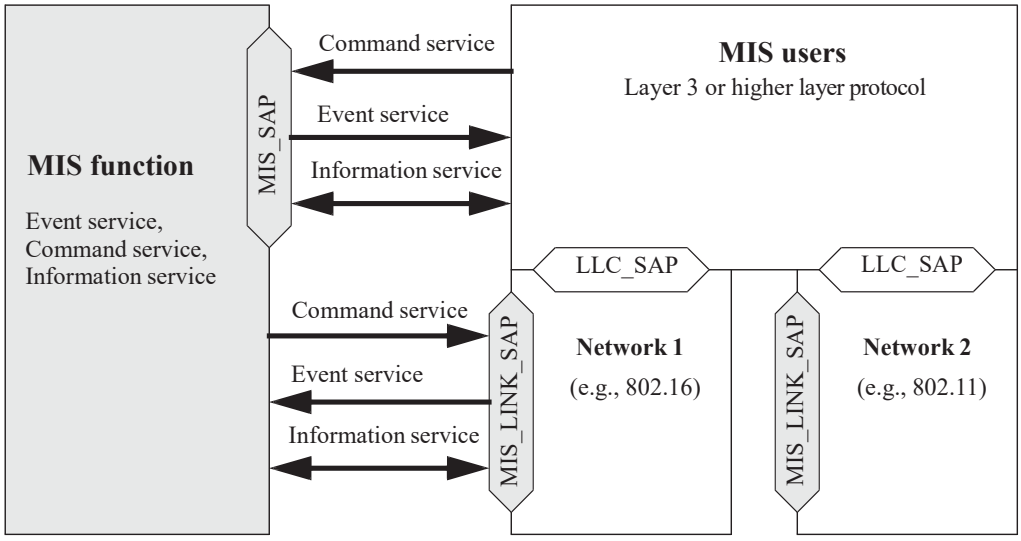


Figure 1—MIS services and their initiations

1.4 Assumptions

The following assumptions have been made in the development of this standard:

a) The MN is capable of supporting multiple link-layer technologies, such as wireless, wired, or mixed.

b) The MISF is a logical entity, whose definition is independent of its deployment location on the MN or in the network.

c) The MISF, regardless of whether it is located on the MN or in the network, receives and transmits information about the configuration and condition of access networks around the MN. This information originates at different layers of the protocol stack within the MN or at various network elements.

   1) When the information originates at a remote network element, the MISF on the local network element obtains it through MIS message exchanges with a peer MISF instance that resides in the remote network element.

   2) When the information originates at lower layers of the protocol stack within an MN or network entity, the MISF on that entity obtains it locally through the service primitives of the SAPs that define the interface of the MISF with the lower layers.

1.5 Media independence

The intent of this standard is to provide generic link-layer intelligence and other network resources information independent of the specifics of mobile nodes or radio networks.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

The defined SAPs and primitives in this standard provide generic link-layer intelligence. Depending upon the specific use cases, individual media-specific technologies may need to be enhanced to support the media-specific SAPs and primitives and to satisfy the generic abstractions of this standard.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

3GPP TS 23.003 (2015-06), Numbering, addressing and identification (Release 12).

3GPP TS 25.215 (2015-03), Physical layer—Measurements (FDD) (Release 12).

3GPP TS 25.401 (2013-12), UTRAN overall description (Release 12).

3GPP TS 25.413 (2015-03), UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling (Release 12).

3GPP TS 45.008 (2014-09), Radio subsystem link control (Release 12).

3GPP2 C.S0004-D (2004-03), Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems.

ANSI X3.159-1989: Programming Language C.[2]

FIPS 198, The Keyed-Hash Message Authentication Code (HMAC).[3]

IEEE Std 802.1AB™-2009, IEEE Standard for Local and Metropolitan Area Networks—Station and Media Access Control Connectivity Discover. [4, 5]

IEEE Std 802.1AR™-2009, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identity.

IEEE Std 802.1Q™-2014, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.

IEEE Std 802.1X™-2010, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control.

IEEE Std 802.3™-2012, IEEE Standard for Ethernet.

IEEE Std 802.11™-2012, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Std 802.16™-2012, IEEE Standard for Air Interface for Broadband Wireless Access Systems.

[2] ANSI publications are available from the American National Standards Institute (http://www.ansi.org/).

