BSI Standards Publication

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

Part 21-1: Media independent services

bsi.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 8802-21-1:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/6, Data communications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 51418 0

ICS 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-21-1

First edition
2018-04

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

Part 21-1: Media independent services

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

Partie 21-1: Services indépendants des supports

Reference number
ISO/IEC/IEEE 8802-21-1:2018(E)

© IEEE 2017

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

Documents
Document Sharing Hub

© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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 8802-21-1 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.21.1-2017) 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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

IEEE Standard for
Local and metropolitan area networks—

Part 21.1: Media Independent Services

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 February 2017

IEEE-SA Standards Board

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Abstract: Several use cases and services are defined, namely, handover between heterogeneous networks, home energy management system, software-defined radio access networks (SDRANs), radio resource management (RRM), and device-to-device (D2D) communication service that need to be implemented in conjunction with the media independent services (MIS) framework as specified in IEEE Std 802.21™-2017.

Keywords: home energy management system, IEEE 802®, IEEE 802.21™, IEEE 802.21.1™, media independent handover, media independent service, mobile node, mobility, network-assisted device-to-device communication, point of attachment, point of services, radio resource management, seamless, software-defined radio access network, use case

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 7 April 2017. 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.

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

Bluetooth is a registered trademark of the Bluetooth SIG.

cdma2000 is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

W3C is a trademark (registered in numerous countries) of the World Wide Web Consortium; marks of W3C are registered and held by its host institutions MIT, ERCIM, Keio, and Beihang.

Wi-Fi and Wi-Fi Direct are registered trademarks of the Wi-Fi Alliance.

WiMAX and WiMAX Forum are trademarks or registered trademarks of the WiMAX Forum.

PDF: ISBN 978-1-5044-3706-6 STD22402
Print: ISBN 978-1-5044-3707-3 STDPD22402

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Participants

During development of this IEEE standard, the Media Independent Handover Services Working Group had the following officers:

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

At the time this IEEE standard was completed, the 802.21.1 Task Group had the following membership:

Subir Das, *Chair*
Hyeong Ho Lee, *Technical Editor*

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

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

Yusuke Doi
Krzysztof Grochla
Keiichi Teramoto
Torleiv Maseng
Yoichi Masuda
Christian Niephaus
Naoki Ogura
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
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
Thomas Kurihara
Hyeong Ho Lee
Jae Seung Lee
Moon-Sik Lee
Michael Lynch
Elvis Maculuba
Stephen McCann
Michael McInnis
Nick S. A. Nikjoo
Paul Nikolich
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.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Introduction

This introduction is not part of IEEE Std 802.21.1-2017, IEEE Standard for Local and metropolitan area networks—Part 21.1: Media Independent Services.

This standard defines several use cases and services, namely, handover between heterogeneous networks, home energy management system (HEMS), software-defined radio access networks (SDRANs), radio resource management (RRM), and device-to-device (D2D) communication service that need to be implemented in conjunction with the media independent services (MIS) framework as specified in IEEE Std 802.21-2017.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Contents

1. Overview 11
1.1 Scope 11
1.2 Purpose 11
1.3 General 11
1.4 Assumptions 12
1.5 Media independence 12

2. Normative references 13

3. Definitions 14

4. Acronyms and abbreviations 19

5. Media independent handover service 22
5.1 Introduction 22
5.2 General design principles 24
5.3 Deployment example and functional model for MIS services 24
5.4 Single-radio handover procedures 27
5.5 Proxy operations 28
5.6 Media independent event service 35
5.7 Media independent command service (MICS) 35
5.8 Media independent information service 37
5.9 Media dependent SAPs 38
5.10 MIS_LINK_SAP primitives 39
5.11 MIS_SAP primitive 43
5.12 MIS_NET_SAP primitive 84
5.13 MIS protocol messages 88

6. Media independent service for software-defined radio access networks 102
6.1 Introduction 102
6.2 Service scenarios and signaling flows 105
6.3 Service access points (SAPs) and primitives 110
6.4 MIS protocol messages 111

7. Media independent service for home energy management system 111
7.1 Introduction 111
7.2 Service scenarios and signaling flows 112

8. Media independent service for radio resource management 119
8.1 Introduction 119
8.2 Service scenarios and signaling flows 119
8.3 RRM service specific MIS_LINK_SAP primitives 136
8.4 RRM service specific MIS_SAP primitives 138
8.5 RRM service specific MIS protocol messages for command service 145

9. Media independent service for D2D communication 148
9.1 Introduction 148
9.2 Service scenarios and signaling flows 148
9.3 D2D service specific MIS_SAP primitives 159
9.4 D2D service specific MIS protocol messages 162

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Annex A (informative) Bibliography 164
Annex B (informative) Handover procedures 167
Annex C (normative) Mapping MIS messages to reference points 180
Annex D (normative) Media specific mapping for SAPs 181
Annex E (normative) Data type definition 182
Annex F (normative) Information element identifiers 188
Annex G (normative) MIS protocol message code assignments 189
Annex H (normative) Protocol implementation conformance statement (PICS) proforma 192
Annex I (informative) Authentication and key distribution procedures 195
Annex J (informative) Mobile node's network access identifier format 200
Annex K (informative) Network discovery for single-radio handover 201
Annex L (normative) Handover decision 204
Annex M (informative) Practical uses of proxy Information Server 206
Annex N (informative) Certificate revocation list guidelines 207

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

IEEE Standard for
Local and metropolitan area networks—

Part 21.1: Media Independent Services

1. Overview

1.1 Scope

This standard defines several media independent services (MIS); handover, home energy management system (HEMS), software-defined radio access networks (SDRANs), radio resource management (RRM), and device-to-device (D2D) communication that shall be implemented in conjunction with the MIS framework as defined in IEEE Std 802.21™-2017 to optimize the performance of such services.

1.2 Purpose

The purpose of this standard is to describe the media independent use cases and services, and when implemented using the framework described in IEEE Std 802.21-2017, the user experience and management of mobile devices can be greatly improved. The services described in this specification are applicable for interworking between IEEE 802® networks and non IEEE 802 networks (e.g., cellular networks).

1.3 General

This standard describes the following use cases that can be independently implemented using the MIS framework (IEEE Std 802.21-2017), which improves the user experience of mobile devices and management of these devices by operators while mobile devices are either connected or interworking in a heterogeneous networking environment:

— Media independent handover service (Clause 5).

— Media independent service for software-defined radio access networks (SDRANs) (Clause 6).

— Media independent service for home energy management system (HEMS) (Clause 7).

— Media independent service for radio resource management (RRM) (Clause 8).

— Media independent service for device-to-device (D2D) communication (Clause 9).

The handover service use case provides link-layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous networks. This includes media types specified by Third Generation (3G) Partnership Project (3GPP™), 3G Partnership Project 2 (3GPP2), both wired and wireless media in the IEEE 802 family of standards, and downlink-only (DO) media such as Digital Video

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Broadcasting (DVB), Terrestrial Digital Multimedia Broadcasting (T-DMB), and Advanced Television Systems Committee—Mobile/Handheld (ATSC-M/H).[1] The use case addresses the support of handovers for both mobile and stationary users supporting both dual-radio and single-radio mode of operation. For mobile users, handovers can occur when wireless link conditions change due to the users' movement. For the stationary user, handovers become imminent when the surrounding network environment changes, making one network more attractive than another.

The SDRANs use case describes how the MIS framework is used to support the seamless handover in a software-defined radio access network (SDRAN) environment that includes both fronthaul and backhaul networks. The MIS framework enables operators to provide link-layer intelligence, allocate radio resources, and optimize handovers when a mobile device is switching between heterogeneous networks that are managed by a software-defined networking (SDN) controller.

The HEMS use case describes how MIS framework is used to control the devices in a home networking environment for energy management purpose. This use case leverages the media independent command service (MICS) framework and multicast group management capabilities as defined in IEEE Std 802.21-2017.

The RRM service use case describes how MIS framework is used to support resource management in heterogeneous networks. The MIS framework enables mobile node (MN) to monitor its link status (e.g., signal strength and data rate), communicate it to the network, and provide control to its physical layer and data link layers. Leveraging these capabilities, this use case describes how an operator controls and manages the radio resources (e.g., frequency and power) in a heterogeneous networking environment that uses various communication technologies and various frequency bands.

The D2D communication service use case describes how MIS framework is used to provide D2D communication service between MNs that are in close proximity. Using MIS framework, communication service providers and network operators help an MN to search for and connect to its peer when requested. The MN then discovers other MNs in close proximity and connects them using network assistance. Network operators save network resources by offloading data to D2D communication.

This standard also defines additional primitives and messages that are required to support the preceding use cases, which are not specified in IEEE Std 802.21-2017. The configuration and management parameters for all MIS are defined in a MIB, see Annex I of IEEE Std 802.21-2017.

1.4 Assumptions

The following assumptions apply during a single-radio handover for a device that has two or more radios:

a) In a single-radio scenario, the mobile device transmits on only one radio at a time. The target radio shall not transmit while the source radio is transmitting.

b) While the source radio is receiving, the target radio shall not transmit in a manner causing interference to the source radio receiver.

c) Prior to handover completion, only the source radio link is used to carry data.

1.5 Media independence

This standard, in conjunction with IEEE Std 802.21-2017, is intended to provide a generic interface between higher layer protocol stack and existing media-specific link layers, such as those specified by 3GPP, 3GPP2, the IEEE 802 family of standards, and downlink-only media.

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

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

The handover use case uses service access points (SAPs) and primitives that provide generic link-layer intelligence. Individual media-specific technologies thereafter need to enhance their media-specific SAPs and primitives to satisfy the generic abstractions of this standard. Suitable adaptations are required to existing lower layer [medium access control (MAC) layer and physical (PHY) layer] standards of different media-specific technologies such as IEEE Std 802.3™-2015, IEEE Std 802.11™-2012, IEEE Std 802.16™-2012, 3GPP, 3GPP2, and DVB to satisfy the requirements of generic link-layer intelligence identified by this standard.[2]

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.

IEEE Std 802.1Q™-2014, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.[3, 4]

IEEE Std 802.3™-2015, 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.

IEEE Std 802.21™-2017, IEEE Standard for Standard for Local and metropolitan area networks—Part 21: Media Independent Services Framework.