[3] FIPS publications are made available at http://csrc.nist.gov/publications/PubsFIPS.html.

[4] IEEE publications are available from the Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).

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

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

IEEE Std 802.16.1™-2012, IEEE Standard for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems.

IEEE Std 802.20™-2008, IEEE Standard for Local and metropolitan area networks—Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility—Physical and Media Access Control Layer Specification.

IEEE Std 802.21.1™-2017, IEEE Standard for Standard for Local and metropolitan area networks Part 21.1: Media Independent Services.

IEEE Std 802.22™-2011, IEEE Standard for Information Technology—Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN)—Specific requirements—Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands.

IETF RFC 1661 (1994-07), The Point-to-Point Protocol (PPP).[6]

IETF RFC 2627 (1999-06), Key Management for Multicast: Issues and Architectures.

IETF RFC 2865 (2000-06), Remote Authentication Dial In User Service (RADIUS).

IETF RFC 2988 (2000-11), Computing TCP's Retransmission Timer.

IETF RFC 3748 (2004-06), Extensible Authentication Protocol (EAP).

IETF RFC 4119 (2005-12), A Presence-based GEOPRIV Location Object Format.

IETF RFC 4302 (2005-12), IP Authentication Header.

IETF RFC 4303 (2005-12), IP Encapsulating Security Payload (ESP).

IETF RFC 4443 (2006-03), Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.

IETF RFC 4555 (2006-06), IKEv2 Mobility and Multihoming Protocol (MOBIKE).

IETF RFC 4776 (2006-11), Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information.

IETF RFC 5184 (2008-05), Unified L2 Abstractions for L3-Driven Fast Handover.

IETF RFC 5246 (2008-08), The Transport Layer Security (TLS) Protocol Version 1.2.

IETF RFC 5280 (2008-05), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

IETF RFC 5677 (2009-12), IEEE 802.21 Mobility Services Framework Design (MSFD).

IETF RFC 5678 (2009-12), Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Server (MoS) Discovery.

IETF RFC 5679 (2009-12), Locating IEEE 802.21 Mobility Services Using DNS.

[6] IETF RFCs are available from the Internet Engineering Task Force website at http://www.ietf.org/rfc.html.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

IETF RFC 6225 (2011-07), Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information.

IETF RFC 6347 (2012-01), Datagram Transport Layer Security Version 1.2.

IETF RFC 6733 (2012-10), Diameter Base Protocol.

IETF RFC 6696 (2008-08), EAP Extensions for EAP Re-authentication Protocol (ERP).

IETF RFC 7296 (2014-06), Internet Key Exchange Protocol Version 2 (IKEv2).

IETF RFC 7542 (2015-05), The Network Access Identifier.

ISO 3166-1 (1997), Codes for the representation of names of countries and their subdivisions—Part 1: Country codes.[7]

ISO 4217, Codes for the Representation of Names of Countries.

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.

ITU-T Recommendation X.290 (1995), OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications—General concepts.[8]

ITU-T Recommendation X.296 (1995), OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications—Implementation conformance statements.

ITU-T Recommendation Y.1540, Internet protocol data communication service—IP packet transfer and availability performance parameters.

NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation.[9]

NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation—The CMAC Mode for Authentication.

NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation—The CCM Mode for Confidentiality and Authentication.

NIST SP 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, 2012.

NIST SP800-108, Recommendation for Key Derivation using Pseudorandom Functions, 2009.

W3C Recommendation, RDF/XML Syntax Specification.[10]

W3C Recommendation, Resource Description Framework (RDF)—Concepts and Abstract Syntax.

W3C Recommendation, SPARQL Query Language for RDF.

[7] ISO publications are available from the ISO Central Secretariat (http://www.iso.org/). ISO publications are also available from the American National Standards Institute (http://www.ansi.org/).
[8] ITU-T publications are available from the International Telecommunications Union (http://www.itu.int/).
[9] NIST publications are available from the National Institute of Standards and Technology (http://www.nist.gov/).
[10] W3C recommendations are available from http://www.w3.org.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[11]

authenticated encryption: An algorithm to convert plaintext data to ciphertext and generate a message authentication code with a cryptographic key as a parameter to provide confidentiality, integrity, and authenticity of the data. *See also:* **encryption**; **MIC algorithm**.

authentication process: A process to assure that the claimed identity belongs to the entity. It is also called entity authentication. In this standard, an access authentication is an entity authentication with the identity used to access a specific network or a media independent service (MIS).

authentication server: A server used for authentication purposes. When extensible authentication protocol (EAP) is used as an authentication protocol, the authentication server is an EAP server.

authenticator: A network entity to execute extensible authentication protocol (EAP) with a mobile node called a peer. An authenticator can use a backend server to conduct EAP execution. *Syn*: **EAP authenticator**.

candidate network: A network that is a potential target to the mobile node's movement.

candidate point of attachment (candidate PoA): A point of attachment (PoA) under evaluation to which the link may be switched.

certificate authority (CA): A trusted entity that issues and revokes public key certificates.

decryption: An algorithm to convert ciphertext of data to plaintext with a cryptographic key as a parameter. It is an inverse operation of encryption.

device key: A cryptographic key assigned to a device. Each device is provisioned with a set of device keys.

EAP authenticator: *See:* **authenticator**.

EAP peer: The entity that responds to the extensible authentication protocol (EAP) authenticator.

EAP re-authentication: An authentication protocol using a key established in a previous extensible authentication protocol (EAP) execution as defined in IETF RFC 6696.

EAP server: The entity that terminates the extensible authentication protocol (EAP) execution with the EAP peer. In the case where no backend authentication server is used, the EAP server is a part of the EAP authenticator. In the case where a backend authentication server is used, the EAP server is located on the backend authentication server.

encryption: An algorithm to convert plaintext data to ciphertext to provide confidentiality with a cryptographic key as a parameter.

extensible authentication protocol (EAP): An access authentication framework specified in IETF RFC 3748. It supports different authentication methods, called EAP methods.

group addressed message: A media independent service (MIS) message sent to nodes that belongs to a group identified by an MIS function (MISF) Group ID. A group addressed message is sent using a multicast transport mechanism, which is out of the scope of this specification. An exception to this is that a unicast transport mechanism when used for a two-member group.

group key block (GKB): A data entity carrying an encapsulated group key in such a manner that only those nodes that have the corresponding device keys are able to decapsulate it.

group key wrapping: Security procedure that uses group key block (GKB) as a data element to encrypt group keys.

[11] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org/.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

group management tree: A perfect binary tree used for group management purposes.

group manager (GM): A media independent service (MIS) user that manages the group by adding, deleting, and updating the group membership information. It also generates the group key when needed. It is also the entity that issues group manipulation commands.

group manipulation command: A command, sent to a group of nodes or to an individual node, that instructs the recipient to perform certain operations such as joining and leaving a group, updating group membership, and so on. By group manipulation command, we refer to the following commands: MIS_Pull_Group_Manipulate and MIS_Push_Group_Manipulate.

handover policies: A set of rules that contribute to making the handover decision for a mobile node.

handover: The process by which a mobile node obtains facilities and preserves traffic flows upon occurrence of a link switch event. The mechanisms and protocol layers involved in the handover vary with the type of the link switch event (i.e., with the type of the serving and target point of attachment and the respective subnet associations). Different types of handover are defined based on the way facilities for supporting traffic flows are preserved. *See also:* **hard handover**; **soft handover**; **seamless handover**.

hard handover: Handover where facilities for supporting traffic flows are subject to complete unavailability between their disruption on the serving link and their restoration on the target link (break-before-make).

horizontal handovers: A handover where a mobile node moves between point of attachments of the same link type (in terms of coverage, data rate, and mobility), such as universal mobile telecommunications systems (UMTS™[12]) to UMTS or wireless local area network (WLAN) to WLAN. *Syn:* **intra-technology handovers**.

information server: A server providing information about candidate access networks. The information server may be implemented in a media independent information server but may also be implemented with other standards such as the Access Network Discovery and Selection Function (ANDSF) defined in 3GPP or a server using Access Network Query Protocol (ANQP) defined in IEEE Std 802.11-2012.

internal node: A node having two children and one parent node.

inter-technology handovers: *See:* **vertical handovers**.

leaf key: A node key which is assigned to a leaf node of a group management tree.

leaf node: A node having one parent node without having a child node.

leaf number: The integer representation of the node index assigned to a leaf node.