IETF RFC 3748 (2004-06), Extensible Authentication Protocol (EAP).[5]

IETF RFC 4140 (2005-08), Hierarchical Mobile IPv6 Mobility Management (HMIPv6).

IETF RFC 4857 (2007-06), Mobile IPv4 Regional Registration.

IETF RFC 4881 (2007-06), Low-Latency Handoffs in Mobile IPv4.

IETF RFC 5268 (2008-06), Mobile IPv6 Fast Handovers.

IETF RFC 5944 (2010-10), IP Mobility Support for IPv4, Revised.

IETF RFC 6275 (2011-07), Mobility Support in IPv6.

[2] Information on references can be found in Clause 2.
[3] IEEE publications are available from the Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).
[4] The IEEE standards or products referred to in Clause 2 are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.
[5] IETF documents (i.e., RFCs) are available for download at http://www.rfc-archive.org/.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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. [6]

authentication process: A process to assure that the claimed identity belongs to the entity. It is also called *entity authentication*.

NOTE—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).[7]

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

bidirectional network: A general communication network providing bidirectional transmission such as IEEE 802.3, IEEE 802.11, IEEE 802.16, 3GPP, and 3GPP2.

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

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

candidate point of service (PoS): A potential PoS that serves the mobile nodes (MNs) after movement.

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

downlink-only (DO) network: A broadcasting network providing unidirectional transmission from the point of attachment (PoA) to the user device, such as digital video broadcasting (DVB), terrestrial-digital media broadcast (T-DMB), and advanced television system committee mobile handheld (ATSC-M/H).

dual-radio operation: In this mode a dual-radio device is capable of receiving and transmitting simultaneously on both the radios. Since both radios are active simultaneously in these types of devices, the target radio connects with the target network to prepare the target network for handover. The source radio maintains connection with the source network during the handover. *See also:* **single-radio operation**.

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

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

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 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.

[6] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org.
[7] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

MIS_Push_Group_Manipulate

handover: The process by which a mobile node (MN) 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 (PoA) 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**.

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

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).

home subscriber network: Network managed by an operator with whom the subscriber has a business relationship (subscription). *See also:* **visited network; serving network**.

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

NOTE—UMTS is a trademark of The European Telecommunications Standards Institute (ETSI).

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.

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

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.

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 (MN) 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 MN.

lower layers: The layers located at OSI Level 2 and below across different link-layer technology standards supported by this standard, IEEE Std 802.21.1-2017. 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), L1/LAPDm in the case of GSM CS, and L1/MAC/RLC in the case of general packet radio service (GPRS)/Enhanced GPRS (EGPRS), respectively. The term *lower layers* also includes Logical Link Control Layers such as IEEE 802.2™ Logical Link Control (LLC) or 3GPP Radio Link Control (RLC). The media independent service function (MISF) uses the services provided by these layers.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

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

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

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

media independent service (MIS) node: A media independent service function (MISF) capable entity [mobile node (MN) 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 (MN).

media independent service point of service (MIS PoS): Network-side MISF instance that exchanges MIS messages with a mobile node (MN)-based MISF. The same MIS Network Entity includes an MIS PoS for each MIS-enabled MN 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 PoSs capable of providing different combinations of MIS services to the respective MNs 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 independent service (MIS) users: Entities that use the services provided by the MISF. MIS users use the MIS_SAP to interact with the MISF.

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

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

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

multimedia program (MMP): An instance of certain content (e.g., voice, data, or video) with some specific attributes, e.g., chapter 2 of a TV series.

multimedia service (MMS): A sequence of multimedia programs (MMPs) under the control of a content aggregator and provider, e.g., TV Channel One, TV Channel Two.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

network detection: The process by which a mobile node (MN) collects information on networks in its locality, identifies the different points of attachment, and ascertains the validity of link-layer configuration.

network entity: A communication node inside the network.

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

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

network selection: The process by which a mobile node (MN) 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 MN and/or obtained from the network.

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

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.

preregistration: Preparatory handover signaling (possibly including security establishment) that is accomplished before the handover actually occurs.

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

proxy information server: A server that assists the mobile node (MN) to obtain the required information when a query is made via the source network. To the MN, the proxy information server appears to be an information server of the source network.

proxy point of attachment (PoA): An entity that provides service to a mobile node (MN) and a target PoA via the source network. To the MN, this entity appears to be a PoA in the target network. In some scenarios, it is a non-PoA network entity that is collocated at a media independent service (MIS) point of service (PoS), and it enables such services as preregistration of the MN.

seamless handover: A handover associated with a link switch between points of attachment (PoAs), where the mobile node (MN) 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.

serving network: A network that provides services to the user. The serving network can be a home subscriber network or a visited network. *See also:* **home subscriber network; visited network**.

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

serving point of service (serving PoS): A media independent service (MIS) PoS that is currently providing the MIS services to the mobile node (MN).

single-radio handover: A handover between (possibly heterogeneous) radio access technologies (RATs) during which a mobile node (MN) transmits over only one radio link at a time.

single-radio handover (SRHO)-capable node: A media independent service function (MISF) capable node that processes single-radio MIS packets.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

single-radio MIS packet: A packet that may contain one or more of the following commands—MIS_Prereg_Xfer, MIS_N2N_Prereg_Xfer, MIS_Prereg_Ready, or MIS_CTRL_Transfer—in its payload.

single-radio operation: In this mode, a dual-radio device is capable of receiving and transmitting on only one radio at a time. This is usually the mode of operation when radio frequencies of the two radios are close to each other (e.g., in IMT 2000 bands). Since only one radio is active at a time in these types of devices, the source radio uses the back-end connection of the source network with the target network to prepare the target network for handover while maintaining the client-side connections. Once the target preparation is complete the device switches from source radio to target radio. Since all the target preparation has been completed a priori, the target radio quickly establishes connectivity with the target network and all the connections are then transferred from source network to target network. *See also:* **dual-radio operation**.

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 (PoA) to the target PoA. The network allocates transport facilities to the target PoA prior to the occurrence of the link switch event (make-before-break).

source network PoS: The point of service (PoS) in the network of the mobile node's (MN's) current point of attachment (PoA).

source radio: The mobile nodes's (MN's) radio interface that transmits and/or receives over the radio link that the MN currently has established with the source network.

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 network PoA: A point of attachment (PoA) in the target network, to which a mobile node (MN) will be attached after a handover has been completed.

target network PoS (TPoS): A point of service (PoS) in the target network of the target point of attachment (PoA) that will serve a mobile node (MN) after a handover has been completed.

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

target radio: The mobile node's (MN's) radio interface that will transmit and/or receive information with the target network over the radio link.

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 (MN) moves between points of attachment (PoAs) of different link types, such as from universal mobile telecommunications system (UMTS) to wireless area network (WLAN). *Syn:* **inter-technology handovers**.

visited network: A network managed by an operator other than the subscriber's home operator and in which the subscriber is receiving service. *See also:* **home subscriber network**; **serving network**.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

4. Acronyms and abbreviations

3G	3rd generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	authentication, authorization, and accounting
AID	action identifier
ANDSF	access network discovery and selection function
ANQP	access network query protocol
AP	access point
ATSC-M/H	advanced television system committee mobile handheld
BS	base station
CA	certificate authority
CN	core network
CRL	certificate revocation list
D2D	device to device
DHCP	dynamic host configuration protocol
DO	downlink only
DVB	digital video broadcasting
EAP	extensible authentication protocol
FA	foreign agent
GKB	group key block
GM	group manager
GPRS	general packet radio service
GSM	global system for mobile communication
HEMS	home energy management system
HGW	home gateway
HPoS	home network point of service (PoS)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet protocol
IPsec	IP security
IPTV	IP television
IS	information service
ITU	International Telecommunications Union
L1	layer 1 (PHY)
L2	layer 2 (MAC and/or LLC)

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

L3	layer 3
LAN	local area network
LLC	logical link control
LTE	long term evolution
MAC	medium access control
MIAK	media independent authentication key
MIB	management information base
MICS	media independent command services
MIES	media independent event services
MIIS	media independent information service
MIP	mobile IP
MIS	media independent service
MISF	media independent service function
MISK	media independent session key
MLME	MAC layer management entity
MMP	multimedia program
MMS	multimedia service
MN	mobile node
MSK	master session key
MSPMK	media specific pairwise master key
MSRK	media specific root key
N/A	not applicable
NADC	network-assisted D2D communication
NAI	network access identifier
PAC	peer aware communication
PDU	protocol data unit
PHY	physical layer
PMIP	proxy mobile IP
PoA	point of attachment
PoS	point of service
PRF	pseudorandom function
ProSe	proximity services
PV	photovoltaics
QoE	quality of experience
QoS	quality of service
RAN	radio access network
RAT	radio access technology

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

RDF	resource description framework
RFC	request for comment
RLC	radio link control
rMSK	re-authentication master session key
RP	reference point
RRM	radio resource management
SA	security association
SAP	service access point
SDN	software-defined networking
SDO	standards development organization
SDRAN	software-defined radio access network
SID	service identifier
SINR	signal over interference plus noise ratio
SLA	service level agreement
SP	service provider
SPoS	source network point of service (PoS)
SRHO	single-radio handover
TCP	transmission control protocol
T-DMB	terrestrial-digital media broadcast
TLS	transport layer security
TLV	type length value (a form of encoding, or an item encoded using that coding)
TPoA	target network point of attachment (PoA)
TPoS	target network point of service (PoS)
UDP	user datagram protocol
UMTS	universal mobile telecommunications system
URI	uniform resource identifier
URL	uniform resource locator
WLAN	wireless local area network
WPAN	wireless personal area network
XML	extensible mark-up language

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5. Media independent handover service

5.1 Introduction

5.1.1 General

This use case supports different handover methods. Such methods are generally classified as “hard” or “soft,” depending on whether the handover procedure is “break-before-make” or “make-before-break” with respect to the data transport facilities that support the exchange of data packets between the MN and the network.

Handover decision making involves cooperative use of both MN and network infrastructure. Handover control, handover policies, and other algorithms involved in handover decision making are generally handled by communication system elements that do not fall within the scope of this standard. However, it is beneficial to describe certain aspects of the overall handover procedure so that the role and purpose of the MIS services in the handover process are clear. The following subclauses give an overview of how the different factors that affect handovers are addressed within this standard.

5.1.2 Service continuity

Service continuity is defined as the continuation of the service during and after the handover while minimizing aspects such as data loss and duration of loss of connectivity during the handover without requiring any user intervention. The change of access network need not be noticeable to the end user. However, irrespective of that, there should be no need for the user to re-establish the service. There can be a change in service quality as a consequence of the transition between different networks due to the varying capabilities and characteristics of the access networks. For example, if the quality of service (QoS) supported by the new access network is unacceptable, higher layer entities decide not to handover or terminate the current session after the handover based on applicable policies. This standard specifies essential elements that enable service continuity.

5.1.3 Network discovery

This standard defines the information that helps in network discovery and specifies the means by which such information shall be obtained and be made available to the MIS users. The network information includes information about link type, link identifier, link availability, link quality, etc.

5.1.4 Network selection

Network selection is the process by which an MN or a network entity selects a network (possibly out of many available) to establish network-layer connectivity. The selection is based on various criteria such as required QoS, cost, user preferences, or the network operator’s policies. This standard specifies means by which such information shall be made available to the MIS users to enable effective network selection.

5.1.5 Handover policy

The primary role of the media independent service function (MISF) is to facilitate handovers and provide intelligence to the network selector entity. The MISF aids the network selector entity with the help of the

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

event service, command service, and information service. The network selector entity and the handover policies that control handovers are outside the scope of this standard.

5.1.6 Media independent single-radio handover

In single-radio handover, the opportunities to deliver handover messages are limited. To improve single-radio handover performance, it is important to accomplish as much of the handover signaling (including security establishment) before the handover actually occurs; this preparatory signaling is called *preregistration*. The exact signaling steps included in the preregistration process may depend on the requirements of the target network and is independent of the signaling nature of the source network. As a general rule, preregistration typically involves one or more of the following steps, which are often needed for handovers:

— Proactive authentication—that is, authenticating the MN before it arrives in the target network

— Address allocation—one or more Internet protocol (IP) addresses to be used by the MN after it arrives in the target network

— Data path setup—establishing tunnels and forwarding entries for the MN in the target network

— Context establishment—building all necessary state information such as QoS parameters and access permissions within target network entities

Each of these operations is often time-consuming. If they have to be carried out after the MN moves into the coverage area of the target network radio access, seamless session handover for many applications would be impossible. This is due to the break-before-make dead time before packets could start flowing again via the target network. Moreover, it shall be possible to carry out each of the operations securely to prevent hijacking attempts or mismanagement of target network resources. As long as handovers occur only between access points within the same operator network, it is often possible to guarantee that signaling packets are never exposed to attack. In contrast, for access networks belonging to different operators, the data path between neighboring access points of serving and target access networks are more likely to traverse the Internet, potentially exposing preregistration signaling to attack.

5.1.7 Enabling fast authentication using PoS for single-radio handover

Enabling movement between the networks of roaming partners for single-radio smart phones and Internet-enabled wireless devices can be facilitated by enabling preregistration via the point of service (PoS) and making use of certain functions as developed in 3GPP (TS23.401 [B4]), 3GPP2 (C.S0001-D [B9]), and the WiMAX Forum® [B49].[8, 9] Using the PoS, signaling messages related to security information between roaming partners are exchanged, and as a result low-latency optimized session handover is achievable. Communications between the source and target networks shall be secured. However, authentication has been typically quite time-consuming because of reliance on distant authentication agents. A method is defined to establish a secure communication channel between source and target networks as part of handover preregistration procedures (see 5.5.4.1). Improving the security model and reducing authentication delay enables improvements in handover performance, because single-radio systems are not capable of taking advantage of parallel authentication operations.

[8] WiMAX Forum is a registered trademark of the WiMAX Forum.
[9] The numbers in brackets correspond to those of the bibliography in Annex A.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.2 General design principles

5.2.1 Single-radio handover MISF design principles

The following are functional requirements that facilitate single-radio handover between possibly heterogeneous radio access technology (RAT) networks:

a) Tunneling mechanism to deliver the preregistration messages

b) Control for preregistration states and delivery for preregistration contexts

5.3 Deployment example and functional model for MIS services

5.3.1 Deployment example for MIS services

A network model including MIS services is shown in Figure 1 to better illustrate the MIS reference points (see 5.4.2 of IEEE Std 802.21-2017). Moving from left to right, the model includes an MIS-capable mobile node (MN, far left) that supports multiple wired and wireless access technologies. The model assumes that the serving network either operates multiple link-layer technologies or allows its user to roam into other networks when a service level agreement (SLA) in support of inter-working has been established.

The model illustrates access networks that are connected in some loose, serial way to a given core network (CN) (i.e., Core Operator 1, 2, or 3). Also depicted is an access network that is more tightly coupled (Access Network-3). Not depicted in Figure 1, an access network can also connect to a CN via the Internet. Each Core Operator network (1, 2, or 3) might represent a service provider, corporate intranet provider, or just another part of the visited or home access. In this depicted model, the provisioning provider is operating Access Network-3, which couples the terminal to the core (labeled Home Core Network) via reference point RP1. At any given point in time, the subscriber's serving network can be the home subscriber network or a visited network.

The network providers offer MIS services in their access networks (Access Network 1 to 4) in order to facilitate heterogeneous handovers into their networks. Each access technology either advertises its MIS capability or responds to MIS service discovery. Each service provider for these access networks allows access to one or more MIS Points of Service (PoS) node(s). These PoS nodes provide some or all of the MIS services as determined during the MIS capabilities discovery. The PoS location varies based on the operator deployment scenario and the technology-specific MIS architecture.

An MIS PoS resides next to, or is co-located with, the point of attachment (PoA) node in the access network (e.g., Access Network 1, 2, 4). Alternatively, the PoS can reside deeper inside the access or core networks (e.g., Access Network 3). As shown in Figure 1, the MIS entity in the MN communicates with MIS network entities using reference points RP1, RP2, or RP3 over any of the available access networks. If the PoA in the serving access network has a co-located MISF, the RP1 reference point terminates at the PoA that is also the PoS (MN to Access Network 1, 2, 4 of the model can all be RP1). In that case, an RP3 reference point would be terminated at any non-PoA (illustrated by MN connectivity to Access Networks 1, 2, 4). MIS events originate at both sides of an active RP1 link. The MN is typically the first node to react to these events.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

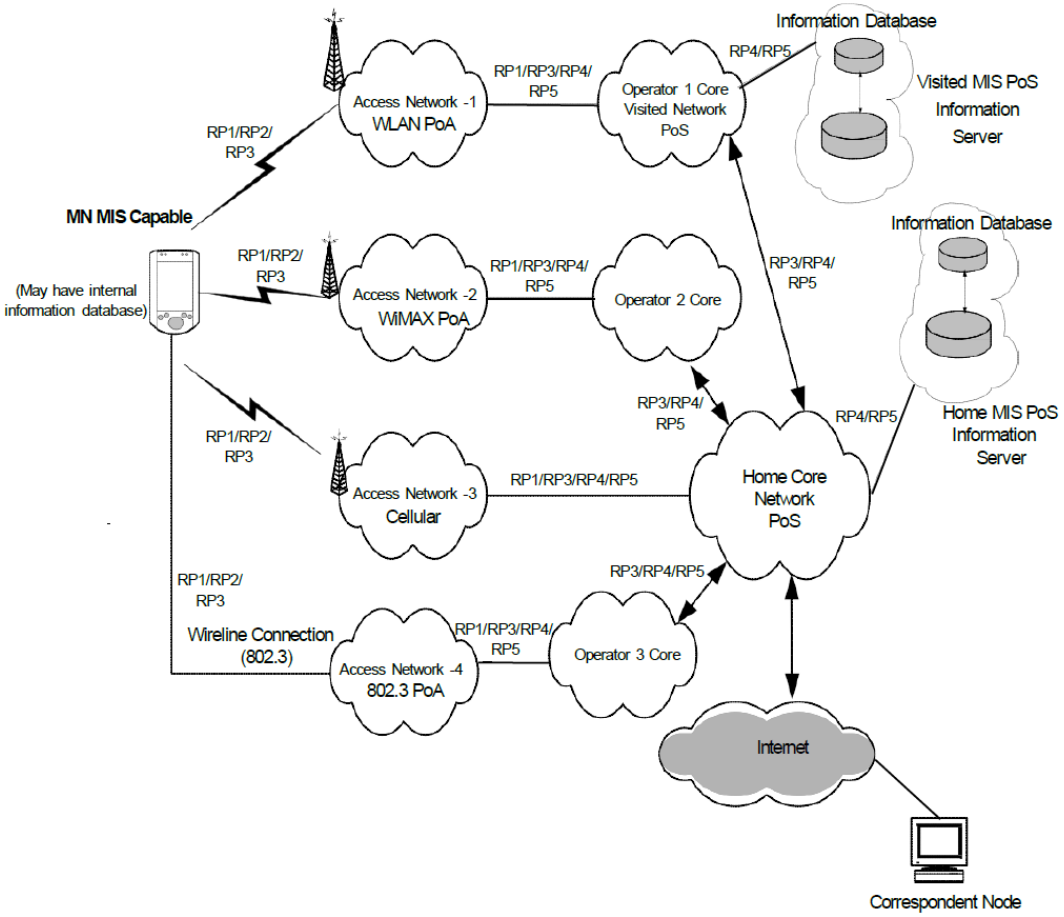

Figure 1—Example of network model with MIS services

The interaction of visited and home subscriber networks could be either for control and management purposes or for data transport purposes. It is also possible that due to roaming or SLA agreements, the home subscriber network allows the MN to access the public Internet directly through a visited network. As illustrated, two MIS network entities communicate with each other via RP4 or RP5 reference points. The MIS-capable PoA communicates with other MIS network entities via RP4 and RP5 reference points. The MIS-capable MN have MIS communication with other PoA in the candidate access networks via the RP2 reference point to obtain information services about the candidate network.

With regard to the MIS information service, visited providers offer access to their Information Server located in an MIS PoS node (upper far right). The operator provides the media independent information service (MIIS) to MNs so they can obtain pertinent information including, but not limited to, new roaming lists, costs, provider identification information, provider services, priorities, and any other information that would enable the selection and utilization of these services. As illustrated, it is possible for the MN to be pre-provisioned with MIIS data by its provider. It is also possible for the MN to obtain MIS information services from any access network of its service provider or from visited networks that maintain SLA agreements with the MN's service provider. MIIS can also be available from another overlapping or nearby visited network, using that network's MIIS point of service. The serving network utilizes RP4 and RP5 interfaces to access other MIS entities. As an example, in Figure 1 the home subscriber network accesses its own MIS Information Server or core operator 1 (visited network) MIS Information Server.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.3.2 Single-radio handover MISF relationship to reference model

To prepare for handover, the MN may exchange link-layer protocol data units (PDUs) with the target network PoA through a communication link that is established between an MN and the target PoA using the active network connection. These PDUs contain the same information as in the PDUs that would be exchanged if the target links were active. There is no guarantee that the target link is accessible during a single-radio handover. A proxy PoA is used to enable the MN and the target PoA to exchange link-layer PDUs.

During a single-radio handover, an L2 frame may be encapsulated in a MIS message, which is then exchanged via an active link between the MISFs of a local and a remote node using MIS protocol over higher layer transport [transmission control protocol (TCP) or user datagram protocol (UDP) over IP].

5.3.3 Single-radio handover functional model and signaling flow

The functional model for single-radio handover is shown in Figure 2.

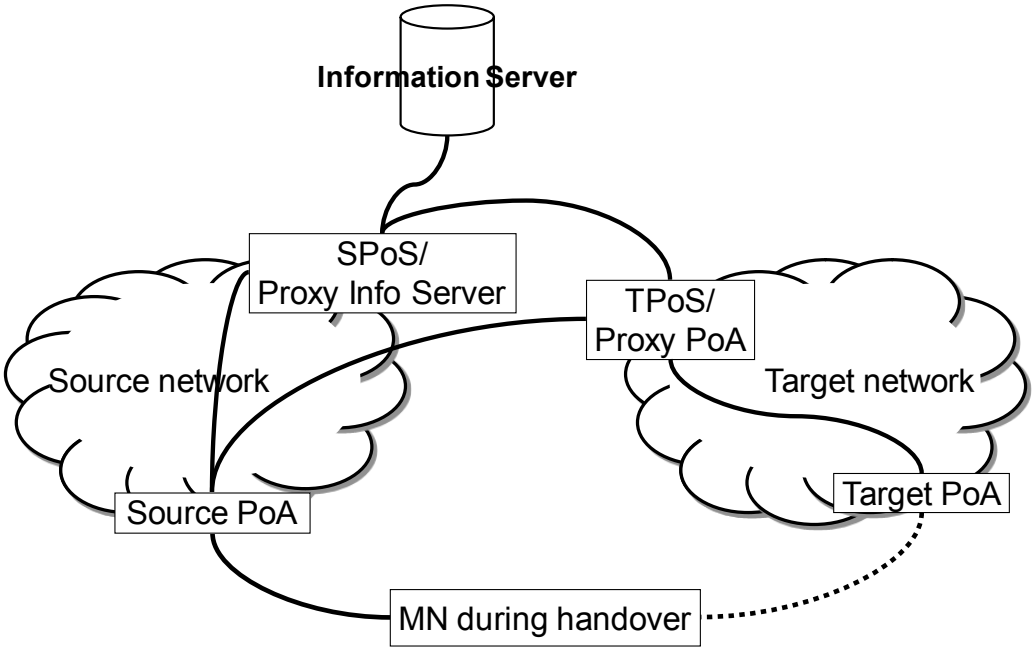

Figure 2—Single-radio handover functional model

In the preceding scenario, the source network PoS (SPoS) is providing the service to the source network users, in which the proxy Information Server (see 5.5) is co-located. Source network users are connected via source PoA. The target network PoS (TPoS) belongs to the target network and provides the service to the target networks users that are connected via target PoA. It is not always necessary that a source PoA and a target PoA need to be served by two different PoSs. A PoS may cover a plurality of networks. In that case, the source PoS and TPoS are collocated and an MN performs handover from the source PoA to the target PoA using the same PoS. This scenario is captured in Figure 1 (5.3.1).

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.4 Single-radio handover procedures

A single-radio handover following the reference model in 5.3.2 consists of various handover procedures and involves different information elements (5.9, 5.10, 5.11, and 5.12) and messages (5.13). Examples of handover are described in Annex B. Figure 3 shows the single-radio handover process consisting of the following five procedures:

a) **Network discovery** enables the MN to determine whether or not there is a candidate target network available for handover. Network discovery may involve the following:

   1) The MN may query the Information Server to discover candidate networks and their handover policies. Such information includes whether candidate networks and MN support single-radio handover (SRHO) or not, and the availability of proxy services on the candidate network. Network discovery also allows the MN to acquire the corresponding system information blocks for candidate points of attachment (candidate PoAs) to perform the radio measurements.

   2) The MN may request that the source network PoS identify one or more candidate target networks.

   3) During idle times when the source radio is not in use, the MN may activate its target radio to scan for one or more reachable TPoAs.

b) The **handover decision** may involve the following:

   1) A handover trigger, which may be a command

   2) Target network selection

   3) Proxy services discovery

   4) Evaluating the handover benefit: the evaluation is made by either the MN or the network, e.g., based on parameters such as signal strength, target quality of experience, cost, and operator policy

c) **Preregistration** includes pro-active authentication and establishing context (user identity, security, resource information) at the target network. With the help of proxy services, the MN performs preregistration procedures within the target network while still retaining its data connection with the source network. Optionally, the preregistration procedure may occur before the handover decision procedure as in the case of WiMAX™ target networks. [10]

b) During **target link preparation,** the MN and target network prepare the establishment of the target link. This procedure ascertains whether the target network has enough resources to accommodate the new link and may include performing resource reservation or admission control as well as confirming that the signal conditions are favorable enough to establish the target link.

c) Finally, during **SRHO execution**, the source link is disconnected, the target radio is activated, and the target link is established. The association of the network layer address to the link-layer address will change from the source link-layer address to the target link-layer address for IP-based mobility management, and future incoming packets are then routed to the target radio.

[10] WiMAX is a trademark of the WiMAX Forum.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

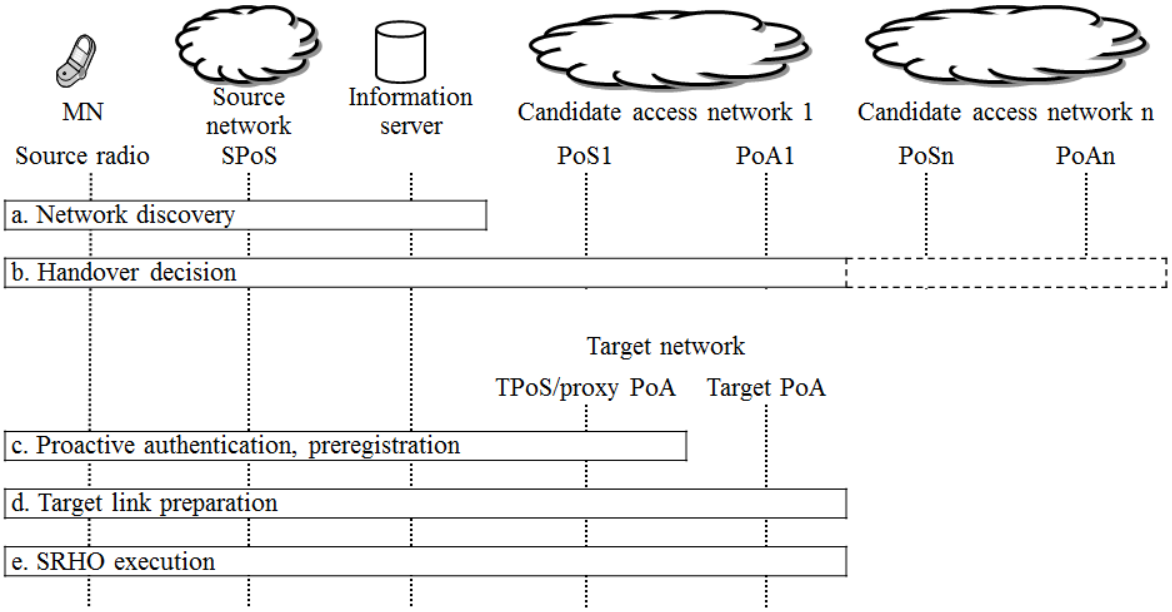

Figure 3—Single-radio handover procedures

5.5 Proxy operations

5.5.1 Introduction

The signaling between the MN and the target network via the source network or between the MN and the Information Server can be accomplished through proxy services. In single-radio handover, the MN sends signal to the proxy PoA as if signaling to the target PoA (TPoA), and the TPoA responds by signaling to the proxy PoA as if signaling to the MN. The MN sends signal to the proxy Information Server as if signaling to the Information Server, and the Information Server responds by signaling to the proxy Information Server as if signaling to the MN.

In a WiMAX network, the proxy services may be implemented as an extension of the Signal Forwarding Function (SFF) (WiMAX Forum [B49]) and may reside at the Access Service Network Gateway (ASN-GW).

In a 3GPP network, the proxy services may be implemented as an extension of the Mobility Management Entity (MME) (3GPP TS23.401 [B4]).

In a 3GPP2 network, the proxy services may be implemented in the High-Rate Packet Data Signal-Forwarding Function (HRPD-SFF) and the existing functions of the Packet Control Function (PCF) (3GPP2 C.S0001-D [B9]).

In a network employing a centralized or distributed mobility management architecture, the proxy services may be collocated within the mobility management anchors (IETF [B24]).

Signaling between the MN and the proxy service may be accomplished in a media independent manner using the functions of the source network PoS and the target network PoS (TPoS) and the signaling messages defined in this specification.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.5.2 Network discovery using proxy Information Server

The MN may need to communicate with the Information Server to discover a target access network. If the MN directly accesses the Information Server, it discovers its target network by using MIS_Get_Information request and response messages. However, the MN may not always be able to directly access the Information Server, and the MN and the Information Server may be located in different networks and in different administrative domains. For example, the MN may need to query via access network query protocol (ANQP) messages in a Wi-Fi® access network while the information is available in an access network discovery and selection function (ANDSF) server that is located in a cellular provider's network.[11] Network discovery in this scenario is accomplished if the Wi-Fi PoA is SRHO-capable, and an intermediate entity called *proxy Information Server* is available to forward the MN's request to the ANDSF server.

Figure 4 shows an example call flow of the network discovery process using a proxy Information Server. The goal of the MN is to discover the target network. The steps of the discovery process are as follows:

a) The MN requests information about the target network using MIS_CTRL_Transfer request or a non-MIS message such as ANQP query.

b) The SRHO-capable PoA transmits the MIS_CTRL_Transfer request message to the proxy Information Server. If the SRHO-capable PoA received a non-MIS message in step a), the SRHO-capable PoA encapsulates the query message into the MIS_CTRL_Transfer request message and transmits the message to the proxy Information Server (see 5.11.14).

c) The proxy Information Server extracts a non-MIS message (e.g., ANQP query) from the MIS_CTRL_Transfer request message, and then exchanges signaling with the Information Server by using the extracted non-MIS message. Note that signaling (e.g., ANQP and ANDSF) between the proxy Information Server and the Information Server is out of the scope of this specification.

d) The proxy Information Server transmits a MIS_CTRL_Transfer response message to the SRHO-capable PoA by encapsulating the response that is obtained from the functional entity (i.e., MIS user).

e) The SRHO-capable PoA responds to the MN with information about the target network using MIS_CTRL_Transfer request or a non-MIS message such as an ANQP response. In case the MN did not use MIS as the protocol to transmit the original query, the SRHO-capable PoA decapsulates the MIS_CTRL_Transfer response message and forwards the content (e.g., the ANQP response) to the MN. If the MN used the MIS protocol for the initial query, then the SRHO-capable PoA forwards the MIS_CTRL_Transfer response message to the MN.

Use cases of the proxy Information Server are included in Annex M.

[11] Wi-Fi is a registered trademark of theWi-Fi Alliance.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

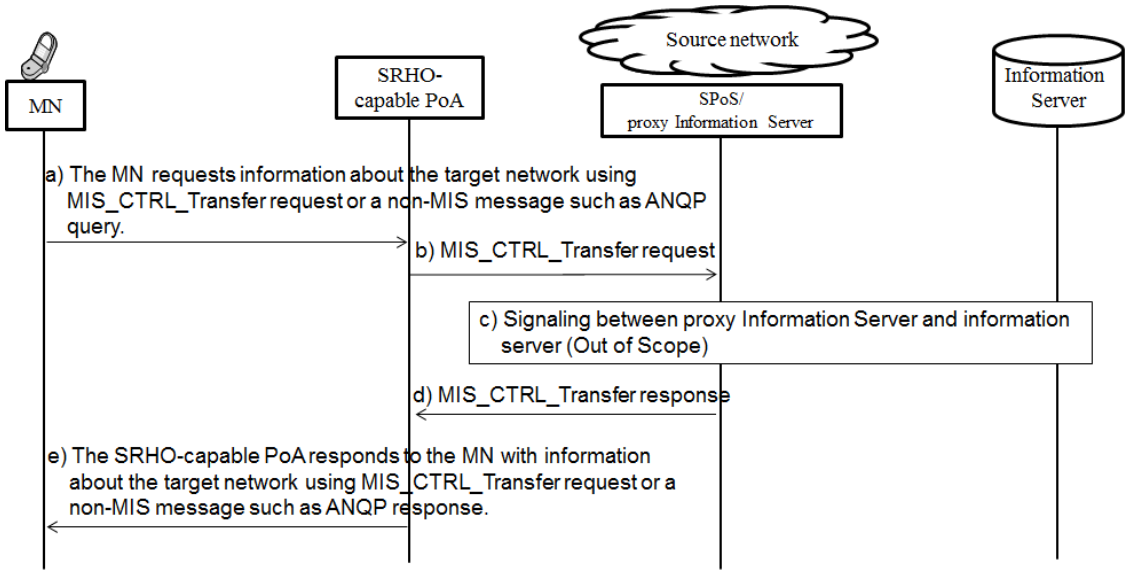

Figure 4—Network discovery using a proxy Information Server

5.5.3 Preregistration using proxy PoA

To prepare for handover, the MN needs to communicate with the target network PoA (TPoA) by performing a network access procedure with the target access network. The first part of this communication is the transport of TCP or UDP/IP packets to the proxy PoA (Figure 5 and Figure 6). The second part of this communication depends on whether the TPoA is SRHO-capable (Figure 5) or whether it is a legacy PoA lacking such capability (Figure 6). If the target PoA is SRHO-capable, the L2 frame is encapsulated into a MIS packet to be forwarded to the target radio.

Figure 5 shows the transport of the target radio control frame as a payload of a MIS packet between the MN and the proxy PoA via the source radio interface since the target radio link is unavailable. In this figure, the MN has 2 interfaces (1) and (2). It uses the wireless interface (1) with PHY_1 and $L2_1$ to connect to the source network. The MN uses reference point 1 (RP1) (see Figure 3 in 5.4.2 of IEEE Std 802.21-2017) to communicate with TPoS / proxy PoA via network layer transport.

If the target radio were used, the MN would have used the target radio with protocol stack PHY_2 and $L2_2$ to communicate with the TPoA, which also implements the corresponding protocol stack PHY_2 and $L2_2$. Without using the target radio to communicate, the target radio link-layer control frame $L2_2$ is encapsulated into a MIS packet. The TPoS/proxy PoA communicates with the SRHO-capable TPoA using reference point 5 (RP5) (see Figure 3 in 5.4.2 of IEEE Std 802.21-2017) over network layer transport. When the MIS packet arrives at the SRHO-capable TPoA, it is decapsulated to retrieve the target $L2_2$ frame.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

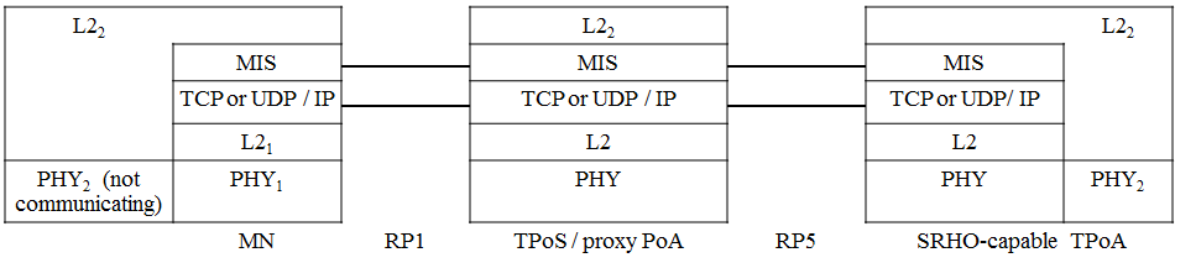

Figure 5—Transport of the L2 frame of the target interface via a MIS using the logical connection at the TPoS to the SRHO-capable TPoA

Figure 6 also shows the transport of the target radio L2 control frame as a payload of a MIS packet between the MN and the proxy PoA via the source radio since the target radio link is unavailable. However, since the TPoA is not SRHO-capable, the MIS user at the proxy PoA has to communicate with the TPoA using other mechanisms that are out of scope of this specification.

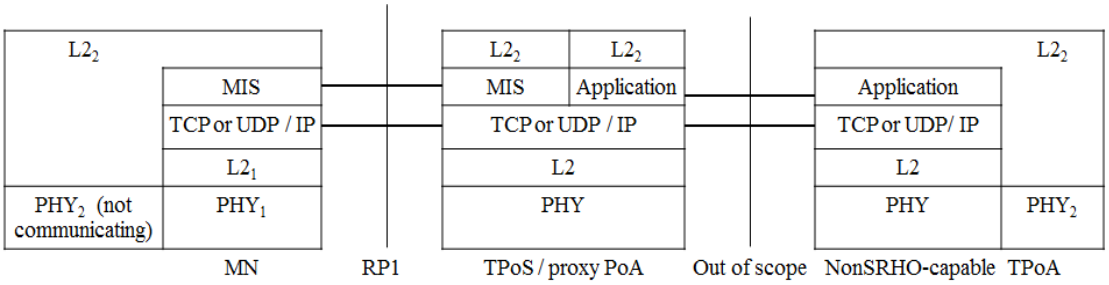

Figure 6—Transport of L2 frame via the proxy PoA to a legacy TPoA that is not SRHO-capable

The procedures of communication between the MN and the TPoA are shown in Figure 7 and are as follows:

a) The MN sends a message to the SPoS or directly to the TPoS/proxy PoA with a payload containing a target network L2 handover frame. If the message is directly sent to the TPoS/proxy PoA, the SPoS is bypassed. If the message is sent to the SPoS, the SPoS will forward the message to the TPoS/proxy PoA.

b) Upon receiving this message from the MN, the TPoS/proxy PoA helps to discover a suitable TPoA if not already known. It will determine whether the target PoA is SRHO-capable. If not, the TPoS / proxy PoA will communicate the link-layer frames to the target PoA using a mechanism that is outside the scope of this specification.

   1) The TPoS or proxy PoA signals with this TPoA using MIS message if the TPoA is a SRHO-capable node (the target PoA supports MIS_Prereg_Xfer messaging).

   2) Otherwise, the proxy PoA signals with the candidate target PoA using other L2-specific protocol messages. SPoS will relay the reply messages to MN, indicating whether the L2 preregistration signaling is successful. Also, the reply will include an indication of the fact that the messages used for the proxy PoA to signal with the TPoA are outside the scope of this document. L2 frames are passed to the target PoA either by way of proxy PoA or by MIS_Prereg_Xfer commands.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

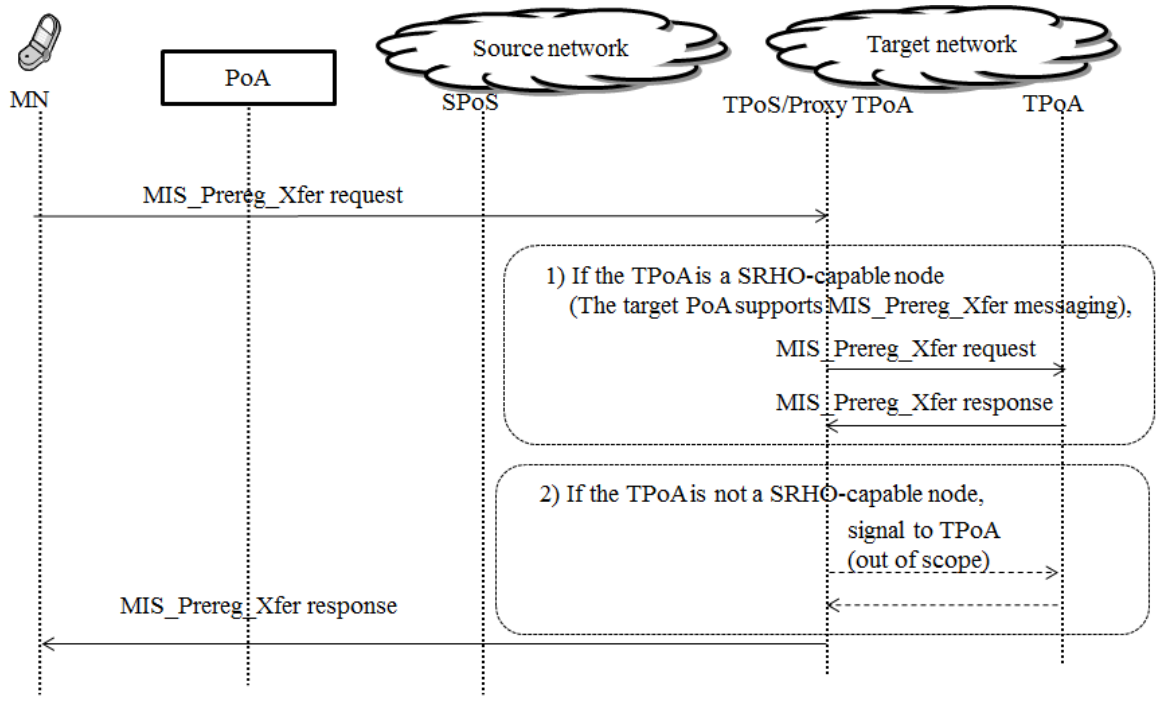

Figure 7—Communication between the MN and the TPoA

As previously shown, the MN and the target network exchange link-layer PDUs without using the target PoA's physical radio channel. The exchanged single-radio control frames are processed by the MISF, which receives them at port 4551, the assigned transport layer protocol's port number (IETF [B26]).

5.5.4 PoS facilitated proactive authentication for single-radio handover service

For single-radio handover, it is desired to conduct proactive authentication for preregistration to reduce the latency brought about by the authentication required to be attached to the target network. The PoS is a convenient and natural place to facilitate such proactive authentication. The security protections are needed between different PoS modules to transmit authentication credentials.

5.5.4.1 Establishing MIS Security Association between roaming partners

It is out of scope for this document to specify exactly how the secure communication channel should be established. The specific method shall be agreed upon as a part of the roaming agreement. For example, the certificate of the trusted certificate authority (CA) shall be configured so that it is established on demand by using IKEv2 (IETF RFC 7296 [B37]). The following overview describes some circumstances enabling dynamic establishment of security association between the SPoS and the TPoS.

MIS_Prereg_Xfer and MIS_N2N_Prereg_Xfer messages exchanged between the SPoS and the TPoS may require security protection. Furthermore, the TPoS may reject these messages from an unauthorized source network PoS. To protect the link between the SPoS and the TPoS, several approaches are possible.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

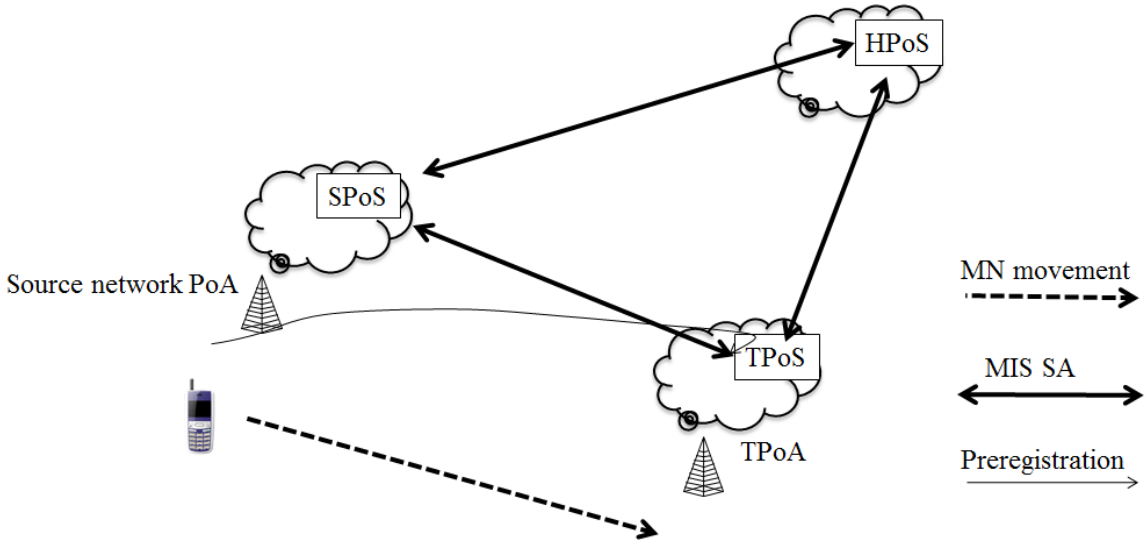

Figure 8—MN handover signaling for preregistration using SPoS

An MIS SA (Security Association) (see 8.4.2 of IEEE Std 802.21-2017) is used for protecting the communications between an SPoS and a TPoS. In this case, the SPoS acts as the initiating end-point of an MIS SA and a TPoS as the other end-point of the MIS SA. The MIS SA is established using (datagram) transport layer security [(D)TLS] over MIS or extensible authentication protocol (EAP) over MIS (see 9.2 of IEEE Std 802.21-2017).

Other mechanisms for providing message integrity and confidentiality, such as IP security (IPsec) and transport layer security (TLS) over TCP, can also be used for protecting the communications between SPoS and TPoS.

Except for the initial network attachment, by the time an MN enters a network, it can also have a security relationship with the PoS in that network by using MIS_Prereg_Xfer commands. For each newly visited network, this security relationship is created on demand, enabled by signaling from another PoS. The PoS creating the visited security relationship can either be the MN's home PoS (HPoS, a PoS in MN's home network) or the PoS in the network previously visited by the MN. When the MN first attaches to one of the partner networks of the roaming partners, it is either the MN's home network or a visited network. If the first attachment is to the MN's home network, the MN is expected to already have a security association with HPoS; otherwise, the MN bootstraps this security association with the assistance of the HPoS.

After initial attachment, there is signaling defined so that at all times the MN has a security association with the PoS in the network at its current PoA, i.e., the SPoS. As the MN moves from one partner network to the next target network, the MN establishes or renews a security association with the PoS in the target network, the TPoS. When handover is completed, the TPoS begins to play the role of the MN's serving PoS, and subsequently when a handover is required the TPoS plays the role of the SPoS.

In order to enable a wider application of handovers and in particular preregistration signaling, security is essential for the control traffic. As previously described, this signaling traffic is mediated by the PoS in each target network, which may be unknown to the MN until the need for handover has been determined. In such cases, for secure signaling, the MN needs to establish a security association with the TPoS. Clause 9 of IEEE Std 802.21-2017 defines methods for an MIS SA to be established through (D)TLS or EAP. The methods specified there shall be used to establish an MIS SA between an MN and a TPoS so that TPoS is capable of providing security service, in particular, facilitating proactive authentication for an MN in a handover event. For single-radio handover, an optimized MIS SA establishment mechanism is introduced to speed up when the home networks of SPoS and TPoS have an existing trust relationship through partnership agreement.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.5.4.2 Optimized MIS SA establishment for single-radio handover service

This clause specifies one optimized MIS SA establishment for single-radio handover service. It allows a TPoS to obtain a key derivation key *K* from a SPoS or from a higher level entity. The key derivation key *K* is used to derive other keys such as the media independent session key (MISK) as described in 9.2.2 of IEEE Std 802.21-2017 between the MN and the TPoS, enabling further secure preregistration activities. Because of previous protocol operations (e.g., derivation of MIAK upon arrival in the source network), the MN has a current security association with the SPoS. As discussed in 5.5.4.1 the protection mechanisms applied between SPoS and TPoS are out of the scope of this specification. If the key *K* is distributed by SPoS to MN and to TPoS, the key distribution is protected by MIS SA between MN and SPoS and by out-of-scope mechanisms between SPoS and TPoS.

In order to establish an SA between the MN and the TPoS, they need to exchange Nonce-M and Nonce-S through messages MIS_Prereg_Xfer Request, MIS_Prereg_Xfer Response, and MIS_N2N_Prereg_Xfer Request. They also need to agree on a ciphersuite code specified in 9.2.3 of IEEE Std 802.21-2017. With this information, MN and TPoS derive the MISK as specified in 9.2.2 of IEEE Std 802.21-2017.

NOTE 1—The optimized MIS SA establishment is allowed only when a trust relationship has established between the network domains of SPoS and TPoS. It shall fall back to an SA establishment mechanism as specified in IEEE Std 802.21-2017 whenever it is possible, or if any of the MN or TPoS requests so.

NOTE 2—If protocol of establishing SAs between an MN and a TPoS is EAP, the optimized MIS SA establishment applies. In this case, the MN and the TPoS use key derivation key *K* as it is obtained through an EAP or EAP re-authentication protocol (ERP) execution.

NOTE 3—If protocol of establishing SAs between an MN and a TPoS is TLS, then the optimized SA establishment method does not apply, because the MN and the TPoS are not able to use key derivation key *K* in TLS.

NOTE 4—If any SPoS is compromised, the generated key *K* is compromised and so is the remaining of the PoS chains assuming that a TPoS will become a SPoS. To prevent such domino effect, the chain shall be limited. That is, after certain number of executions of the optimized SA establishment, it shall force an SA establishment through the methods specified in IEEE Std 802.21-2017.

5.5.4.3 TPoS selection by the SPoS

It is possible for the SPoS to take a more active role to promote smooth handover. When the MN determines the need for handover, but does not already know the address of the TPoS for the intended target network, the MN starts the preregistration sequence by sending all the known information to the SPoS. If the SPoS has access to information about the MIS PoS in each such surrounding network, the SPoS can make a determination about which target network is best to be able to provide connectivity and service to the MN. This also depends on the SPoS having access to location and configuration information about the MN—for example, which radio access technologies (RATs) are configured for operation on the MN. When the candidate TPoS is in another operator's network, it is also important that the SPoS should have a security relationship with a candidate TPoS in order to avoid interference from malicious nodes. This would typically mean that the operators are also roaming partners.

Subsequently, the SPoS will provide the address of the TPoS to the MN along with *K*, as previously described. The exact nature of the information about TPoS provided by the MN is dependent on the RAT type of the target network and is outside the scope of this document.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.6 Media independent event service

5.6.1 Link events for handover services

In addition, to link events in 6.3.4 of IEEE Std 802.21-2017, the following handover services related events are defined:

— **Link Handover events:** These events inform upper layers about the occurrence of L2 handovers/link switches if supported by the given media type.[12]

Table 1 defines link events for handover services.

Table 1—Link events for handover services

Link event name	Link event type	Description	Defined in
Link_Handover_Imminent	Link handover	L2 handover is imminent based on changes in link conditions.	5.10.1
Link_Handover_Complete	Link handover	L2 link handover to a new PoA has been completed.	5.10.2

5.6.2 MIS events for handover services

In addition to MIS events in Table 5 of IEEE Std 802.21-2017, Table 2 defines MIS events for handover services. An MIS event is marked as local only (L), remote only (R), or local and remote (L, R), indicating whether it is subscribed by a local MIS user, a remote MIS user, or both, respectively.

Table 2—MIS events for handover services

MIS event name	(L)ocal (R)emote	Description	Defined in
MIS_Link_Handover_Imminent	L, R	L2 handover is imminent based on either the changes in the link conditions or additional information available in the network. For example, the network decides that an application requires a specific QoS that can be best provided by a certain access technology.	5.11.1
MIS_Link_Handover_Complete	L, R	L2 link handover to a new PoA has been completed.	5.11.2

5.7 Media independent command service (MICS)

5.7.1 Link commands for handover services

In addition to link commands in Table 6 of IEEE Std 802.21-2017, Table 3 defines link commands for handover services.

[12] The mechanism that triggers and executes a link-layer handover/switch (also referred as an *L2 handover*) is specified within the corresponding media-specific standard and out of scope of this standard.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Table 3—Link commands for handover services

Link command	Comments	Defined in
Link_Prereg_Ready	Request a preregistration on a target link	5.10.3

5.7.2 MIS commands for handover services

5.7.2.1 General

In addition to MIS commands in Table 7 of IEEE Std 802.21-2017, Table 4 defines MIS commands for handover services. An MIS command is marked as local only (L), remote only (R), or local and remote (L, R), indicating whether it is issued by a local MIS user, a remote MIS user, or both, respectively.

Table 4—MIS commands for handover services

MIS command	(L) ocal, (R) emote	Comments	Defined in
MIS_Net_HO_Candidate_Query	R	Network initiates handover and sends a list of suggested networks and associated points of attachment.	5.11.3
MIS_MN_HO_Candidate_Query	R	Command used by MN to query and obtain handover related information about possible candidate networks.	5.11.4
MIS_N2N_HO_Query_Resources	R	This command is sent by the serving MISF entity to the target MISF entity to allow for resource query.	5.11.5
MIS_MN_HO_Commit	R	Command used by MN to notify the serving net- work of the decided target network information.	5.11.6
MIS_Net_HO_Commit	R	Command used by the network to notify the MN of the decided target network information.	5.11.7
MIS_N2N_HO_Commit	R	Command used by a serving network to inform a target network that an MN is about to move toward that network, initiate context transfer (if applicable), and perform handover preparation.	5.11.8
MIS_MN_HO_Complete	R	Notification from MISF of the MN to the target or source MISF indicating the status of handover completion.	5.11.9
MIS_N2N_HO_Complete	R	Notification from either source or target MISF to the other (i.e., peer) MISF indicating the status of the handover completion.	5.11.10
MIS_Net_HO_Bcst_Commit	R	Command used by the network to notify the specific group of MNs of the decided target network information.	5.11.11
MIS_Prereg_Xfer	R	Transport parameters and link-layer frames.	5.11.12
MIS_N2N_Prereg_Xfer	R	Transport link-layer frames between the SPoS and the TPoS.	5.12.1
MIS_Prereg_Ready	R	Check readiness of preregistration on a target link.	5.11.13
MIS_CTRL_Transfer	R	Deliver control message encapsulated by the MIS header	5.11.14

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.7.2.2 Naming convention for MIS handover commands

Generally, there are three types of MIS handover command primitives based on the functionality specified for the following scenarios:

a) MN to network

b) Network to MN

c) Network to network

This classification helps to ensure the specification of the proper protocol functionality and the relevant parameters for specific use as determined by the origination and the destination points.

Accordingly, these commands have a naming convention that identifies the origination point in the primitive name, as shown in Table 5. This convention is followed by the MISF to help ensure that these commands are utilized for the intended purpose. The destination point applies for remote commands only.

Table 5—Naming convention for MIS handover command primitives

Primitive name prefix	Originating point	Destination point
MIS_MN_HO_***	MN	Network
MIS_Net_HO_***	Network	MN
MIS_N2N_HO_***	Network	Network

5.7.2.3 Mobile initiated handovers

In this case, the MN initiates the handovers. The network selection policy function in this case resides on the MN. The MN directly uses the set of MIS_MN_HO_*** commands and may indirectly cause some MIS_N2N_HO_*** commands to be used when initiating handovers. The MN uses these commands to query the list of available candidate networks, reserve any required resources at the candidate target network, and indicate the status of handover operation to the MISF in the network.

5.7.2.4 Network initiated handovers

In this case, the network initiates the handovers. The network selection policy function in this case resides on the network. The network uses the set of MIS_Net_HO_*** in conjunction with any MIS_N2N_HO_*** commands for initiating handovers. The network uses these commands to query the list of resources currently being used by the MN, the serving network reserves any required resources at the candidate target network, and the network commands the MN to commit to performing a handover to a specific network.

5.8 Media independent information service

5.8.1 Information elements

Table 6 represents the list of handover-related information elements and their semantics in addition to what has been defined in 6.5.4 of IEEE Std 802.21-2017. Each information element has an abstract data type [see Annex E and also Annex E of IEEE Std 802.21-2017 for detailed definitions]. The binary and resource description framework (RDF) representation of these information elements are described in 6.5.6.2, 6.5.6.3,

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

and 6.5.7.2 of IEEE Std 802.21-2017, respectively. These information elements shall be used in conjunction with others that are described in IEEE Std 802.21-2017.

Table 6—Information elements

Name of information element	Description	Data type
Access network specific information elements		
IE_NET_MOB_MGMT_PROT	Type of mobility management protocol supported.	IP_MOB_MGMT
IE_NET_MOBILE_NETWORK	Indicator whether the access network itself is mobile.	BOOLEAN
IE_PoS_TUNN_MGMT_PRTO	Type of tunnel management protocol supported.	IP_TUNN_MGMT
IE_PoS_NAI	NAI of the PoS	MISF_ID

5.8.2 IE containers

— **IE_CONTAINER_NETWORKS**—contains the information depicting an access network that are necessary for handover use case in addition to what has been specified in Table 12 of IEEE Std 802.21-2017, as shown in Table 7.

Table 7—IE_CONTAINER_NETWORKS definition

Information element ID = [see Table F.1 of IEEE Std 802.21-2017]	**Length=** *variable*
IE_NET_MOB_MGMT_PROT (optional)	

5.9 Media dependent SAPs

5.9.1 MIS_LINK_SAP

The primitives defined as part of the MIS_LINK_SAP are described in Table 8. These are specific to handover use case and shall be used with others that are defined in 7.3 of IEEE Std 802.21-2017. Annex D contains their mapping to several specific link technologies. IETF RFC 5184 [B33] specifies many of these primitives as L2 abstractions.

Table 8—MIS_LINK_SAP primitives

Primitives	Service category	Description	Defined in
Link_Handover_Imminent	Event	L2 handover is imminent	5.10.1
Link_Handover_Complete	Event	L2 handover has been completed	5.10.2
Link_Prereg_Ready	Command	Used by MISFs at the MN and the PoS to prepare for preregistration	5.10.3
Link_Up	Event	L2 connectivity is established	5.10.4

5.9.2 MIS_NET_SAP

The primitive defined for MIS_NET_SAP is described in Table 9. This is specific to handover use case and shall be used with others that are defined in 7.5 of IEEE Std 802.21-2017.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Table 9—MIS_NET_SAP primitive

Primitive	Service category	Description	Defined in
MIS_N2N_Prereg_Xfer	Command	Used by MISFs at the SPoS and the TPoS for cross-network preregistration operations	5.12.1

5.9.3 Media independent SAP: MIS_SAP

The primitives defined as part of MIS_SAP are described in Table 10. These are specific to handover use case and shall be used with others that are defined in 7.4 of IEEE Std 802.21-2017.

Table 10—MIS_SAP primitives

Primitives	Service category	Description	Defined in
MIS_Link_Handover_Imminent	Event	L2 handover is imminent	5.11.1
MIS_Link_Handover_Complete	Event	L2 handover has been completed	5.11.2
MIS_Net_HO_Candidate_Query	Command	Initiate handover	5.11.3
MIS_MN_HO_Candidate_Query	Command	Initiate MN query request for candidate network	5.11.4
MIS_N2N_HO_Query_Resources	Command	Query available network resources	5.11.5
MIS_MN_HO_Commit	Command	Notify the serving network of the decidedtarget network information	5.11.6
MIS_Net_HO_Commit	Command	Network has committed to handover	5.11.7
MIS_N2N_HO_Commit	Command	Notify target network that the serving network has committed to handover	5.11.8
MIS_MN_HO_Complete	Command	Initiate MN handover complete notification	5.11.9
MIS_N2N_HO_Complete	Command	Handover has been completed	5.11.10
MIS_Net_HO_Bcst_Commit	Command	Command a specific group of MNs to handover from DO network to other networks	5.11.11
MIS_Prereg_Xfer	Command	Used by MISFs at the MN and the PoS for preregistration operations	5.11.12
MIS_Prereg_Ready	Command	Used by MISFs at the MN and the PoS to prepare for preregistration	5.11.13
MIS_CTRL_Transfer	Command	Used by the MISF to deliver control messages	5.11.14
MIS_Capability_Discover	Service management	Discover list of Events and Command supported by MISF	5.11.15
MIS_Link_Up	Event	L2 connection has been established	5.11.16

5.10 MIS_LINK_SAP primitives

5.10.1 Link_Handover_Imminent.indication

5.10.1.1 Function

Link_Handover_Imminent is generated when a native link-layer handover or switch decision has been made and its execution is imminent (as opposed to Link_Going_Down that only indicates that a link is losing connectivity due to a change in a certain link condition such as signal strength, but does not guarantee that a link switch-over has been decided by the link layer itself). It contains information about the

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

new PoA of the MN (the LinkIdentifier parameter contains information about the new PoA). This is a Link Handover event as discussed in 5.6.1.

5.10.1.2 Semantics of service primitive

Link_Handover_Imminent.indication (
Old Link Identifier,
New Link Identifier,
OldAccessRouter,
NewAccessRouter
)

Parameters:

Name	Data type	Description
OldLinkIdentifier	LINK_TUPLE_ID	Identifier of the old link.
NewLinkIdentifier	LINK_TUPLE_ID	Identifier of the new link.
OldAccessRouter	LINK_ADDR	(Optional) Link address of old Access Router.
NewAccessRouter	LINK_ADDR	(Optional) Link address of new Access Router.

5.10.1.3 When generated

Depending on whether it is the MN or the network, it is generated when a native link-layer handover or switch decision has been made and its execution is imminent.

5.10.1.4 Effect on receipt

The MISF receives this event from the link layer. The MISF then passes this notification to the MIS user(s) that has subscribed for this notification. The MIS user(s) takes necessary actions to minimize the effect of the pending native link-layer handover or switch on user data transfer. This event is also used as an indication to start buffering packets.

5.10.2 Link_Handover_Complete.indication

5.10.2.1 Function

Link_Handover_Complete event is generated whenever a native link-layer handover/switch has just been completed (as opposed to Link_Up that only indicates that a link has been brought up for L2 connectivity, but does not indicate that a native link handover/switch-over has just been completed by the link layer). Notifying the upper layer of this event improves transport, session, and application layer responsiveness to the link changes, which allows them to better adapt their data flows by resuming flows upon receiving this indication. The upper layers also use this event to check whether their IP configuration needs to be updated. This is a link-layer event that exists for intra-technology handovers defined in many media types. This event is applicable for the MN only and is valid only for intra-technology handovers. This is a Link Handover event as discussed in 5.6.1.

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.10.2.2 Semantics of service primitive

Link_Handover_Complete.indication (
OldLinkIdentifier,
NewLinkIdentifier,
OldAccessRouter,
NewAccessRouter,
LinkHandoverStatus
)

Parameters:

Name	Data type	Description
OldLinkIdentifier	LINK_TUPLE_ID	Identifier of the old link.
NewLinkIdentifier	LINK_TUPLE_ID	Identifier of the new link.
OldAccessRouter	LINK_ADDR	(Optional) Link address of old Access Router.
NewAccessRouter	LINK_ADDR	(Optional) Link address of new Access Router.
LinkHandoverStatus	STATUS	Status of the link handover.

5.10.2.3 When generated

This is generated whenever an L2 link-layer handover or switch has just been completed.

5.10.2.4 Effect on receipt

The MISF receives this event from the link layer. The MISF then passes this notification to the MIS user(s) that has subscribed for this notification. Upon reception of this event, an upper layer stops any handover adaptation that it has engaged to cope with the just completed native link-layer handover/switch and resume normal data transfer. This event is also used as an indication that a reverification of the IP parameter should be considered.

5.10.3 Link_Prereg_Ready

5.10.3.1 Link_Prereg_Ready.request

5.10.3.1.1 Function

The primitives defined here are used by MIS functions running on the MN and PoS to prepare for preregistration for MN on a target PoA. See Annex L for examples.

5.10.3.1.2 Semantics of service primitive

Link_Prereg_Ready.request (
ExecutionDelay
)

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

Parameters:

Name	Data type	Description
ExecutionDelay	UNSIGNED_INT(2)	Time (in ms) to elapse before the action should be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instance the request arrives until the time when the execution of the action is carried out.

5.10.3.1.3 When generated

This primitive is generated by the MISF to prepare preregistration of the target link.

5.10.3.1.4 Effect on receipt

Upon receipt of this primitive, the target link interface prepares preregistration at the time specified by the ExecutionDelay parameter. The L2 messages for preregistration are transmitted to the MISF for preregistration preparation with the target link layer.

5.10.3.2 Link_Prereg_Ready.confirm

5.10.3.2.1 Function

This primitive is used by link-layer technologies to provide an indication of the result of the preregistration preparation on the target link layer.

5.10.3.2.2 Semantics of service primitive

Link_Prereg_Ready.confirm (
Status
)

Parameters:

Name	Data type	Description
Status	STATUS	Status of the operation. Code 3 (Authorization Failure) is not applicable. (See Table E.2 of IEEE Std 802.21-2017.)

5.10.3.2.3 When generated

This primitive is generated in response to a Link_Prereg_Ready.request operation.

5.10.3.2.4 Effect on receipt

Upon reception of this primitive, the MISF knows the status of the preregistration on the target link.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.10.4 Link_Up.indication

This primitive is defined in 7.3.2 of IEEE Std 802.21-2017. The following additional parameter is needed while using this primitive for handover use:

Use case specific parameters:

Name	Data type	Description
MobilityManagementSupport	IP_MOB_MGMT	(Optional) Indicates the type of Mobility Management Protocol supported by the new PoA.

5.11 MIS_SAP primitive

5.11.1 MIS_Link_Handover_Imminent.indication

5.11.1.1 Function

This primitive is issued by the MISF to report the imminent occurrence of an intra-technology link handover. This MIS event is either local or remote. This indication directly corresponds to the link-layer event Link_Handover_Imminent.indication defined in 5.10.1.

5.11.1.2 Semantics of service primitive

MIS_Link_Handover_Imminent.indication (
SourceIdentifier,
OldLinkIdentifier,
NewLinkIdentifier,
OldAccessRouter,
NewAccessRouter
)

Parameters:

Name	Data type	Description
SourceIdentifier	MISF_ID	This identifies the invoker of this primitive, which is either the local MISF or a remote MISF.
OldLinkIdentifier	LINK_TUPLE_ID	Identifier of the old link.
NewLinkIdentifier	LINK_TUPLE_ID	Identifier of the new link.
OldAccessRouter	LINK_ADDR	(Optional) Link address of old Access Router.
NewAccessRouter	LINK_ADDR	(Optional) Link address of new Access Router.

5.11.1.3 When generated

This notification is generated by the MISF when a link-layer intra-technology handover is about to occur. The event could be triggered by the reception of a Link_Handover_Imminent.indication from a link or on receipt of an MIS_Link_Handover_Imminent indication message.

5.11.1.4 Effect on receipt

Upper layer entities take different actions upon notification.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

5.11.2 MIS_Link_Handover_Complete.indication

5.11.2.1 Function

This primitive is issued by the MISF to report the completion of an intra-technology link handover. This MIS event is either local or remote. MIS_Link_Handover_Complete indication is a result of a Link_Handover_Complete indication from the link layer.

5.11.2.2 Semantics of service primitive

MIS_Link_Handover_Complete.indication (
SourceIdentifier,
OldLinkIdentifier,
NewLinkIdentifier,
OldAccessRouter,
NewAccessRouter,
)

Parameters:

Name	Data type	Description
SourceIdentifier	MISF_ID	This identifies the invoker of this primitive, which is either the local MISF or a remote MISF.
OldLinkIdentifier	LINK_TUPLE_ID	Identifier of the old link.
NewLinkIdentifier	LINK_TUPLE_ID	Identifier of the new link.
OldAccessRouter	LINK_ADDR	(Optional) Link address of old Access Router.
NewAccessRouter	LINK_ADDR	(Optional) Link address of new Access Router.

5.11.2.3 When generated

This notification is generated by the MISF when a link-layer intra-technology handover is completed. The event could be triggered by the reception of a Link_Handover_Complete.indication from a link or on receipt of an MIS_Link_Handover_Complete indication message.

5.11.2.4 Effect on receipt

Upper layer entities take different actions on this notification. An MIS user makes use of this notification to configure other layers (IP, Mobile IP) for various upper layer handovers that are needed. Transport layers (e.g., TCP) also make use of this primitive to fine tune their flow control and flow congestion mechanisms.

5.11.3 MIS_Net_HO_Candidate_Query

5.11.3.1 General

For network initiated handovers, the network controller provides a list of candidate network choices to the MN (via MIS_Net_HO_Candidate_Query request message). The MN indicates resources required on each of these candidate networks in the MIS_Net_HO_Candidate_Query response message. The network controller then queries each of the candidate networks for available resources (using

Copyright 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018

MIS_N2N_HO_Query_Resources primitive). Once the target network has been selected, the network controller sends an MIS_Net_HO_Commit message. An example of this operation is illustrated in B.2.

5.11.3.2 MIS_Net_HO_Candidate_Query.request

5.11.3.2.1 Function

The primitive is invoked by an MIS user on a network node to communicate to a peer MIS user about its intent of handover initiation.

5.11.3.2.2 Semantics of service primitive

MIS_Net_HO_Candidate_Query.request (
DestinationIdentifier,
SuggestedNewLinkList,
SuggestedCandidateAuthenticatorList,
QueryResourceReportFlag
)

Parameters:

Name	Data type	Description
DestinationIdentifier	MISF_ID	This specifies MISF ID of the remote MISF(s) to be configured of this request.
SuggestedNewLinkList	LIST(LINK_POA_LIST)	A list of PoAs for each link, suggesting the new access networks to which handover initiation should be considered. The access networks towards the top of the list are more preferable than those towards the bottom of the list.
SuggestedCandidateAuthenticator List	LIST(LINK_AUTHENTICATOR_ LIST)	List of media specific authenticator's address for the suggested candidate PoAs.
QueryResourceReportFlag	BOOLEAN	Flag to specify if resources need to be reported by MN: TRUE: Required to report resource list FALSE: Not required to report resource list.

5.11.3.2.3 When generated

This primitive is invoked by an MIS user to communicate with a remote MIS user about its intent of handover initiation. Serving PoS requests MN to provide information about resources required to initiate a handover by setting the QueryResourceReportFlag parameter.

Copyright 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 8802-21-1:2018