link layer: Conceptual layer of control or processing logic that is responsible for maintaining control of the data link. The data link-layer functions provide an interface between the higher layer logic and the data link.

link switch: The process by which a mobile node changes the link that connects it to the network. Changing a link implies changing the remote link endpoint and therefore the point of attachment of the mobile node.

link: A communication channel through which nodes communicate for the exchange of L2 protocol data units. Each link is associated with two endpoints and has a unique identifier.

lower layers: The layers located at OSI Level 2 and below across different link-layer technology standards supported by this standard. For example, the IEEE 802.11 lower layers are the MAC sublayer and the PHY, while the 3GPP lower layers are L1/MAC/radio link control (RLC)/packet data convergence protocol (PDCP) in the case of wideband code division multiple access (W-CDMA) frequency division duplex (FDD)/time division duplex (TDD), respectively. The term *lower layers* also includes logical link control (LLC) layers such as IEEE 802.2 LLC or 3GPP radio link control (RLC). The MISF uses the services provided by these layers.

[12] UMTS is a trademark of The European Telecommunications Standards Institute (ETSI).

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

media independent service (MIS) network entity: Network entity with media independent service function (MISF) capability.

media independent service (MIS) node: An media independent service function (MISF) capable entity (mobile node or network).

media independent service (MIS) non-PoS: An MIS network entity that directly exchanges MIS messages with other MIS network entities but is not capable of directly exchanging MIS messages with any MIS-enabled mobile node.

media independent service (MIS) transport protocol: A protocol for transporting MIS protocol messages between a pair of MIS entities.

media independent service (MIS) users: Entities that use the services provided by the MISF. MIS users use the MIS_SAP to interact with the MISF.

media independent service function (MISF): A function that realizes MIS services.

media independent service function broadcast identifier (MISF Broadcast ID): An MISF Group ID of zero length, i.e., '0x00' (OCTET_STRING with *Length* field = 0x00 and no *Value* field).

media independent service function group identifier (MISF Group ID): An identifier of a group of MISF peer entities.

media independent service point of service (MIS PoS): Network-side MISF instance that exchanges MIS messages with an MN-based MISF. The same MIS network entity includes an MIS PoS for each MIS-enabled mobile node with which it exchanges MIS messages. A single MIS PoS is capable of hosting more than one MIS service. The MIS network entity that includes multiple MIS Points of Service is capable of providing different combinations of MIS services to the respective mobile nodes based on subscription or roaming conditions. Note that for a network entity comprising multiple interfaces, the notion of MIS PoS is associated with the network entity itself and not with just one of its interfaces. For MIS service access authentication, a PoS serves as an authenticator. Moreover, when a service access authentication establishes keys for proactive authentication, a PoS provides key distribution service for media-specific authenticators.

media-specific authenticator: An authenticator used for a media-specific network access authentication.

media-specific network access authentication: An authentication protocol for media access purpose specified for a specific media access. It establishes keys to be used in media-specific protection mechanisms.

media-specific protection mechanism: A mechanism that is applied to media-specific layers to protect the data traffic using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combination of an encryption algorithm and an integrity protection algorithm.

message authentication code: A data string generated over a message with a symmetric key by an algorithm, called *message authentication code algorithm*. It is used to verify the integrity of the message and to authenticate the origin of the message. *Syn:* **message integrity code**.

message authentication code algorithm: An algorithm to generate a message authentication code on a data message with a symmetric key to provide integrity protection and message origination authentication. *See also:* **message authentication code**.

message integrity code (MIC): *See:* **message authentication code**.

MIS security association (SA): A media independent service (MIS) security association is a set of cryptographic attributes established between the peer MIS entities for protecting MIS messages at the MIS protocol layer. An MIS SA is established via Transport Layer Security (TLS) handshake, extensible authentication protocol (EAP) execution, or via a group key distribution mechanism using group key block (GKB) where all of the TLS handshake, EAP execution, and group key distribution take place over the MIS protocol. When an MIS SA is established via TLS handshake, the TLS master key and its child keys, TLS random values, and the TLS ciphersuite negotiated in the TLS handshake are a part of the MIS SA. When an MIS SA is established via EAP execution, a master session key (MSK) or re-authentication master

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

session key (rMSK) and its child keys, MIS random values, and the MIS ciphersuite negotiated between the peer MIS entities are associated with the MIS SA. When an MIS SA is established via group key distribution mechanism using GKB, the master group key and its child keys, and the MIS group ciphersuite indicated to the peer MIS entities are associated with the MIS SA.

MIS service access authentication server: An authentication server used to execute the media independent service (MIS) service access authentication. *See:* **authentication server**.

MIS service access authentication: An authentication process that authorizes the access to media independent services (MISs).

mobile node (MN): Communication node that is capable of changing its point of attachment from one link to another.

neighborhood network: The area of interest in which the network discovery and selection entity seeks to determine the available coverage of a wired/wireless network with identical or different link-layer technologies.

network entity: A communication node inside the network.

network point of attachment (network PoA, or **PoA):** The network-side endpoint of a layer 2 link that includes a mobile node as the other endpoint. *See also:* **candidate PoA**; **serving PoA**; **target PoA**.

network selection: The process by which a mobile node or a network entity makes a decision to connect to a specific network (possibly out of many available) based on a policy configured in the mobile node and/or obtained from the network.

network selector: The entity that undertakes the network selection decisions that can lead to a handover.

network-controlled handover: A handover where the network has the primary control over the handover process.

network-initiated handover: The network initiates the handover process by indicating to the mobile node that the handover is necessary or desired.

node index: A binary string assigned to a node in a group management tree.

node key: A cryptographic key assigned to a node in a group management tree. It is a device key and is shared by multiple devices when the node is not a leaf node.

operator identifier (operator ID): An identifier of the access or core network provider.

perfect binary tree: A binary tree with all leaf nodes at the same depth and all internal nodes having two children.

proactive authentication: A media-specific authentication with the candidate network(s) executed prior to a handover to one of the candidate networks.

protection mechanisms for media independent service (MIS) messages: A protection mechanism that is applied to MIS protocol data unit (PDU) using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combination of an encryption algorithm and an integrity protection algorithm.

protocol implementation conformance statement (PICS) proforma: A normative document to express in compact form the static conformance requirements of a specification. As such, it serves as a reference to the static conformance review.

seamless handover: A handover associated with a link switch between points of attachment, where the mobile node either experiences no degradation in service quality, security, and capabilities, or experiences some degradation in service parameters that is mutually acceptable to the mobile subscriber and to the network that serves the newly connected interface.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

security association identifier (SAID): An identifier of an media independent service (MIS) security association. When an SA is established through Transport Layer Security (TLS), it is the TLS session ID. When an SA is generated through an extensible authentication protocol (EAP) execution, it is assigned by the authenticator and the ID value is an octet string unique for a pair of MIS functions. When an SA is generated via group key distribution mechanism using group key block (GKB), it is assigned by the group manager (GM) and the ID value is an octet string unique for groups of MIS functions.

serving point of attachment (serving PoA): The PoA of the current link being used by the mobile node.

serving PoS: An MIS PoS that is currently providing the MIS services to the mobile node.

soft handover: Handover where facilities for supporting traffic flows are continuously available while the mobile node link-layer connection transfers from the serving point of attachment to the target point of attachment. The network allocates transport facilities to the target point of attachment prior to the occurrence of the link switch event (make-before-break).

static conformance requirement: One of the requirements that specify the limitations on the combinations of implemented capabilities permitted in a real open system, which is claimed to conform to the relevant specification(s).

static conformance review: A review of the extent to which the static conformance requirements are claimed to be supported by the system under test, by comparing the answers in the implementation conformance statement(s) and the system conformance statement with the static conformance requirements expressed in the relevant specifications.

target point of attachment (target PoA): A candidate PoA that has been selected to become the new serving PoA.

two-member group: A group consisting of exactly two members.

uniform resource identifier (URI): A compact sequence of characters that identifies an abstract or physical resource including video.

vertical handovers: A handover where the mobile node moves between point of attachments of different link types, such as from universal mobile telecommunications system (UMTS) to wireless area network (WLAN). *Syn:* **inter-technology handovers**.

4. Abbreviations and acronyms

3G	3rd generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	authentication, authorization, and accounting
ACK	acknowledgement
AES	advanced encryption standard
AID	action identifier
ANDSF	access network discovery and selection function
ANQP	access network query protocol
AP	access point

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved