IEEE P™/D  
Draft for Local and Metropolitan Area Networks- Part 21: Media Independent Handover Services

Amendment 3: Optimized Single Radio Handovers

Sponsor

**Committee**of the **IEEE Computer Society**

NOTE: This amendment is to be applied to the result of original 802.21-2008, 802.21a-2012, and 802.21b-2012.

Approved <XX MONTH 20XX>

**IEEE-SA Standards Board**

Copyright © 2012 by The Institute of Electrical and Electronics Engineers, Inc.

Three Park Avenue

New York, New York 10016-5997, USA

All rights reserved.

This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of international standardization consideration. Prior to adoption of this document, in whole or in part, by another standards development organization, permission must first be obtained from the IEEE Standards Association Department (stds.ipr@ieee.org). Other entities seeking permission to reproduce this document, in whole or in part, must also obtain permission from the IEEE Standards Association Department.

IEEE Standards Association Department

445 Hoes Lane

Piscataway, NJ 08854, USA

Abstract: <Select this text and type or paste Abstract—contents of the Scope may be used>

Keywords: <Select this text and type or paste keywords>

[[1]](#footnote-1)•

**IEEE Standards** documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

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

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854

USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Notice to users

Laws and regulations

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

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

Errata

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

Participants

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

, *Chair*

, *Vice Chair*

Participant1

Participant2

Participant3

Participant4

Participant5

Participant6

Participant7

Participant8

Participant9

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

***(to be supplied by IEEE)***

Balloter1

Balloter2

Balloter3

Balloter4

Balloter5

Balloter6

Balloter7

Balloter8

Balloter9

When the IEEE-SA Standards Board approved this on <XX MONTH 20XX>, it had the following membership:

***(to be supplied by IEEE)***

**<Name>,** *Chair*

**<Name>,** *Vice Chair*

**<Name>,** *Past Chair*

**<Name>,** *Secretary*

SBMember1

SBMember2

SBMember3

SBMember4

SBMember5

SBMember6

SBMember7

SBMember8

SBMember9

\*Member Emeritus

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

<Name>, *DOE Representative*

<Name>, *NRC Representative*

<Name>

*IEEE Standards Program Manager, Document Development*

<Name>

*IEEE Standards Program Manager, Technical Program Development*

Introduction

This introduction is not part of IEEE P/D, Draft for Local and Metropolitan Area Networks- Part 21: Media Independent Handover Services

Amendment 3: Optimized Single Radio Handovers

.

This document specifies optimizations to reduce the latency during single radio handovers between heterogeneous access networks.

Contents

[1. Overview 2](#_Toc343090507)

**[1.1](#_Toc343090508)** [2](#_Toc343090508)

**[1.2](#_Toc343090509)** [2](#_Toc343090509)

**[1.3](#_Toc343090510)** [2](#_Toc343090510)

[1.4 Assumptions 2](#_Toc343090511)

[2. Normative references 2](#_Toc343090512)

[3. Definitions 2](#_Toc343090520)

[4. Abbreviations and acronyms 3](#_Toc343090521)

[5. General architecture 4](#_Toc343090522)

[5.1 Introduction 4](#_Toc343090523)

**[5.1.1](#_Toc343090524)** [4](#_Toc343090524)

**[5.1.2](#_Toc343090525)** [4](#_Toc343090525)

**[5.1.3](#_Toc343090526)** [4](#_Toc343090526)

**[5.1.4](#_Toc343090527)** [4](#_Toc343090527)

**[5.1.5](#_Toc343090528)** [4](#_Toc343090528)

**[5.1.6](#_Toc343090529)** [4](#_Toc343090529)

**[5.1.7](#_Toc343090530)** [4](#_Toc343090530)

**[5.1.8](#_Toc343090531)** [4](#_Toc343090531)

**[5.1.9](#_Toc343090532)** [4](#_Toc343090532)

[5.1.10 Media independent single radio handover 4](#_Toc343090533)

[5.1.11 Securing Single-Radio messages using PoS 5](#_Toc343090534)

[5.1.12 5](#_Toc343090535)

[5.2 General design principles 5](#_Toc343090536)

**[5.2.1](#_Toc343090537)** [5](#_Toc343090537)

**[5.2.2](#_Toc343090538)** [5](#_Toc343090538)

[5.2.3 Single Radio Handover MIHF (SR-MIHF) Design Principles 5](#_Toc343090539)

[5.3 MIHF service overview 6](#_Toc343090540)

**[5.3.1](#_Toc343090541)** [6](#_Toc343090541)

**[5.3.2](#_Toc343090542)** [6](#_Toc343090542)

**[5.3.3](#_Toc343090543)** [6](#_Toc343090543)

[5.3.4 Media independent information service 6](#_Toc343090544)

[5.4 Media independent handover reference framework 6](#_Toc343090545)

**[5.4.1](#_Toc343090546)** [6](#_Toc343090546)

**[5.4.2](#_Toc343090547)** [6](#_Toc343090547)

**[5.4.3](#_Toc343090548)** [6](#_Toc343090548)

[5.4.4 Information Repository 6](#_Toc343090549)

[5.4.5 General MIHF reference model and SAPs / Single Radio handover Control Function <was 11.1.2 -- fold into MIHF, perhaps SR-MIHF> 6](#_Toc343090550)

[5.4.6 SR-Gateway services at Home Network, Source Network, and Target Network 7](#_Toc343090551)

[5.5 MIHF reference models for link-layer technologies 7](#_Toc343090552)

**[5.5.1](#_Toc343090553)** [7](#_Toc343090553)

[6. MIH Services 7](#_Toc343090554)

**[6.1](#_Toc343090555)** [7](#_Toc343090555)

**[6.2](#_Toc343090556)** [7](#_Toc343090556)

**[6.3](#_Toc343090557)** [7](#_Toc343090557)

**[6.4](#_Toc343090558)** [7](#_Toc343090558)

[6.5 Media independent information service 7](#_Toc343090559)

**[6.5.1](#_Toc343090560)** [7](#_Toc343090560)

**[6.5.2](#_Toc343090561)** [7](#_Toc343090561)

**[6.5.3](#_Toc343090562)** [7](#_Toc343090562)

[6.5.4 Information Elements 7](#_Toc343090563)

[7. Service Access Point (SAP) and primitives 8](#_Toc343090564)

**[7.1](#_Toc343090565)** [8](#_Toc343090565)

**[7.2](#_Toc343090566)** [8](#_Toc343090566)

[7.3 MIH\_LINK\_SAP primitives 8](#_Toc343090567)

**[7.3.1](#_Toc343090568)** [8](#_Toc343090568)

**[7.3.2](#_Toc343090569)** [8](#_Toc343090569)

**[7.3.3](#_Toc343090570)** [8](#_Toc343090570)

**[7.3.4](#_Toc343090571)** [8](#_Toc343090571)

**[7.3.5](#_Toc343090572)** [8](#_Toc343090572)

**[7.3.6](#_Toc343090573)** [8](#_Toc343090573)

**[7.3.7](#_Toc343090574)** [8](#_Toc343090574)

**[7.3.8](#_Toc343090575)** [8](#_Toc343090575)

**[7.3.9](#_Toc343090576)** [8](#_Toc343090576)

**[7.3.10](#_Toc343090577)** [8](#_Toc343090577)

**[7.3.11](#_Toc343090578)** [8](#_Toc343090578)

**[7.3.12](#_Toc343090579)** [8](#_Toc343090579)

**[7.3.13](#_Toc343090580)** [8](#_Toc343090580)

**[7.3.14](#_Toc343090581)** [8](#_Toc343090581)

[7.3.15 Link\_IF\_PreReg\_Ready 8](#_Toc343090582)

[7.4 MIH\_SAP primitives 9](#_Toc343090583)

**[7.4.1](#_Toc343090584)** [9](#_Toc343090584)

**[7.4.2](#_Toc343090585)** [9](#_Toc343090585)

**[7.4.3](#_Toc343090586)** [9](#_Toc343090586)

**[7.4.4](#_Toc343090587)** [9](#_Toc343090587)

**[7.4.5](#_Toc343090588)** [9](#_Toc343090588)

**[7.4.6](#_Toc343090589)** [9](#_Toc343090589)

**[7.4.7](#_Toc343090590)** [9](#_Toc343090590)

**[7.4.8](#_Toc343090591)** [9](#_Toc343090591)

**[7.4.9](#_Toc343090592)** [9](#_Toc343090592)

**[7.4.10](#_Toc343090593)** [9](#_Toc343090593)

**[7.4.11](#_Toc343090594)** [9](#_Toc343090594)

**[7.4.12](#_Toc343090595)** [9](#_Toc343090595)

**[7.4.13](#_Toc343090596)** [9](#_Toc343090596)

**[7.4.14](#_Toc343090597)** [9](#_Toc343090597)

**[7.4.15](#_Toc343090598)** [9](#_Toc343090598)

**[7.4.16](#_Toc343090599)** [9](#_Toc343090599)

**[7.4.17](#_Toc343090600)** [9](#_Toc343090600)

**[7.4.18](#_Toc343090601)** [9](#_Toc343090601)

**[7.4.19](#_Toc343090602)** [9](#_Toc343090602)

**[7.4.20](#_Toc343090603)** [9](#_Toc343090603)

**[7.4.21](#_Toc343090604)** [9](#_Toc343090604)

**[7.4.22](#_Toc343090605)** [9](#_Toc343090605)

**[7.4.23](#_Toc343090606)** [9](#_Toc343090606)

**[7.4.24](#_Toc343090607)** [9](#_Toc343090607)

**[7.4.25](#_Toc343090608)** [9](#_Toc343090608)

**[7.4.26](#_Toc343090609)** [9](#_Toc343090609)

**[7.4.27](#_Toc343090610)** [9](#_Toc343090610)

**[7.4.28](#_Toc343090611)** [9](#_Toc343090611)

**[7.4.29](#_Toc343090612)** [9](#_Toc343090612)

[7.4.30 MIH\_LL\_Transfer 9](#_Toc343090613)

[7.4.31 MIH\_N2N\_LL\_Transfer 13](#_Toc343090614)

[7.4.32 MIH\_IF\_PreReg\_Ready 17](#_Toc343090615)

[7.4.33 MIH\_TNMN\_SA\_Estab 19](#_Toc343090616)

[7.4.34 MIH\_N2N\_MNTN\_SA\_Estab 23](#_Toc343090617)

**[7.5](#_Toc343090618)** [27](#_Toc343090618)

**[7.6](#_Toc343090619)** [27](#_Toc343090619)

[8. Media independent handover protocols 27](#_Toc343090620)

**[8.1](#_Toc343090621)** [27](#_Toc343090621)

**[8.2](#_Toc343090622)** [27](#_Toc343090622)

**[8.3](#_Toc343090623)** [27](#_Toc343090623)

[8.4 MIH protocol frame format 27](#_Toc343090624)

[8.4.1 General frame format 27](#_Toc343090625)

**[8.5](#_Toc343090626)** [27](#_Toc343090626)

[8.6 MIH protocol messages 27](#_Toc343090627)

**[8.6.1](#_Toc343090628)** [27](#_Toc343090628)

**[8.6.2](#_Toc343090629)** [27](#_Toc343090629)

[8.6.3 MIH messages for command service 27](#_Toc343090630)

[8.6.4 MIH messages for gateway service 31](#_Toc343090631)

[9. MIH protocol protection 32](#_Toc343090632)

**[9.1](#_Toc343090634)** [32](#_Toc343090634)

[9.2 Key establishment through an MIH service access authentication 32](#_Toc343090635)

**[9.2.1](#_Toc343090636)** [32](#_Toc343090636)

[9.2.2 Key derivation and key hierarchy 32](#_Toc343090637)

[10. Proactive Authentication 33](#_Toc343090638)

[10.1 Media specific proactive authentication 33](#_Toc343090639)

**[10.2](#_Toc343090640)** [35](#_Toc343090640)

[10.3 Establishing Security Association roaming partners for MIH 35](#_Toc343090641)

[10.3.1 Key distribution by OPoS 36](#_Toc343090642)

[10.3.2 TPoS selection by OPoS 38](#_Toc343090643)

[11. Single Radio Handover 38](#_Toc343090644)

[11.1 Introduction (keep in reduced version) 38](#_Toc343090645)

[11.2 Major single radio handover processes 38](#_Toc343090689)

[12. Gateway Service 40](#_Toc343090690)

[12.1 Introduction 40](#_Toc343090691)

[12.2 Communication between the MN and the target PoA < Was 11.1.4> 41](#_Toc343090692)

[12.3 L2 Message Transfer (SID=5, AID=1) 43](#_Toc343090693)

[12.4 Interworking Protocol Delivery (SID=5, AID>1) 43](#_Toc343090694)

[12.4.1 Examples of Interworking Protocol Delivery: ANQP Delivery 44](#_Toc343090695)

[Annex A 46](#_Toc343090696)

[Bibliography 46](#_Toc343090697)

[Annex B 46](#_Toc343090698)

[Annex C 46](#_Toc343090699)

[Annex D 46](#_Toc343090700)

[Annex E 46](#_Toc343090701)

[Annex F 46](#_Toc343090702)

**[F.1](#_Toc343090703)** [47](#_Toc343090703)

**[F.2](#_Toc343090704)** [47](#_Toc343090704)

[F.3 Derived data types 47](#_Toc343090705)

**[F.3.1](#_Toc343090706)** [47](#_Toc343090706)

**[F.3.2](#_Toc343090707)** [47](#_Toc343090707)

**[F.3.3](#_Toc343090708)** [47](#_Toc343090708)

[F.3.4 Data types for link identification and manipulation 47](#_Toc343090709)

**[F.3.5](#_Toc343090710)** [48](#_Toc343090710)

**[F.3.6](#_Toc343090711)** [48](#_Toc343090711)

**[F.3.7](#_Toc343090712)** [48](#_Toc343090712)

[F.3.8 Data types for information elements 48](#_Toc343090713)

[F.3.9 48](#_Toc343090714)

[F.3.10 48](#_Toc343090715)

[F.3.11 48](#_Toc343090716)

[F.3.12 48](#_Toc343090717)

**[F.3.13](#_Toc343090718)** [48](#_Toc343090718)

**[F.3.14](#_Toc343090719)** [48](#_Toc343090719)

**[F.3.15](#_Toc343090720)** [48](#_Toc343090720)

[F.3.16 Data type for security 48](#_Toc343090721)

[Annex G 49](#_Toc343090722)

[Annex H 49](#_Toc343090723)

[Annex I 49](#_Toc343090724)

[Annex J 49](#_Toc343090725)

[Annex K 49](#_Toc343090726)

[Annex L 49](#_Toc343090727)

[Annex M 50](#_Toc343090728)

[Annex N 50](#_Toc343090729)

**[N.1](#_Toc343090730)** [50](#_Toc343090730)

**[N.2](#_Toc343090731)** [50](#_Toc343090731)

**[N.3](#_Toc343090732)** [50](#_Toc343090732)

**[N.4](#_Toc343090733)** [50](#_Toc343090733)

**[N.5](#_Toc343090734)** [50](#_Toc343090734)

[N.6 Use of MIH\_LL\_Transfer and MIH SA\_Estab messages for the exchange of L2 frames, including Optimized SA Establishment 50](#_Toc343090735)

[Annex O 55](#_Toc343090736)

[Annex P MN’s Network Access Identifier Format 55](#_Toc343090737)

[Annex Q Network discovery for single radio handover 56](#_Toc343090738)

[Q.1 Network discovery: listening to the target link 56](#_Toc343090739)

[Q.2 Network discovery: using location information 56](#_Toc343090740)

[Q.3 Network discovery: using user schedule information 57](#_Toc343090741)

[Annex R Examples of SRHO 58](#_Toc343090743)

[R.1 WLAN to WiMAX single radio handover 85](#_Toc343090744)

[R.1.1 Transport of WiMAX L2 control frames between MN and the WiMAX ASN 85](#_Toc343090745)

[R.1.2 WLAN to WiMAX Single Radio Handover processes 85](#_Toc343090746)

[R.2 3GPP to WiMAX single radio handover 85](#_Toc343090747)

[R.2.1 Transport of WiMAX L2 control frames between MN and the WiMAX ASN 85](#_Toc343090748)

[R.2.2 3GPP to WiMAX Single Radio Handover processes 85](#_Toc343090749)

[R.3 WiMAX to WLAN single radio handover 85](#_Toc343090750)

[R.3.1 Transport of WLAN L2 control frames between MN and the WLAN AN 85](#_Toc343090751)

[R.3.2 WiMAX to WLAN Single Radio Handover processes 85](#_Toc343090752)

[R.4 WiMAX to 3GPP single radio handover 85](#_Toc343090753)

[R.4.1 Transport of 3GPP L2 control frames between MN and the 3GPP network 85](#_Toc343090754)

[R.4.2 WiMAX to 3GPP Single Radio Handover processes 85](#_Toc343090755)

[R.5 WLAN to 3GPP single radio handover 85](#_Toc343090756)

[R.5.1 Transport of 3GPP L2 control frames between MN and the 3GPP network 85](#_Toc343090757)

[R.5.2 Non-trusted WLAN AN to 3GPP Single Radio Handover processes 85](#_Toc343090758)

[Annex S Handover Decision 85](#_Toc343090759)

[S.1 Weak SINR of the source link 86](#_Toc343090760)

[S.2 QoS and/or cost check 86](#_Toc343090761)

[S.3 Power consumption comparison of the link interfaces 87](#_Toc343090762)

Draft for Local and Metropolitan Area Networks- Part 21: Media Independent Handover Services

Amendment 3: Optimized Single Radio Handovers

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

***This IEEE document is made available for use subject to important notices and legal disclaimers.   
These notices and disclaimers appear in all publications containing this document and may   
be found under the heading “Important Notice” or “Important Notices and Disclaimers   
Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at*** [***http://standards.ieee.org/IPR/disclaimers.html***](http://standards.ieee.org/IPR/disclaimers.html)***.***

NOTE—The editing instructions contained in this <amendment/corrigendum> define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview



   4. Assumptions

*Insert at end of Clause 1.4*

The following assumptions apply during the single radio handover:

1. While the source radio is transmitting, the target radio cannot transmit.

The mobile device can transmit on only one radio at a time. Prior to handover completion, the source radio link is used to support data transfer so that the priority to transmit is given to the source radio.

1. It shall be possible that while the source radio is receiving, the target radio shall not transmit at a frequency close to the frequency of the source radio receiver..
2. It shall be possible that while the source radio is receiving, the target radio shall not receive at a frequency close to the frequency of the source radio receiver..
3. The mobile node (MN) and the target network may communicate with each other via the source network using the source link.

It is possible that the source point of attachment and the target point of attachment may: (a) belong to the same access network, (b) belong to different access networks connecting to the same backhaul network, or (c) belong to different access networks connecting to different backhaul networks. In (a) and (b), the capability to communicate between the source radio and the target network usually does not utilize internetwork interfaces. In (c), the two networks may require internetwork addresses in order to be able to communicate with each other.

1. Normative references

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

1. Definitions

*Insert these definitions in appropriate order*

**MIH-capable device:** A network node that implements one or more MIH commands. For instance, a mobile node MN is MIH-capable if it implements at least MIH\_LL\_Transfer commands.

**Originating network PoS**: The Point of Service in the network of the Mobile Node’s current Point of Attachment

**Preregistration:** preparatory handover signaling (including security establishment) which is accomplished before the handover actually occurs.

**Proxy Gateway**: A gateway to bridge the mobility signaling between a mobile node (MN) and a target point of attachment via the source network. To the MN, the Proxy GW acts like a virtual point of attachment (PoA) to the target network. It enables such functions as preregistration and proactive authentication of the MN.

**Single radio handover (SRHO)**: A handover among heterogeneous radio access technologies during which a mobile node can transmit on only one radio at a time.

**Single Radio handover MIHF (SR-MIHF)**: A media independent control function to enable MN and Target PoA to exchange the network entry link-layer PDUs without depending on the existence of the target radio’s physical channel. It uses the available radio’s IP transport to deliver the deactivated target radio’s network entry L2 PDUs. It interfaces with the transport layer (e.g., UDP) through the Media Independent Control Service Access Point (MICSAP) so that it may exchange SRC frames with remote SR-MIHF entities through IP transport. The exchanged SRC frames are processed by the SR-MIHF which has the assigned transport layer protocol’s port number [RFC 5677]. SR-MIHF also interfaces with the link-layer (L2) through the Media independent Control Link-layer Service Access Point (MICLSAP) so that it may provide transport of L2 frames of a deactivated target radio to and from a remote SR-MIHF entity.

**Single radio MIH frame**: A packet which contains the target radio’s network entry link-layer PDUs in its payload.

**Target network PoS**: A Point of Service in the target network of the target Point of Attachment, to which a Mobile Node will be attached after a handover has been completed

1. Abbreviations and Acronymns

*Note to editor:* *insert these definitions in appropriate order*

ANDSF Access network discovery selection functions

MIHF media independent control function

MICSAP media independent control service access point

MICLSAP media independent control link-layer service access point

PoS point of service

SR-MIHF Single radio - media independent handover function

SRC single radio handover control

SRHO single radio handover

OPoS originating PoS

TPoS target PoS

1. General architecture
   1. Introduction










      11. Media independent single radio handover

The concept of media independence applies to single radio handover just as it does to the dual-radio handover. A media independent handover may be accomplished in a media independent way, but the signaling messages for a single radio handover may differ from that for a dual-radio However, the MIHF is extended with the definitions of MICSAP and MICLSAP defined in the draft Std IEEE P802/D1.4 on architecture and are described in Clause 0 . With these extensions, the MIHF can be now described as a parallel control plane and is called media independent control function (MICF) in the draft Std IEEE P802/D1.4.

Security is indispensable to mobility management (see section 10.2), but it has been typically quite time consuming because of reliance on distant authentication agents. Improving the security model and reducing authentication delay enables crucial improvements in handover performance. For the single radio handover design using media independent messages, the same transport possibilities as MIHF may apply. For single-radio performance improvement, 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 naturally depend on the requirements of the target network, and can be quite independent of the nature of the network (as above, the "source network") providing the current point of attachment for the MN. As a general rule, preregistration typically involves the following steps:

* pre-authentication -- that is, authenticating the MN before it arrives in the target network,
* address allocation -- one or more 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, and
* context establishment -- building all necessary state information such as QoS parameters and access permissions within target core network entities.

Each of these operations can be time-consuming, and if they had to be carried out after the MN had returned to the target network radio access, smooth handover might be impossible because of the dead time before packets could start flowing again (break-before-make). Moreover, each of the operations must be carried out 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. On the other hand, for access networks belonging to different operators, the data path between neighboring access points of originating and target access networks are more likely to traverse the Internet, potentially exposing preregistration signaling to attack. See section 5.1.11.

* + 1. Securing Single-Radio messages using PoS

Enabling movement between the networks of roaming partners for single-radio smartphones 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 the WiMAX Forum, 3GPP2, and 3GPP <insert xrefs>. Using the PoS along with some signaling to transmit security information between roaming partners enables a low-latency, optimized handover for even the single-radio devices. Since communication between the source and target networks may traverse the Internet, these communications must be secured; but this can be 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 section <insert xref here>). Improving the security model and reducing authentication delay enables crucial improvements in handover performance.

* 1. General design principles



     4. Single Radio Handover MIHF (SR-MIHF) Design Principles

The following assumptions apply during the single radio handover: (\*\*\* are the assumptions moved to Clause 1.4?\*\*\*)

1. While the source radio is transmitting, the target radio cannot transmit; the mobile device can transmit on only one radio at a time. Some single-radio devices may have the capability to receive on multiple radios at the same time, but that capability is not used in the 802.21 media-independent design.
2. The mobile node (MN) and the target network may communicate with each other via the source network using the source link.

The following requirements facilitate single radio handover between different radio access technology networks.

**Functional Requirements for SR-MIHF:**

* tunneling mechanism to deliver the preregistration messages
* control for pre-registered states and delivery for pre-registered contexts.
* capabilities exchange between mobile station and SR-MIHF at the network.
  + Supported radio access technology (RAT) types (3GPP, WiMAX, WiFi, 3GPP2, etc.)
  + Supported target network capabilities
  + Any required layer-2 parameters
  1. MIHF service overview




     5. Media independent information service
  2. Media independent handover reference framework




     5. Information Repository

The network service information and the location information, such as the availability of candidate target network etc., are needed to make handover decisions. For example, the Information Repository may be implemented as part of a media independent information server (MIIS) or may be implemented as the Access Network Discovery and Selection Function (ANDSF) defined in 3GPP standard [3GPP TS23.402].

The type of information needed in the mobility management protocol depends on the mobility management protocol being used. For example, when mobile IP is used for the inter-network management protocol, the location of the MN in the network is the care-of-address (CoA) and the identity of the MN is the home address in the home network of the MN. The location management information for mobile IP may then be the binding of the home address to the care-of-address. Furthermore, in accordance with existing procedures for subscriber management, mobility management may also require access to policy information controlling the allowable behavior of the mobile devices.

The distributed database of the Information Repository allows flexibility for different owners to manage their data separately. An example is for each network to host the master copy of the data that is most convenient to be managed by that network. The servers in the different networks constitute a distributed database of the Information Repository, organized so that each server knows which data belongs to which component of the Repository.

* + 1. General MIHF reference model and SAPs / Single Radio handover Control Function <was 11.1.2 -- fold into MIHF, perhaps SR-MIHF>

To prepare for handover, the MN’s target radio exchanges link-layer network entry PDUs with the target PoA at the target network. These network entry PDUs can be the same PDUs that would be exchanged if the target link were active. There is no guarantee that the target link is available during a single radio handover. A single radio handover control function (SR-MIHF) is used here to enable the MN and the target PoA to exchange the network entry link-layer PDUs without depending on the existence of the target radio’s physical channel but with the help of the active source radio.

In figure 4 (above in this section 5.5.2) the Single Radio MIHF (SR-MIHF) in a multiple interface node is implemented using the media independent control function (MIHF) in the control plane.

The SR-MIHF use MIH-SAP for communication via TCP/IP or UDP/IP. The SR-MIHF similarly interfaces with the link-layer (L2) MIH\_LINK\_SAP as before. During a single radio hadover, an L2 frame of a deactivated link is encapsulated in an MIH message to constitute a SRC frame, which is then exchanged via an active link between the SR-MIHFs of a local and a remote node using MIH protocol over L3 transport (TCP or UDP).

* + 1. SR-Gateway services at Home Network, Source Network, and Target Network



**Figure 11.2 An architecture of distributed mobility management.**

This distributed mobility management architecture also works for single radio management. Because the logical functions for distributed mobility management must already reside in some physical network elements, new physical network elements are not necessarily needed with this single radio handover reference model.

* 1. MIHF reference models for link-layer technologies



**Figure 11.2 Single radio handover reference model.**

Functions in originating network: OPoS and the proxy function

Functions in target network: TPoS and the proxy function

The proxy functions enable signaling between the MN and the target PoA:

MN signals with target PoA via OPoS/proxy function, which in turn signals with target PoA via TPoS/proxy function.

Target PoA signals with MN via TPoS proxy function, which in turn signals with MN via OPoS proxy function.



**Figure 11.2 Signaling flow for Single radio handover via proxy functions**

MN sends a message to the OPoS with a payload of a target network L2 handover frame.

Upon receiving this message from MN,

OPoS proxy function helps to discover a suitable target network if not already known.

OPoS proxy function signals with the MN via the TPoS proxy function, that is, OPoS proxy function sends the message to TPoS.

Upon receiving this message from MN (either directly or via the OPoS, if the message is received directly from the MN, the via through the OPoS is bypassed), TPoS proxy function helps to discover a suitable PoA if not already known.

TPoS proxy function signals with this target PoA using 21c message if the target PoA supports 21c.

TPoS proxy function signals with this target PoA using other message if the target PoA does not support 21c. It will reply to MN via the OPoS proxy function whether the L2 handover frame is successful with an indication that it signals with the target PoA using other message(s).

(The indication is needed because a proxy function that uses 21c messages only is still a proxy, but the SRHO will fail whenever the target PoA does not 21c.)

1. MIH Services





   6. Media independent information service




      5. Information Elements

*Insert ordered list element as follows, and relabel current item (c) as item (d):*

1. The Information Server provides the Point of Service (PoS) information, the Mobile Node (MN) information and the capability for supporting SRHO for each of the available access networks. The PoS information includes PoS addressing information and tunnel management protocol information. The MN information includes location information of the MN.

*Insert information elements in Table 10 as follows:*

1. — Information Elements

|  |  |  |
| --- | --- | --- |
| Name of information element | Description | Data type |
| 802.21 Point of Service information elements | | |
| IE\_PoS\_TUNN\_MGMT\_PRTO | Type of tunnel management protocol supported. | IP\_TUNN\_MGMT |
| IE\_PoS\_FQDN | FQDN of PoS. | FQDN |



1. Service Access Point (SAP) and primitives



   4. MIH\_LINK\_SAP primitives

*Insert following clause 7.3.15*

* + 2. Link\_IF\_PreReg\_Ready
       1. Link\_IF\_PreReg\_Ready.request
          1. Function

This primitive is used by the MIHF to request preregistration on a target link interface of MN.

* + - * 1. Semantics of service primitive

Link\_IF\_PreReg\_Ready.request (

ExecutionDelay

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| ExecutionDelay | UNSIGNED\_INT(2) | Time (in ms) to elapse before the action needs to 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. |

* + - * 1. When generated

This primitive is generated by the SR-MIHF to prepare preregistration of the target link.

* + - * 1. 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 SR-MIHF on behalf of PHY of the target link.

* + - 1. Link\_IF\_PreReg\_Ready.confirm
         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.

* + - * 1. Semantics of service primitive

Link\_IF\_PreReg\_Ready.confirm (

Status

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| Status | STATUS | Status of the operation. Code 3 (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated in response to Link\_IF\_PreReg\_Ready.request operation.

* + - * 1. Effect on receipt

Upon reception of this primitive, the SR-MIHF can know the status of the preregistration

* 1. MIH\_SAP primitives

*Insert following clauses 7.4.30 – 7.4.33*

* + 1. MIH\_LL\_Transfer
       1. MIH\_LL\_Transfer.request
          1. Function

This primitive is used to transport parameters and link layer frames between the MN and a MIHF at the MN’s local PoS (i.e., OPoS) for the purpose of establishing a secure tunnel between the MN and the TPoS in an appropriate target network.

* + - * 1. Semantics of service primitive

MIH\_LL\_Transfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

TargetLinkInfoList,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

Nonce

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | Identifies a remote MIHF as the destination of this request. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional: included if the target link is known) Identifies the remote PoA as the corresponding peer of the L2 exchange.[[2]](#footnote-2) |
| TargetLinkInfoList | LIST (LINK\_PoA\_LIST) | (Optional) Information that the MN can provide to the OPoS for selection of the proper TPoS. This can include values and IEs from tables F.10, F.11, F.14, and G.1. |
| LLInformation | LL\_FRAMES | (Optional: included if the target link is known) Carries link layer frames. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS (TPoS) that will be the destination of the link-layer frames. |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover needs to be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |
| Nonce | NONCE | (Optional) Nonce (Nonce TLV) |

* + - * 1. When generated

This primitive is generated by an MIH user to send a link-layer frame for preregistration to the target PoS. The MN can send this primitive to instruct its OPoS to generate a Security Association with an appropriate TPoS, for instance so that the MN and the TPoS are able to carry out additional preregistration commands before handover to TPoA. The MN can include whatever information it has available about any suitable TPoA for use by OPoS to identify the proper TPoS. If the MN has sufficient information about TPoA to include layer 2 frames, those frames can also be supplied for secure delivery to TPoA. In this way, the number of round trips for preregistration may be minimized.

* + - * 1. Effect on receipt

If the TargetLinkIdentifier is not included, the OPoS shall use the TargetLinkInfoList (if included) to identify the appropriate TPoS that can initiate pre-registration activities with an appropriate TPoA. In the absence of other information, the OPoS can use available link-type information and location information for the MN to identify an appropriate TPoS. Some location information about the MN may be available by associating geographical coordinates with the MN’s current Point of Attachment (i.e., SPoA). After reception of this primitive, OPoS must generate an MIH\_LL\_Transfer request message towards the MIHF of the originating PoS, which must relay the link-layer frames transported in this message to the target PoS.

* + - 1. MIH\_LL\_Transfer.indication
         1. Function

This primitive is used by the local MIHF (i.e., OPoS) to notify the corresponding MIH user about the reception of an MIH\_LL\_Transfer request message.

* + - * 1. Semantics of service primitive

MIH\_LL\_Transfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

TargetLinkInfoList,

CandidateLinkList

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the invoker, f a MN in the same network as OPoS. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional)This identifies the remote PoA that is the corresponding peer of the L2 exchange[[3]](#footnote-3). This attribute shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) This carries link layer frames. This attribute may be included if the target link is known. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS |
| TargetLinkInfoList | LIST (LINK\_PoA\_LIST) | (Optional) Information that the MN can provide to the OPoS for selection of the proper TPoS. This can include values and IEs from tables F.10, F.11, F.14, and G.1. |
| CandidateLinkList | LIST(LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover needs to be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |

* + - * 1. When generated

This primitive is generated by a MIHF after receiving an MIH\_LL\_Transfer request message.

* + - * 1. Effect on receipt

If TPoSIdentifier is not provided, the MIH user application on the OPoS uses the information provided by the MN to identify an appropriate target PoS (TPos). If the TPoS is hosted remotely (e.g., in a separate target network), the MIH user application on the OPoS must generate an MIH\_N2N\_LL\_Transfer.request primitive for TPoS. Otherwise, or upon receipt of corresponding MIH\_N2N\_LL\_Transfer.response, the MIH user must generate an MIH\_LL\_Transfer.response primitive and transmit that response to the MIHF specified by the SourceIdentifier.

* + - 1. MIH\_LL\_Transfer.response
         1. Function

This primitive is used by an MIH user to provide the link-layer frames to the local MIHF.

* + - * 1. Semantics of service primitive

MIH\_LL\_Transfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

TPoSIdentifier,

MIRK,

MNmsrk,

Nonce,

SALifeTime,

Status )

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[4]](#footnote-4) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; included if and only if the corresponding MIH\_LL\_Transfer.indication contained LLInformation. |
| MNnetworkaccessid | MIHF\_ID | (Optional) Carries the MN’s Network Access Identifier in the case optimized pull key distribution is used. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS |
| MIRK | ENCR\_BLOCK | (optional) A shared key, Ktpos, encrypted to be recoverable by MN |
| MNmsrk | ENCR\_BLOCK | (optional) Media Specific root key (for use with EAP methods) |
| Nonce | NONCE\_VALUE | (optional) Nonce |
| SALifeTime | LifeTime | (optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS   1. Success 2. TPoS is identical to OPoS, use *K*opos 3. Failure 4. Code 3 (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated after receiving an MIH\_LL\_Transfer.indication primitive and possibly after receiving an MIH\_N2N\_LL\_Transfer.confirm primitive from the local MIHF. This primitive is generated after receiving an MIH\_N2N\_MNTN\_SA\_Estab.confirm primitive. After the OPoS has received the confirmation that the TPoS has accepted the Security Association, the OPoS MIHF issues this primitive so that the MN can complete the establishment of the secure tunnel. For this purpose, the OPoS has to supply the MIRK, MNmsrk, Nonce, and SALifeTime to the MN according to the formula specified in section 16.1

* + - * 1. Effect on receipt

The local MIHF may generate an MIH\_LL\_Transfer response message in order to provide the required information until the authentication or association process is finished.

* + - 1. MIH\_LL\_Transfer.confirm
         1. Function

This primitive is used to notify the corresponding MIH user about the reception of an MIH\_LL\_Transfer response message.

* + - * 1. Semantics of service primitive

MIH\_LL\_Transfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

TPoSIdentifier,

MIRK,

MNmsrk,

Nonce,

SALifeTime,

Status)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[5]](#footnote-5) |
| LLInformation | LL\_FRAMES | (Optional)This carries link layer frames. This attribute is included if and only if the corresponding MIH\_LL\_Transfer.request contained LLInformation. |
| MNnetworkaccessid | MIHF\_ID | (Optional) This carries the MN’s Network Access Identifier in the case optimized pull key distribution is used |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS |
| MIRK | ENCR\_BLOCK | (optional) A shared key, Ktpos, encrypted to be recoverable by MN |
| MNmsrk | ENCR\_BLOCK | (optional) Media Specific root key (for use with EAP methods) |
| Nonce | NONCE\_VALUE | (optional) Nonce |
| SALifeTime | LifeTime | (optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS   1. Success 2. TPoS is identical to OPoS, use *K*opos 3. Failure 4. (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated by the local MIHF after receiving an MIH\_LL\_Transfer response message.

* + - * 1. Effect on receipt

The MIH user on the MN may generate an MIH\_LL\_Transfer.request primitive unless the authentication or association processes are completed.

* + 1. MIH\_N2N\_LL\_Transfer

The primitives defined are to transport link-layer frames for the target link over the MIH protocol between the originating PoS and the target PoS. Preregistration is conducted between the MN and the target PoA. As part of preregistration, media specific authentication may be conducted with the media specific authenticator deployed in the target PoA..

* + - 1. MIH\_N2N\_LL\_Transfer.request
         1. Function

This primitive is used to transport link layer frames between the originating PoS and the target PoS.

* + - * 1. Semantics of Service Primitive

MIH\_N2N\_LL\_Transfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNID,

Nonce,

Encrypted Key,

CandidateLinkList

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this request. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional) Identifies the remote PoA as the corresponding peer of the L2 exchange; [[6]](#footnote-6) shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; shall be included if the target link is known. |
| MNID | MIHF\_ID | (Optional) MIHF\_ID of the MN to identify the MN’s Media Independent Root Key to be transferred to the target PoS. |
| MNmsrk | KEY | (Optional) MN’s Media Specific Root Key that has been transferred from the originating PoS. This parameter can be used only if the PoA supports EAP or ERP for media-specific access authentication. |
| Nonce | NONCE\_VALUE | A random number. |
| Encrypted Key | ENCR\_BLOCK | A shared key, *K*tpos, encrypted in a way recoverable by TPoS |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover needs to be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |

* + - * 1. When generated

This primitive is generated when the originating PoS receives an MIH\_LL\_Transfer request message, to relay preregistration signaling to the target PoS, possibly to relay link layer frames as well as possibly to establish a security association based on shared key *K*tpos,.

* + - * 1. Effect on receipt

The local MIHF shall generate an MIH\_N2N\_LL\_Transfer request message to the remote MIHF.

* + - 1. MIH\_N2N\_LL\_Transfer.indication
         1. Function

This primitive is used by the target MIHF to notify the corresponding MIH user of the reception of an MIH\_N2N\_LL\_Transfer request message.

* + - * 1. Semantics of service primitive

MIH\_N2N\_LL\_Transfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

MNID,

Nonce,

Encrypted Key,

LLInformation,

CandidateLinkList,

MNmsrk

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional)This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[7]](#footnote-7) This attribute shall be included if the target link is known. |
| MNID | MN\_ID | ID of the MN, used to index and compute the MN’s Media Independent Root Key to be established the target PoS |
| Nonce | NONCE\_VALUE | A random number. |
| Encrypted Key | ENCR\_BLOCK | A shared key, *K*tpos, encrypted in a way recoverable by TPoS |
| LLInformation | LL\_FRAMES | (Optional)This carries link layer frames. This attribute shall be included if and only the target link is known. |
| CandidateLinkList | LIST(LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover needs to be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |
| MNmsrk | KEY | (Optional) MN’s Media Specific Root Key that has been transferred from the originating PoS. This parameter can be used only if the PoA supports EAP or ERP for media-specific access authentication. |

* + - * 1. When generated

This primitive is generated by the target MIHF after receiving an MIH\_N2N\_LL\_Transfer request message.

* + - * 1. Effect on receipt

The TPoS MIH user must recover the *K*tpos according to the formula in Section 16.1 and install it as necessary in the target AAA function. The TPoS also must generate appropriate messages to the TPoA to install a MSPMK which will be used by MN as necessary when MN connects to the target network.

The MIH user must generate a MNnetworkAccessID associated with the MNID provided.

The MIH user must subsequently generate an MIH\_N2N\_LL\_Transfer.response primitive and include MNnetworkAccessID.

*K*tpos or MNmsrk will be further used to derive a key called a media-specific pair-wise master key (MSPMK) defined in 10.2.1.2. The MSPMK will be distributed to the target PoA using media-specific key distribution described in 10.2.2.

*Note to editor: Clauses 10.2.1.2 and 10.2.2 are defined in IEEE 802.21a-2012.*

* + - 1. MIH\_N2N\_LL\_Transfer.response
         1. Function

This primitive is used by an MIH user to provide the link-layer frames to the local MIHF.

* + - * 1. Semantics of service primitive

MIH\_N2N\_LL\_Transfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

SALifeTime,

Status

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[8]](#footnote-8) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; included if and only if the corresponding MIH\_N2N\_LL\_Transfer.indication contained LLInformation. |
| MNnetworkaccessid | MIHF\_ID | (Optional) Carries the MN’s Network Access Identifier when optimized pull key distribution is used. |
| SALifeTime | LifeTime | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS   1. Success 2. (TPoS is identical to OPoS), is not applicable. 3. Failure 4. (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated after receiving an MIH\_N2N\_LL\_Transfer.indication primitive.

* + - * 1. Effect on receipt

The target MIHF (TPoS) must generate an MIH\_N2N\_LL\_Transfer response message in order to provide the required information until the authentication is finished.

* + - 1. MIH\_N2N\_LL\_Transfer.confirm
         1. Function

This primitive is used to notify the corresponding MIH user about the reception of an MIH\_N2N\_LL\_Transfer response message.

* + - * 1. Semantics of service primitive

MIH\_N2N\_LL\_Transfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

Status

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[9]](#footnote-9) |
| LLInformation | LL\_FRAMES | (Optional) This carries link layer frames. This attribute is included if and only if LLInformation was contained in the corresponding MIH\_N2N\_LL\_Transfer.request |
| MNnetworkaccessid | MIHF\_ID | (Optional) This carries the MN’s Network Access Identifier when optimized pull key distribution is used |
| Status | STATUS | Status of the preregistration transfer with TPoS   1. Success 2. (TPoS is identical to OPoS), is not applicable. 3. Failure 4. (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated by the remote MIHF after receiving an MIH\_N2N\_LL\_Transfer response message.

* + - * 1. Effect on receipt

The OPoS MIH user generates an MIH\_LL\_Transfer.response primitive with the information obtained from this primitive. The OPoS also retrieves its stored value for *K*tpos which had previously been sent to TPoS, encrypts it, and makes it available for the MIH\_ LL\_Transfer.response.

* + 1. MIH\_IF\_PreReg\_Ready
       1. MIH\_IF\_PreReg\_Ready.request
          1. Function

This primitive is used by the SR-MIHF user to request preregistration on a target link interface of the MN.

* + - * 1. Semantics of service primitive

MIH\_IF\_PreReg\_Ready.request (

DestinationIdentifier,

ExecutionDelay

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies the local MIHF or a remote MIHF that will be the destination of this request. |
| ExecutionDelay | UNSIGNED\_INT(2) | Time (in ms) to elapse before the action needs to 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. |

* + - * 1. When generated

This primitive is generated by the SR-MIHF user to prepare preregistration of the target link.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the local SR-MIHF generates and sends an MIH\_IF\_PreReg\_Ready request message to the remote SR-MIHF identified by the Destination Identifer. The remote SR-MIHF issues Link\_IF\_PreReg\_Ready.request(s) to the specified lower layer link(s).

* + - 1. MIH\_IF\_PreReg\_Ready.confirm
         1. Function

This primitive is used by the SR-MIHF to confirm that MIH\_IF\_PreReg\_Ready response message was received from a peer SR-MIHF.

* + - * 1. Semantics of service primitive

MIH\_IF\_PreReg\_Ready.confirm (

SourceIdentifier,

Status

)

**Parameters**:

|  |  |  |
| --- | --- | --- |
| Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker of this primitive, which can be either the local MIHF or a remote MIHF. |
| Status | STATUS | Status of the operation. Code 3 (Authorization Failure) is not applicable. |

* + - * 1. When generated

This primitive is generated by the SR-MIHF on receiving an MIH\_IF\_PreReg\_Ready response message form a peer SR-MIHF.

* + - * 1. Effect on receipt































Upon receipt of this primitive, the SR-MIHF user can know success of preregistration preparation on the target link. However, if Status does not indicate “Success,” the recipient performs appropriate error handling.



1. Media independent handover protocols




   5. MIH protocol frame format
      1. General frame format

*Insert new description for the new SID value, 5, into Table L.1.*

|  |  |  |
| --- | --- | --- |
| Field name | Size (bits) | Description |
| MIH message ID (MID)  -- Service identifier (SID) | 4 | 5: Gateway Service |

* 3. MIH protocol messages



     4. MIH messages for command service
        1. MIH\_LL\_Transfer request

This message is used by an MIHF to request its OPoS initiate the establishment of a security association with an appropriate TPoS, and possibly to carry link layer frames to expedite an authentication. The corresponding primitive is defined in Section 7.4.29.1. A Nonce is included if and only if MN uses non-EAP-based MIRK and an MIRK has not been received from the originating PoS. TargetLinkInfoList is included if MN has information available about the desired target link.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=1, AID=10) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| TargetLinkInfoList (optional)  (TargetLinkInfolist TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| TPoSIdentifier (optional)  (TPoS Identifier TLV) |
| CandidateLinkList (optional)  (Link identifier list TLV) |
| Nonce (optional)  (Nonce TLV) |

*(Note to editor: Nonce TLV is defined in IEEE 802.21a-2012.)*

* + - 1. MIH\_LL\_Transfer response

This message is used for an MIHF to complete the establishment of a security association between an MN and an appropriate TPoS. The corresponding primitive is defined in Section 7.4.29.3. A Nonce is carried if and only if MN uses non-EAP-based MIRK and the Nonce has not been sent to the target PoS. An MIRK contains an encrypted *K*tpos. An MIRK and a SALifetime are carried if and only if non-EAP-based MIRK is used and the encrypted *K*tpos has not been distributed to the MN.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=2, AID=10) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| MNnetworkaccessid (optional)  (Network Access Identifier TLV) |
| CandidateLinkList (optional)  (Link identifier list TLV) |
| TPoSIdentifier (optional)  (TPoS Identifier TLV) |
| MIRK (optional)  (Media Independent root key TLV) |
| MNmsrk (optional) (Media Specific root key TLV) |
| Nonce (optional) (Nonce TLV) |
| SALifeTime (optional)  (Lifetime TLV) |
| Status  (Status TLV) |

*(Note to editor: Lifetime TLV is defined in IEEE 802.21a-2012.)*

* + - 1. MIH\_N2N\_LL\_Transfer request

This message is used for an MIHF to carry link layer frames to conduct an authentication. The corresponding primitive is defined in Section (*must be “section”*) 7.4.30.1. An MIRK may be carried either if non-EAP-based MIRK is used and an MNID is carried or if non-EAP-based MIRK is used and a Nonce and SALifetime are carried. When non-EAP-based MIRK is used, the MIRK contains an encrypted *K*tpos. -. See 9.2.2 for detailed usage of MNID and MIRK. An MNmsrk may also be carried when the PoA identified by the LinkIdentifier supports EAP or ERP for media-specific access authentication. A Nonce and a SALifetime are included if and only if non-EAP-based MIRK is used and the encrypted *K*tpos has not been distributed to the MN.

*Note to editor: Clauses 9.2.2 is defined in IEEE 802.21a-2012.*

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=1, AID=11) |
| **Source Identifier** = sending MIHF ID (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MNID (optional) (Mobile node MIHF ID TLV) |
| MIRK (optional) (Media Independent root key TLV) |
| MNmsrk (optional) (Media Specific root key TLV) |
| Nonce (optional) (Nonce TLV) |
| Encrypted Key (ENCR\_BLOCK TLV) |
| SALifeTime (optional) (Lifetime TLV) |

* + - 1. MIH\_N2N\_LL\_Transfer response

This message is used for an MIHF to complete the establishment of a security association between itself and the incoming MN. The corresponding primitive is defined in Section 7.4.30.3. The SALifeTime may be included if specified by the TPoS for the requested security association.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=2, AID=11) |
| **Source Identifier** = sending MIHF ID (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID (Destination MIHF ID TLV) |
| TargetLinkIdentifier  (Link Identifier TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| MNnetworkaccessid  (Network Access Identifier TLV)(optional) |
| SALifeTime (optional) (Lifetime TLV) |
| Status  (Status TLV) |

* + - 1. MIH\_IF\_PreReg\_Ready request

The corresponding MIH primitive of this message is defined in 7.4.31.1.

This message is transmitted to the remote MIHF to perform preparation of preregistration.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=13) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| ExecutionDelay  (Link Identifier TLV) |

* + - 1. MIH\_IF\_PreReg\_Ready response

The corresponding MIH primitive of this message is defined in 7.4.31.2.

This message returns the result of an MIH\_IF\_PreReg\_Ready request.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=13) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| Status  (Link Identifier TLV) |

* + - 1. MIH\_TNMN\_SA\_Estab request

This message is used by an MN MIHF to request its OPoS initiate the establishment of a security association with an appropriate TPoS. The corresponding primitive is defined in Section 7.4.32.1. TargetLinkInfoList is included if MN has information available about the desired target link.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=1, AID=14) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = OPoS MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| TargetLinkInfoList (optional)  (TargetLinkInfolist TLV) |
| TPoSIdentifier (optional)  (PoS MIHF ID TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |

* + - 1. MIH\_TNMN\_SA\_Estab response

This message is used by a OPoS MIHF to complete the establishment of a security association between an MN and an appropriate TPoS. The corresponding primitive is defined in Section 7.4.32.3. TargetLinkInfoList is included if MN has information available about the desired target link.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=3, AID=14) |
| **Source Identifier** = OPoS MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = MN MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| MNnetworkaccessid  (Network Access Identifier TLV)(optional) |
| MIRK (optional) (Media Independent root key TLV) |
| MNmsrk (optional) (Media Specific root key TLV) |
| Nonce (optional) (Nonce TLV) |
| SALifeTime (optional) (Lifetime TLV) |
| SA\_Status\_Code |

* + - 1. MIH\_N2N\_MNTN\_SA\_Estab Request

This message enables a OPoS MIHF to request that a TPoS MIHF initiate the establishment of a security association with an incoming MN. The corresponding primitive is defined in Section 7.4.33.1.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=1, AID=15) |
| **Source Identifier** = sending OPoS ID  (Source MIHF ID TLV) |
| **Destination Id**entifier = TPoS MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| TargetLinkInfoList (optional)  (TargetLinkInfolist TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| Nonce (Nonce TLV) |
| MNID (Mobile node MIHF ID TLV) |
| Encrypted Key (ENCR\_BLOCK TLV) |

* + - 1. MIH\_N2N\_MNTN\_SA\_Estab response

This message is used by a TPoS MIHF to complete the establishment of a security association between itself and the incoming MN. The corresponding primitive is defined in Section 7.4.33.3. The SALifeTime may be included if specified by the TPoS for the requested security association.

|  |
| --- |
| MIH Header Fields (SID=1, Opcode=3, AID=15) |
| **Source Identifier** = TPoS MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = OPoS MIHF ID  (Destination MIHF ID TLV) |
| MNnetworkaccessid  (Network Access Identifier TLV)(optional) |
| SALifeTime (optional) (Lifetime TLV) |

* + 1. MIH messages for gateway service

MIH gateway service is the service to deliver layer 2 or other interworking messages using SID, “5”. For this kind of delivery services, the MIH message is used as a kind of container of the layer 2 or other interworking messages. The delivered messages can be identified by AID, as shown in Table L.1.Messages in Table L.1 can be explained as follows.

* + MIH\_L2Message\_Delivery: The MIH message for gateway service is used to deliver the layer 2 message.
  + MIH\_ANQP\_Delivery: The MIH message for gateway service is used to deliver the ANQP message for the IEEE 802.11 network.
  + Reserved for other interworking protocols: These AID values are reserved for supporting further interworking protocols.
  + Reserved for vendor specific area: These AID values are reserved for supporting vendor specific messages.
    - 1. Request message for gateway service

Gateway service message is delivered after MIH header encapsulation. Thus, the message format of gateway service is the same as follows.

|  |
| --- |
| MIH Header Fields (SID=5, Opcode=1, AID) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| L2 message or other interworking message depending on the AID value |

* + - 1. Response message for gateway service

This message returns the result of Request message for gateway service.

|  |
| --- |
| MIH Header Fields (SID=5, Opcode=2, AID) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| L2 message or other interworking message depending on the AID value |

1. MIH protocol protection


   3. Key establishment through an MIH service access authentication

*Modify clause 9.2.2 (defined in IEEE 802.21a) as follows:*

* + 3. Key derivation and key hierarchy

Upon a successful MIH service access authentication, the authenticator (i.e., PoS) obtains a master session key (MSK) or a re-authentication master session key (rMSK). Alternatively, via an optimized pull key distribution process, a Target PoS can obtain a 64-octet MIRK (Media-Independent Root Key) from a Originating PoS (see clause 9.2.2.2). The MIRK and the MIHF identifier of the MN that holds the MIRK are used as the symmetric key credentials for a symmetric key based method (e.g., EAP-GPSK) to perform MIH service access authentication between the MN and the target PoS without necessarily communicating with the authentication server located in the MN’s home network.

There are two options to generate an MIRK. In the first option (i.e., EAP-based MIRK), an MIRK is derived from a master session key (MSK) or re-authentication MSK (rMSK) established between the MN and the Originating PoS via MIH service access authentication using EAP. In the second option (i.e., non-EAP-based MIRK), an MIRK is generated by the Originating PoS independently of the MIH SA established between the MN and Originating PoS and distributed to the MN as well as the Target PoS. The first option is described in 9.2.2.2. The second option is described in 11.7.1.

* + - 1. Derivation of media independent session keys (MISKs)
      2. EAP-based MIRK

During an optimized pull key distribution process that involves the MN, the originating PoS and a target PoS, the originating PoS derives a MIRK for a specific target PoS. Strings used in the computation (e.g., MN\_MIHF\_ID, “MIRK”) are never zero terminated. For MIRK derivation, the following notations and parameters are used:

* *K* - key derivation key. The length of *K* is determined by the pseudorandom function (PRF) used to calculate a master session key (MSK) or re-authentication MSK (rMSK). If HMAC-SHA-1 or HMAC-SHA-256 is used as a PRF, then the full MSK or rMSK is used as the key derivation key, *K*. If CMAC-AES is used as a PRF, then the first 128 bits of MSK or rMSK are used as the key derivation key, *K*.
* *L* - The binary length of derived keying material MIRK. *L*=512 bits for the MIRK.
* *h* - The output binary length of PRF used in the key derivation. That is, *h* is the length of the block of the keying material derived by one PRF execution. Specifically, for HMAC-SHA-1, *h* = 160 bits; for HMAC-SHA-256, *h* =256 bits; for CMAC-AES, *h* = 128 bits.
* *n* - The number of iterations of PRF in order to generate *L*-bits of keying material.
* Nonce-T and Nonce-N - The nonces exchanged during the execution of service access authentication.
* c - The ciphersuite code is a one octet string specified for each ciphersuite. The codes are specified in section 9.2.3.
* *v* - The length of the binary representation of *n* (the counter) and *L* (the length of keying material). The default value for *v* is 32 (i.e., *n* and *L* are 32 bit variables).
* [*a*]2 - Binary representation of integer *a* with a given length.
* MN\_MIHF\_ID – Mobile node’s MIHF identity.
* PoS\_MIHF\_ID – Target PoS’s MIHF identity.
* “MIRK” - 0x4D49524B, i.e., the ASCII code in hex for string “MIRK”.

**Fixed input values**: *h* and *v*, *L*=512 bits.

**Input**: K, Nonce-T, Nonce-N, and ciphersuite code c.

**Process**:

a) *n* := ⌈*L*/*h*⌉; /\* ⌈*x*⌉ is the ceiling function, returning the least integer *n* >= *x* \*/

b) If *n* > 2*v* -1, then indicate an error and stop.

c) Result (0) := empty string.

d) For *i* := 1 to *n*, do

i) K(*i*) := PRF (K, “MIRK” || [*i*]2 || Nonce-T || Nonce-N ||

MN\_MIHF\_ID || PoS\_MIHF\_ID || c || [*L*]2).

ii) Result(*i*) := Result (*i*-1) || K(*i*).

e) Return Result (*n*) ; MISK is the leftmost L bits of Result (*n*).

Output: MIRK

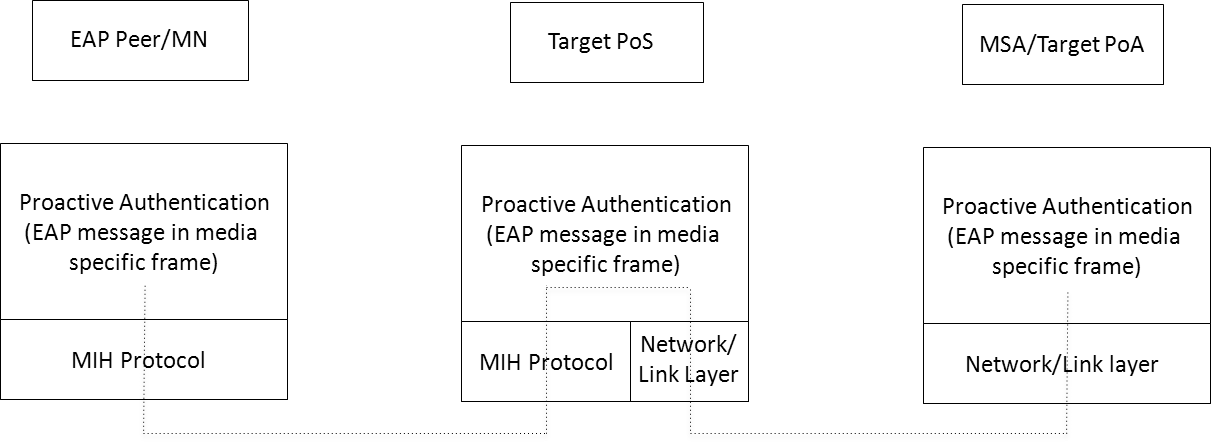
It is important to note that the key distribution of a MIRK from the Originating PoS to the target PoS may produce a security weakness so-called “domino effect” [IETF RFC 4962]. This weakness implies that the compromise of the originating PoS will also compromise the security association between the MN and the target PoS, since an attacker can know and derive the MIRK that is delivered to the target PoS. Reducing the latency of proactive authentication based on transferring a MIRK is at the cost of taking such a risk.

1. Proactive Authentication
   1. Media specific proactive authentication

*Change first paragraph of 10.1 (defined in IEEE 802.21a) as follows:*

In a media access proactive authentication, a Target PoS (TPoS) passes authentication messages between the mobile node and a media specific authenticator (MSA). The protocol stacks in each interface are illustrated in ~~Figure 43~~ Figure 46 and Figure 47. In scenarios where MSA/Target PoA is reachable via same media as MN and TPoS, EAP messages received at TPoS are directly forwarded to the target PoA. In an optimized pull key distribution, an Originating PoS (OPoS) passes authentication messages between the mobile node, the target PoS and a media specific authenticator (MSA).

*Replace Figure 46 (defined in IEEE 802.21a) as follows:*



*Insert new figure, renumber existing figure 47*

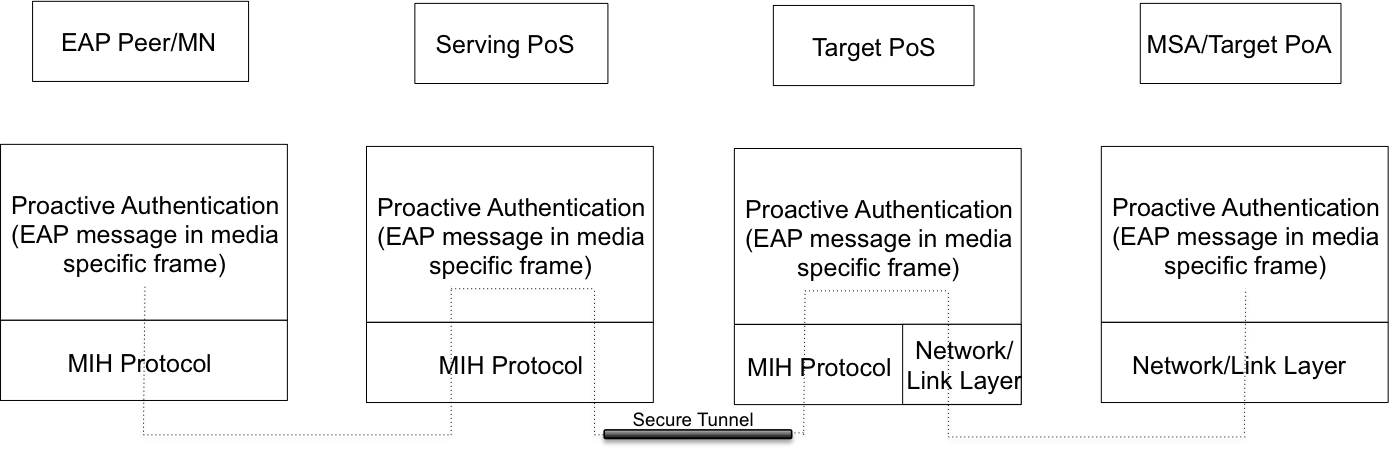


Figure 47—Protocol Stack for MIH Supported optimized pull key distribution with two Points of Service (PoS)

*Insert second paragraph of 10.1 below Figure 47 as follows:*

Figure 47 illustrates the protocol stacks and message passing when the Originating PoS (OPoS) (called Serving PoS in Figure 47) is in a different network than the TPoS.

*Insert following new Clause 10.3*

* 3. Establishing Security Association roaming partners for MIH

The PoS is a convenient and natural place to locate security functions, and roaming partners have in place agreements that can be used to beneficially establish the needed security agreements between different PoSes in partner networks. It is expected that in many cases the PoS functions in partner networks must communicate by data paths that traverse the external Internet; in such cases, a secure communication channel must exist or must be established between the partners. It is out of scope for this document to specify exactly how the secure communication channel should be established, but this can be done by configuration when the partners enter into their roaming agreement. It can also be done on demand by using IKEv2 [IETF RFC 5996]. The following overview describes in more detail the circumstances enabling dynamic establishment of security association between OPoS and TPoS.



**Figure 49: MN handover signaling for preregistration using OPoS**

Except for the initial network attach, by the time a MN enters a network, it can also have a security relationship with the PoS in that network by using the protocol in this document. For each visited network, this security relationship can be 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, then the MN is expected to already have a security association with HPoS; otherwise, the MN can bootstrap this security association using IKEv2 or standard AAA mechanisms or other proprietary means.

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 point of attachment (PoA); the current network is termed the "source" network, and the PoS in the originating network is abbreviated as the OPoS. As the MN moves from one partner network to the next (i.e., to a new "target network"), the MN establishes or renews a security association with the PoS in the target network (i.e., the "TPoS"). When handover is completed, the TPoS naturally becomes the local PoS (OPoS).

In order to enable wider application of high-performance handovers and in particular preregistration signaling, security must be guaranteed for the control traffic. From above, we see that 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 target PoS. The process of establishing such a security association can be quite time consuming and often expensive in processor cycles as well. This clause specifies a much faster and easier method for providing security associations as needed between the MN and the target PoS in any target network within the networks covered by the roaming partners.

MIH\_MNTN\_SA\_Estab and MIH\_N2N\_LL\_Transfer messages exchanged between the originating PoS and the target PoS may require security protection. Furthermore, the target PoS may reject these messages from an unauthorized originating PoS. To protect the link between the originating PoS and the target PoS several approaches are possible.

An MIH SA (Security Association) defined in IEEE 802.21a can be used for protecting the communications between the originating PoS and the target PoS. In this case, the originating PoS acts as the initiating end-point of an MIH SA and the target PoS as the other end-point of the MIH SA. As specified in IEEE 802.21a, the MIH SA can be established using (D)TLS over MIH or EAP over MIH.

Other mechanisms such as IPSec and TLS over TCP can also be used for protecting the communications between the originating PoS and the target PoS. Details on such mechanisms are outside the scope of this standard.

* + 1. Key distribution by OPoS

This section specifies one algorithm to allow OPoS to distribute a shared key to the MN and to its desired TPoS. The shared key is then used as the basis for a secure communications channel between the MN and the TPoS, enabling further secure preregistration activities. The notation for PoS-based handover keys is listed in Table X.

Table X—Key notation for PoS-based handover

|  |  |
| --- | --- |
| *K*hgw | key between MN and HGW |
| *K*opos | key between MN and OPoS |
| *K*tpos | key between MN and TPoS; *K*tpos is also referred to as the Media Independent Root Key (MIRK). |
| *K*hopos | key between HPoS and OPoS |
| *K*htpos | key between HPoS and TPoS |
| *K*stpos | key between OPoS and TPoS |
| PNGopos | pseudo-random number generator between MN and OPoS |
| PNGhopos | pseudo-random number generator between HPoS and OPoS |
| PNGstpos | pseudo-random number generator between OPoS and TPoS |

As mentioned in the foregoing discussion, when the MN has determined that a handover is needed to a new network, we may assume that the MN has a security association with a service in its home network, here called the Home Gateway (HGW), based on a key *K*hgw . Interactions between the MN and its Home Gateway are out of scope for this protocol specification document. We also assume that, because of previous protocol operations, the MN has a current security association with the PoS in the originating network (OPoS). This security association is bidirectional and based on a share key *K*opos.

Suppose the MN determines to move to a new network, the target network. Then the MN needs to preregister, and thus needs to use the PoS in target network (TPoS). Before it can do this, it needs to discover the address of TPoS and establish a security association with TPoS using *K*tpos.

UE can make use of its existing security association with OPoS, because OPoS either already has, or can readily establish, a security association with TPoS. Suppose OPoS already has the required security association with TPoS. Then, when MN begins forwarding preregistration traffic to TPoS via OPoS, OPoS will provide MN and TPoS with a shared key, *K*tpos, for use to protect the remainder of the MN's signaling traffic with TPoS. According to this proposal, the OPoS would thus forward the initial traffic to TPoS on behalf of the MN; the OPoS uses its own security relationship with TPoS to protect this initial preregistration signaling, and it also supplies the value of *K*tpos to TPoS by adding a new extension to the preregistration traffic.

To send Ktpos to TPoS, OPoS provides the following payload within the TLVs of MIH\_MNTN\_SA\_Estab Request, a new 802.21(c) message:

Payload = MNnetworkaccessid, Nonce, [*K*tpos ⊕ PNGstpos (MNnetworkaccessid, Nonce)]

Upon receiving this payload, TPoS calculates PNGstpos (MNnetworkaccessid, Nonce) and XORs the result to the third parameter of the payload to recover *K*tpos.

Similarly, to send Ktpos to MN, OPoS provides the following payload within the TLVs of MIH\_TNMN\_SA\_Estab Response, a new 802.21(c) message:

Payload = TPoSIdentifier, Nonce, [*K*tpos ⊕ PNGopos (TPoSIdentifier, Nonce)]

Upon receiving the payload, MN calculates PNGopos (TPoSaddr, nonce) and XORs the result to the third parameter of the payload to recover *K*tpos.

Alternatively, for both of these messages, the entire contents could be encrypted by OPoS using the keys it has available with TPoS and MN respectively. MN is allowed to send more signaling information to TPoS via OPoS even after OPoS distributes the keys; OPoS continues to forward traffic back and forth between MN and TPoS as needed until both endpoints have used *K*tpos to establish the required security association. For best performance and least likelihood of congestion at OPoS, MN and TPoS should begin to use direct signaling as soon as possible and thus bypass OPoS. Other structures for the message payloads are also possible, depending on requirements.

Once the handover is completed, TPoS "becomes" OPoS and the handover cycle can begin anew whenever MN determines the need for the next handover.

* + 1. TPoS selection by OPoS

It is possible for OPoS to take a more active role to promote smooth handover. When the UE determines the need for handover, but does not already know the address of the TPoS for the intended target network, the MN can start the preregistration sequence by sending all the known information to the OPoS. Subsequently, the OPoS will provide the address of the TPoS to the MN along with *K*tpos, just as described above. The exact nature of the information about TPoS provided by the MN is dependent on the radio access technology type (RAT) of the target network, and may be specified in detail in later revisions of this document. Other alternatives for identifying the target network access point are also envisioned. For MNs configured with ANDSF software, detailed information about TPoS, and the other entities within the target network can easily be made available. Note, however, that discovery and secure communication with TPoS may be easier than discovery and secure communication with ANDSF.

1. Single Radio Handover

*Insert new clause 11*

* 1. Introduction (keep in reduced version)

In a single radio handover, a mobile node can transmit on only one radio at a time. This enables design simplifications that contribute to lower cost and longer battery life for the mobile device, appealing especially to the consumer market. Designing for single radio operation requires that one radio transmitter must be disabled before another radio interface can begin transmitting packets; this leads to a mode of operation commonly referred to as “break-before-make”. Multi-transmitter designs allow for simper designs for smooth handovers because the handover signaling has access to both origin and target networks at the same time. For single radio, the handover must be designed to accomplish as many handover functions as possible in the origin network before breaking communication and re-tuning to the target network. This typically includes preregistration in the target network, so that link establishment and device authentication can be accomplished as quickly as possible when the radio is re-tuned. Only after link establishment and authentication are complete can the mobile device continue running its desired applications. There is inevitably some short time during which communication is impossible, and it is the objective of this standard to minimize the disruption so that it does not adversely affect the applications or the user experience.

* 1. Major single radio handover processes

A single radio handover following the reference model in Section 5.4 may consist of different handover processes and involve different information elements (Section 7) and messages (Section 8). Examples of handover are described in Annex N. Figure 11.7 shows the single radio handover procedures consisting of 5 processes as described below.

**Figure 50 –Single radio handover procedures.**

1. Network discovery: determine whether or not there is a candidate target network available for handover. In network discovery, the MN queries the Information Repository to discover candidate networks and their handover policies. Such information includes whether candidate networks and MN support SRHO or not, and the presence of Proxy GW on the candidate network. Network discovery also allows the MN to acquire the corresponding system information blocks of candidate PoAs to perform the radio measurements. Alternatively, the MN may request that the Source Network PoS identify one or more candidate target networks.
2. The handover decision may involve the following
   * 1. A handover trigger.
     2. Target network selection
     3. Proxy gateway discovery.
     4. Evaluating the handover benefit: the evaluation can be made by the MN or the network, e.g., based on parameters such as signal strength, cost, and operator policy.
3. Preregistration includes pro-active authentication and establishing context (user identity, security, resource information) at the target network. Possibly with the help of Proxy GW, the MN can perform network entry procedures towards the target network while still retaining its data connection with the source network. Optionally, the preregistration process may occur before the network selection process as in the case of WiMAX target networks.
4. Target link preparation: the MN and target network prepare the establishment of the target link. This process 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.
5. SRHO execution process. Here, 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 protocol, and future incoming packets are then routed to the target radio.



*Insert new Clause 12*

1. Gateway Service
   1. Introduction

The Gateway bridges the signaling between the MN and the target network via the source network. When the MN signals to the Proxy GW as if signaling to a point of attachment (PoA), the target PoA may respond by signaling to the Proxy GW which acts like a virtual MN. The Proxy GW may also behave like a virtual PoA to signal with the target PoA. The control frames from the MN tunneled via the source network to the target network are consumed at the Proxy GW, which processes these control frames. Before replying to the control frames, the Proxy GW may communicate with the appropriate network entities in the target network to enable conducting any needed functions requested in the control frame. This gateway in the control plane may therefore proxy any control functions in general, including but not limited to preregistration and proactive authentication of the MN. Such proxy function in the control plane resides in the gateway as shown in Figure 11.2, and its single radio handover control functions may be implemented by the media independent point of service (PoS), as defined in this Clause. The Proxy GW often needs some location management and network service information to perform its function. It may cache the needed information.

The Proxy functions may be located at gateway router of the destination network. In the WiMAX network, these functions may make use of the Signal Forwarding Function (SFF).

In a target WiMAX network, the Proxy functions may be implemented in as an extension of the Signal Forwarding Function (SFF) and may reside at the ASN-GW.

In a target 3GPP network, the Proxy functions may be implemented as an extension of the Mobility Management Entity (MME).

In a target 3GPP2 network, the Proxy functions may be implemented in the HRPD-SFF and the existing functions of the Packet Control Function (PCF).

Control signals between the MN and the GW are provided in a media independent manner. Such signaling uses MIH messages defined in this specification.

In a distributed mobility management design, each network has a mobility routing function. The mobility routing function enables a router to forward packets towards a mobile node according to the new location of a mobile node. The logical functions of mobility routing and of the Proxy may be co-located. The distributed mobility management architecture is then shown in Figure 11.2 in which the Information Repository contains the logical function of location management information only and the GW contains the logical function of mobility routing only.

The Proxy GW works as a gateway to bridge the mobility signaling between a MN and a target network via the source network. The Proxy GW can transfer L2 messages to the target network via the source network, as shown in Figure 52 (b). Moreover, the Proxy GW can convert the L2 messages to other control messages for the target network as a proxy between the MN and the target PoA, as shown in Figure 53 (b).

If the Proxy GW can transfer or convert interworking protocol messages such as ANQP or ANDSF messages, the Proxy GW can enhance cooperation with the network using other interworking protocols.

For the transfer function of the interworking protocol message, the “Gateway Service” means only encapsulation of interworking protocol messages into MICF header on top of the TCP or UDP/IP layer. The transfer function of the interworking protocol message is simple, and thus can be implemented in the PoA without full function of MIH. Use of the transfer function can reduce complexity of the PoA.

For the conversion function of the interworking protocol messages to the other control messages, the Proxy GW can convert encapsulated interworking messages such as ANQP messages to the other control messages. The conversion function can enhance bridging of mobility signaling for the Proxy GW.

For transfer and conversion of the L2 messages or other interworking protocols, the SID for “Gateway Service” is defined as “5.” The “Gateway Service” reduces system complexity and increases compatibility to the other networks.

* 1. Communication between the MN and the target PoA < Was 11.1.4>

The MN needs to communicate eventually with the target PoA to prepare for handover by performing network access procedure with the target access network. The first part of this communication is the transport of TCP or UDP / IP packets to a target PoS (TPoS) in the target network; the MN may (for example) query the Information Repository to find the IP address of the TPoS in order to use this TCP or UDP / IP transport. The second part of this communication depends on whether the target PoA supports MIHF in the 802-architecture or whether it is a legacy PoA lacking such support.

If the target PoA supports MIHF, the network entry L2 frame is encapsulated into an MIH frame to forward to the target radio. Figure 11.5 shows the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the Proxy GW via the source radio interface, in the absence of the target link. The Proxy GW bridges between the MN source link and the target PoA. Fig 12.2 shows the protocol stack resulting from the cross-layer encapsulation after passing through these two MIHFs.

L2(2)

L2(2)

L2(2)

L2(2)

MIH

L3 + L4

L2(1)

L2

PHY(2)

PHY(1)

PHY

PHY(2)

MN

Target

PoA

L2(2)

MIH

L2

PHY

MIHF for Target PoA

L3 + L4

L3 + L4

MIH

**Figure 51: Transport of L2 frame of target interface via MIH using the logical connection at the Target PoS to MIH-capable target PoA, showing the resulting protocol stack.**

If MN cannot send L2 frames to the target PoA, it will rely on a Proxy GW function of the MIHF in order to perform network entry procedure. As before, the SRC frame is sent as the payload of a TCP or UDP / IP packet destined to the Proxy GW as described above. The SRC frame contains information for the target network to identify the target PoA. The Proxy GW will handle target-side communications with the target PoA.

Figure 12.3 shows the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the Proxy GW via the source radio in the absence the target link. The GW communicates with the target PoA using other control messages in order to proxy between the MN and the target PoA. The figure shows the protocol stack resulting from the cross-layer encapsulation after passing through the Proxy GW.

L2(2)

L2(2)

Control

Control

MIHF

MIHF

message

message

TCP or UDP / IP

TCP or UDP /

IP

TCP or

UDP / IP

TCP or

UDP / IP

L2(1)

L2

L2

L2

PHY(1)

PHY

PHY

PHY

MN

GW

Target

PoA

**Figure 12.3 Transport of L2 frame of target interface to the GW which proxies between the MN and the target PoA, showing the resulting protocol stack.**

* 1. L2 Message Transfer (SID=5, AID=1)

As shown in Table L.1, if AID is equal to one, the L2 messages are exchanged between the MN and the target PoA through the source network.

If the target PoA supports MICF and MN does not know the IP address of the target PoA, the Proxy GW functions like a proxy for the MN to send the target radio L2 network entry packets to the target PoA, as shown in Figure 52 (b). If the target PoA does not support MICF, the Proxy GW communicates with the target PoA using other control messages in order to proxy between the MN and the target PoA, as shown in Figure 53 (b).

* 1. Interworking Protocol Delivery (SID=5, AID>1)

As extension of L2 message transfer, the transfer of interworking protocol message, as shown in Figure 57, can be considered. If the target network entity supports “Gateway Service,” the PoA can only encapsulate interworking protocol messages with the MICF header using the SID, “5.” The PoA uses the encapsulated messages to communicate with the target network entity. The PoA only encapsulates interworking protocol messages without full function of the MIH. It means the implementation of the PoA can be simplified.

**Figure 57. Gateway Service for Interworking Protocol Message Transfer**

As extension of L2 message conversion, the interworking protocol message conversion as shown in Figure 58, can be considered. If the other network entity does not support “Gateway Service,” the Proxy GW converts the interworking protocol message into the control message for the other network entity. The control message can be a different interworking protocol message. The Proxy GW functions as a proxy with other interworking protocols to communicate with other interworking network entity, and thus enhances mobility signaling.

**Figure 58. Gateway Service for Interworking Protocol Message Conversion**

* + 1. Examples of Interworking Protocol Delivery: ANQP Delivery

If the MN wants to receive ANQP messages of access network information from the Media Independent Information Server, the WLAN AP (Access Point) can perform as a proxy between the MN and information server as shown in Figure 59 (a). The WLAN AP only encapsulates or decapsulates messages from the MN or the information server as shown in Figure 59 (b). The WLAN AP does not need to have all functions of the MIH. It means the WLAN AP as a proxy of MN can be implemented with simple MIH function with SID, “5.”

**(a) ANQP Transfer using the WLAN AP as a Proxy**

**(b) Protocol Stacks for ANQP Transfer**

**Figure 59. ANQP Transfer from Media Independent Information Server**

If the information server does not support MIH functions, the WLAN AP cannot communicate with the information server using the MIH protocol messages. In this case, the Proxy GW is needed as a proxy between the WLAN AP and the information server. As shown in Figure 60 (a), the WLAN AP only encapsulates or decapsulates messages from the MN, and Proxy GW converts the messages from the WLAN AP to the other interworking protocol messages, such as ANDSF messages. Hence, the information server can communicate with the WLAN AP via the Proxy GW. To explain the ANQP conversion, the protocol stacks for MN, WLAN AP, Proxy GW, and information server are shown in Figure 60 (b).

**(a) ANQP Conversion using the Proxy GW**

**(b) Protocol Stacks for ANQP Conversion**

**Figure 60. ANQP Conversion from Media Independent Information Server**

# 

(informative)

# Bibliography

*Insert these normative references in appropriate order.*

1. IEEE 802 standard, “IEEE Draft Standard for Local and metropolitan Area Networks: overview and Architecture, P802-D1.4, June 2012.
2. 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” TS23.401.
3. 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses,” TS23.402
4. WiMAX Forum Network Architecture: Stage 3 Detailed Protocols and Procedures T33-001-R015
5. WiMAX Forum, “Single radio interworking,” WMF-T37-011-R016v01.
6. WiMAX Forum, “WiFi-WiMAX Interworking,” WMF-T37-010-R016v01.
7. 3GPP2, “WiMAX-HRPD Interworking: Core network aspects,” X.S0058.
8. IETF RFC 6153 (2011-02), DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery

# 

# 

# 

# 

*Insert following Data Type to Table E.1.*

|  |  |  |  |
| --- | --- | --- | --- |
| MIH\_LINK\_SAP\_primitive | | IEEE Std 802.16 C\_SAP | IEEE Std 802.16 M\_SAP |
| Link\_Action | Link\_RX\_ON | N/A | N/A |

# 

(normative)



## Derived data types



### Data types for link identification and manipulation

*Insert number 5 in the description of LINK\_PARAM\_GEN in Table F.4*

|  |  |  |
| --- | --- | --- |
| Data type name | Derived form | Description |
| LINK\_PARAM\_GEN | UNSIGNED\_INT(1) | 5: Average power consumption in active state- the parameter value is represented as an UNSIGNED\_INT(2). its measure is mW.  Value Range: 0 – 216-1 mW  6-255: (Reserved) |

*Insert Following Data Type to Table F.5*

|  |  |
| --- | --- |
| Action name | Description |
| Link\_RX\_ON | Turn on only the receiver of the radio |



### Data types for information elements

### 

### 

### 

### 

*Change Table F.13 as follows:*

**Table F.13 – Data types for information elements**

|  |  |  |
| --- | --- | --- |
| Data type name | Derived from | Definition |
| NET\_CAPS | BITMAP(32) | These bits provide high level capabilities supported on a network.  Bitmap Values:  Bit 0: Security – Indicates that some level of security is supported when set.  Bit 1: QoS Class 0 – Indicates that QoS for class 0 is supported when set  Bit 2: QoS Class 1 – Indicates that QoS for class 1 is supported when set  Bit 3: QoS Class 2 – Indicates that QoS for class 2 is supported when set; Otherwise, no QoS for class 2 support is available.  Bit 4: QoS Class 3 – Indicates that QoS for class 3 is supported when set; Otherwise, no QoS for class 3 support is available.  Bit 5: QoS Class 4 – Indicates that QoS for class 4 is supported when set; Otherwise, no QoS for class 4 support is available.  Bit 6: QoS Class 5 – Indicates that QoS for class 5 is supported when set; Otherwise, no QoS for class 5 support is available.  Bit 7: Internet Access – Indicates that Internet access is supported when set; Otherwise, no Internet access support is available.  Bit 8: Emergency Services – Indicates that some level of emergency services is supported when set; Otherwise, no emergency service support is available.  Bit 9: MIH Capability – Indicates that MIH is supported when set; Otherwise, no MIH support is available.  Bit 10: SRHO Capability – Indicates that SRHO is supported when set; Otherwise, no SRHO support is available.  Bit ~~10~~ 11–31: (Reserved) |
| IP\_TUNN\_MGMT | BITMAP(16) | Indicates the supported tunnel management protocol on PoS.  Bitmap Values:  Bit 0: IPSec  Bit 1–15: (Reserved) |



### Data type for security

*Insert Following Data Types into Table F.24*

|  |  |  |
| --- | --- | --- |
| Data | Derived from | Definition |
| LL\_FRAMES | OCTET\_STRING | One or more link-layer frame(s).  (Note: LL\_FRAMES is defined in 802.21a-2012, but its Description needs to be overridden to cover both 802.21a and 802.21c use cases. |
| TPoS\_ID | CHOICE(IP\_ADDR, MIHF\_ID) | Represents the identifier of the target PoS |

# 

(normative)

*Insert following Information element identifiers values into Table G.1*

**Table G.1—Information element identifier values**

|  |  |
| --- | --- |
| Name of information element or container | IE Identifier |
|  |  |
| IE\_PoS\_TUNN\_MGMT\_PRTO | 0x10000209 |
| IE\_PoS\_FQDN | 0x1000020A |
| IE\_CONTAINER\_PoS | 0x10000303 |

IE\_PoS\_IP\_ADDR is already defined in IEEE 802.21a-2012.

# 

# 

# 

# 

# 

(normative)

*Insert the following rows to Table L.1*

|  |  |
| --- | --- |
| MIH messages | AID |
| MIH messages for Service Management | |
| MIH\_LL\_Transfer | 10 |
| MIH\_N2N\_LL\_Transfer | 11 |
| MIH messages for Command Service | |
| MIH\_IF\_PreReg\_Ready | 13 |
| MIH\_TNMN\_SA\_Estab | 14 |
| MIH\_MNTN\_SA\_Estab | 15 |
| MIH messages for Gateway Service | |
| MIH\_L2Message\_Delivery | 1 |
| MIH\_ANQP\_Delivery | 2 |
| Reserved for other interworking protocols | From 3 to 500 |
| Reserved for vendor specific area | From 501 to 1023 |

*Insert the following TLVs to Table L.2*

|  |  |  |
| --- | --- | --- |
| TLV type Name | TLV type value | Data type |
| Media Independent Root Key | 78 | KEY |
| Media Specific Root Key | 79 | KEY |
| TPoS Identifier TLV | 80 | TPoS\_ID |

# 

# 

(informative)

*Change the number N.6 in 802.21a to N.5*

N.~~6~~5 Termination Phase

*Insert N.6 after N.5*



## Use of MIH\_LL\_Transfer and MIH SA\_Estab messages for the exchange of L2 frames, including Optimized SA Establishment

This first call flow shows how the identity is bootstrapped by TPoS, how the MIRK[[10]](#footnote-14) is sent by the OPoS to the TPoS and how the MSPMK[[11]](#footnote-15) is installed into the TPoS (AAA). Notice that the SPoA does not conceptually play any role in the signal handling, even though signals exchanged between the MN and the OPoS are transmitted through the SPoA.



The signaling diagram illustrated in Figure N.6 1 shows the following steps

1. MIH\_TNMN\_SA\_Estab.request: the MN user application asks to initiate preregistration to a suitable target PoA (TPoA)
2. MIH\_TNMN\_SA\_Estab Request: MN’s MIHF transmits request to Originating PoS (OPoS)
3. MIH\_TNMN\_SA\_Estab.indication: OPoS presents MN’s Request to OPoS MIH user application.
4. MIH\_N2N\_MNTN\_SA\_Estab.request: issued by OPoS MIH user containing information to enable TPoS to compute MIRK (i.e., *K*tpos)
5. MIH\_N2N\_MNTN\_SA\_Estab Request: relayed by OPoS to TPoS, possibly encapsulated with IPSec
6. MIH\_ N2N\_MNTN\_SA\_Estab.indication: presented to TPoS MIH user for extraction of *K*tpos and computation of MNmsrk
7. TPoS MIH application provides MIRK to AAA for future authentication purposes
8. TPoS MIH user computes MNmsrk from MIRK and sends appropriate LL frames to TPoA for key distribution and any other preregistration tasks.
9. MIH\_N2N\_MNTN\_SA\_Estab.response: TPoS MIH user initiates message for OPoS MIH user containing MNnetworkaccessid.
10. MIH\_N2N\_MNTN\_SA\_Estab Response: TPoS relays message to OPoS containing MNnetworkaccessid.
11. MIH\_N2N\_MNTN\_SA\_Estab.confirm: OPoS presents message to OPoS MIH user containing MNnetworkaccessid.
12. MIH\_TNMN\_SA\_Estab.response: OPoS MIH user initiates message to MN user application via OPoS containing MNnetworkaccessid, MIRK.
13. MIH\_TNMN\_SA\_Estab Response: OPoS relays message to MIHF at MN containing MNnetworkaccessid, MIRK.
14. MIH\_TNMN\_SA\_Estab. confirm: MIHFat MN relays message to MN user application containing MNnetworkaccessid, MIRK.
15. MN user application extracts MIRK, computes MNmsrk, continues any necessary preregistration activities

In the second one, the authentication between the MN and the TPoA is depicted. MNmsrk is installed on the TPoS in the bootstrap process in the first figure. After that, TPoS holds the MNmsrk and uses it for media-specific authentication in the next figure. Therefore, another MNmsrk transfer is not needed in the next figure.



In the case the MN can directly contact the TPoS (this case is the same as when OPoS and TPoS are the same entity) the following example diagram applies for authentication at the TPoA:



The signaling diagram illustrated in Figure N.6 3 shows the following steps.

1. MIH\_TNMN\_SA\_Estab.request: the MN user application asks to initiate preregistration to a suitable target PoA (TPoA)
2. MIH\_TNMN\_SA\_Estab Request: MN’s MIHF relays request to Originating PoS (OPoS)
3. MIH\_TNMN\_SA\_Estab.indication: OPoS presents MN’s request to OPoS MIH user application.
4. OPoS MIH user provides MIRK to AAA for future authentication purposes at TPoA
5. OPoS MIH user computes MNmsrk from MIRK and sends appropriate LL frames to TPoA for key distribution and any other preregistration tasks.
6. MIH\_TNMN\_SA\_Estab.response: OPoS MIH user initiates message to MN user application via OPoS containing MNnetworkaccessid, MIRK. The response message informs MN that TPoS is the same as OPoS.
7. MIH\_TNMN\_SA\_Estab Response: OPoS relays message to MIHF at MN containing MNnetworkaccessid, MIRK.
8. MIH\_TNMN\_SA\_Estab. confirm: MIHF at MN relays message to MN user application containing MNnetworkaccessid, MIRK.
9. MN user application extracts MIRK, computes MNmsrk, continues any necessary preregistration activities

Finally when the OPoS and TPoS are the same entity and the MIH\_LL\_Transfer is used to exchange L2 frames (no authentication related), the following example diagram can be applied:



# 

*Insert new Annex P*

# MN’s Network Access Identifier Format

(Informative)

An MNnetworkaccessid attribute (of type MIHF\_ID), which is optionally contained in MIH\_LL\_Transfer.response, MIH\_LL\_Transfer.confirm, MIH\_N2N\_LL\_Transfer.response, and MIH\_N2N\_LL\_Transfer.confirm primitives, is assigned by the target PoS to the MN such that the MN can use the value of this attribute as the EAP peer identity for subsequent reactive pull key distribution or optimized pull key distribution from the target PoS. The username part of the MIHF\_ID carried in this attribute may contain the identifier of the MSRK used between the MN and the target PoS, and the realm part of the MIHF\_ID may contain a Fully Qualified Domain Name of the target PoS.

*Insert new Annex Q*

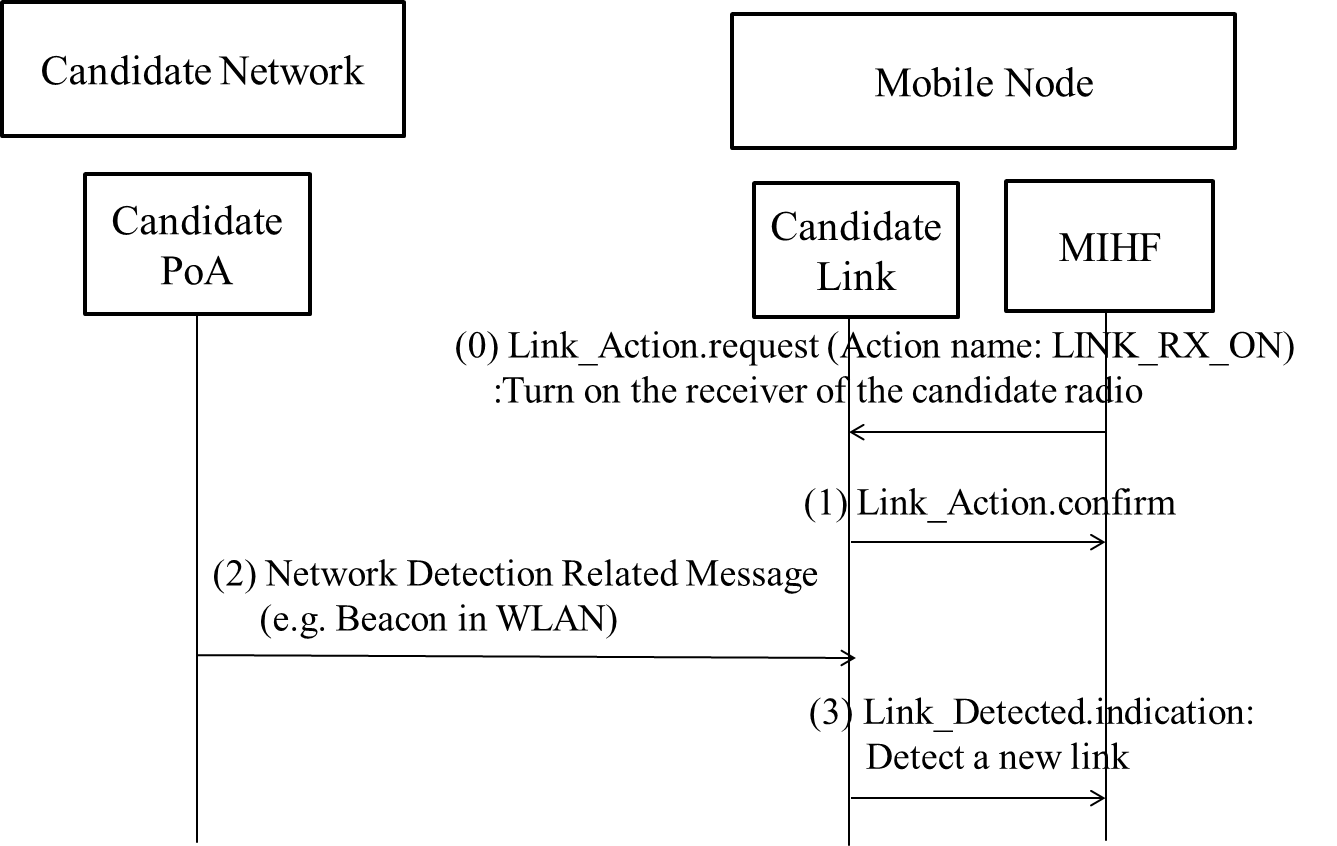
# Network discovery for single radio handover

(Informative)

The single radio handover has limitation in network discovery because of interference and power consumption problem of the network interfaces. This means that a mobile node is not free to use the target radio when the source radio is operating. Considering the problem, there are possible network discovery methods as follows. Three methods are described in the following:

## Network discovery: listening to the target link

The first method is listening to the target link. When the mobile node can listen to the target link and signal strength of the source link decrease, the mobile node can scan candidate links and then can find the target link. Moreover, periodic scanning for the target link can support network discovery. This method serves the accurate detection of the target links, but the mobile node may follow the assumptions in Section 1.4.

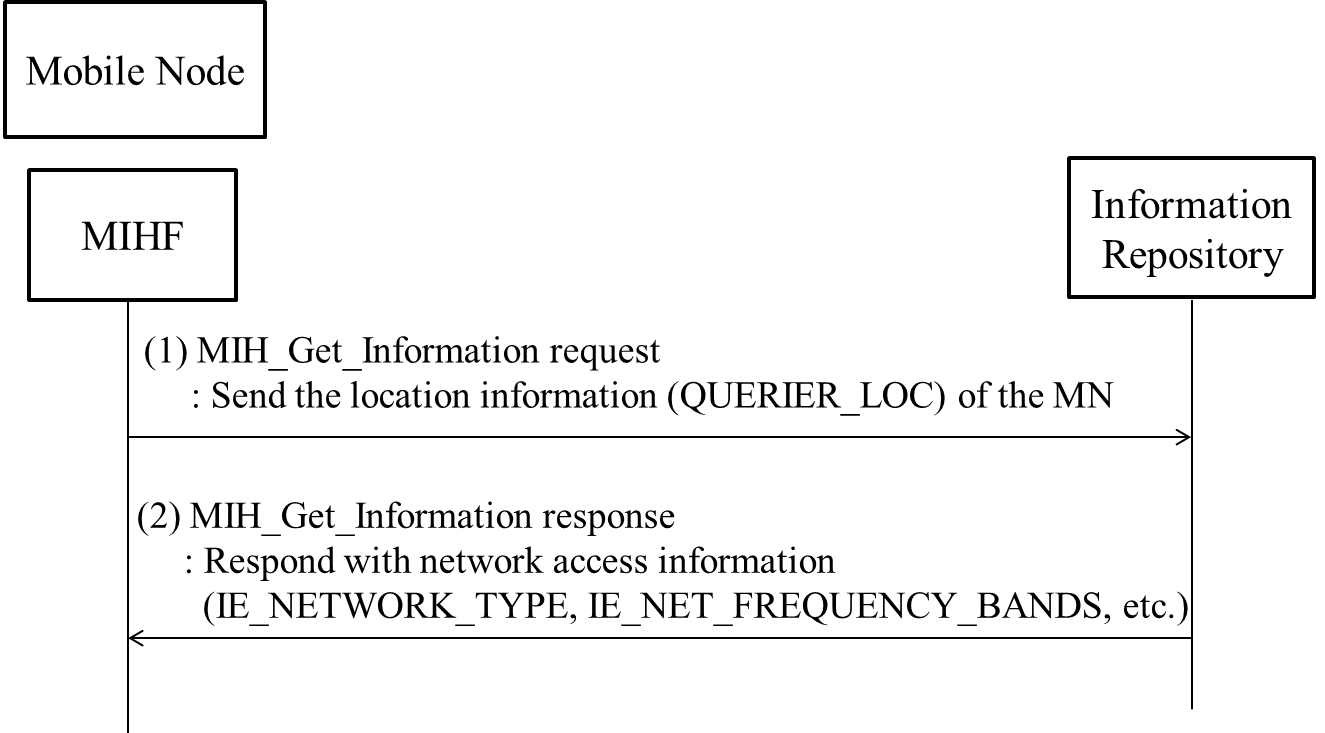


**Figure Q.1- Network discovery listening to the target link**

Figure Q.1 shows the case for network discovery listening to the target link with extended Link\_Action. In (0) and (1), SR-MIHF turns on only the receiver of the candidate radio using Link\_Action message with newly defined action name which is LINK\_RX\_ON. In (2), the candidate link listens to network detection related messages, such as beacon of IEEE 802.11 network. In (3), candidate link informs detection of a new link using Link\_Detected message. This method serves the accurate detection of the target links, but the mobile node may follow the assumptions in Section 1.4.

## Network discovery: using location information

The second method is network discovery based on the location information of the mobile node. This mechanism finds the target network using GPS (Global Positioning System) location information and interacting with the IR (Information Repository) explained in Section 11.4.2. This mechanism will avoid the interference explained above. Although location information from global positioning system (GPS) can enhance network detection, the GPS also dissipates power in the mobile node which is often limited by the power capability of its battery. Also, the GPS systems performance is often degraded with the weak signals in an indoor environment. In the event of GPS signal loss, such as when entering a building, the last known location could be used. Moreover, it can be a huge load to the network to invoke a network information repository to support network discovery for the mobile nodes which are equipped with the GPS.



**Figure Q.2- Network discovery using location information**

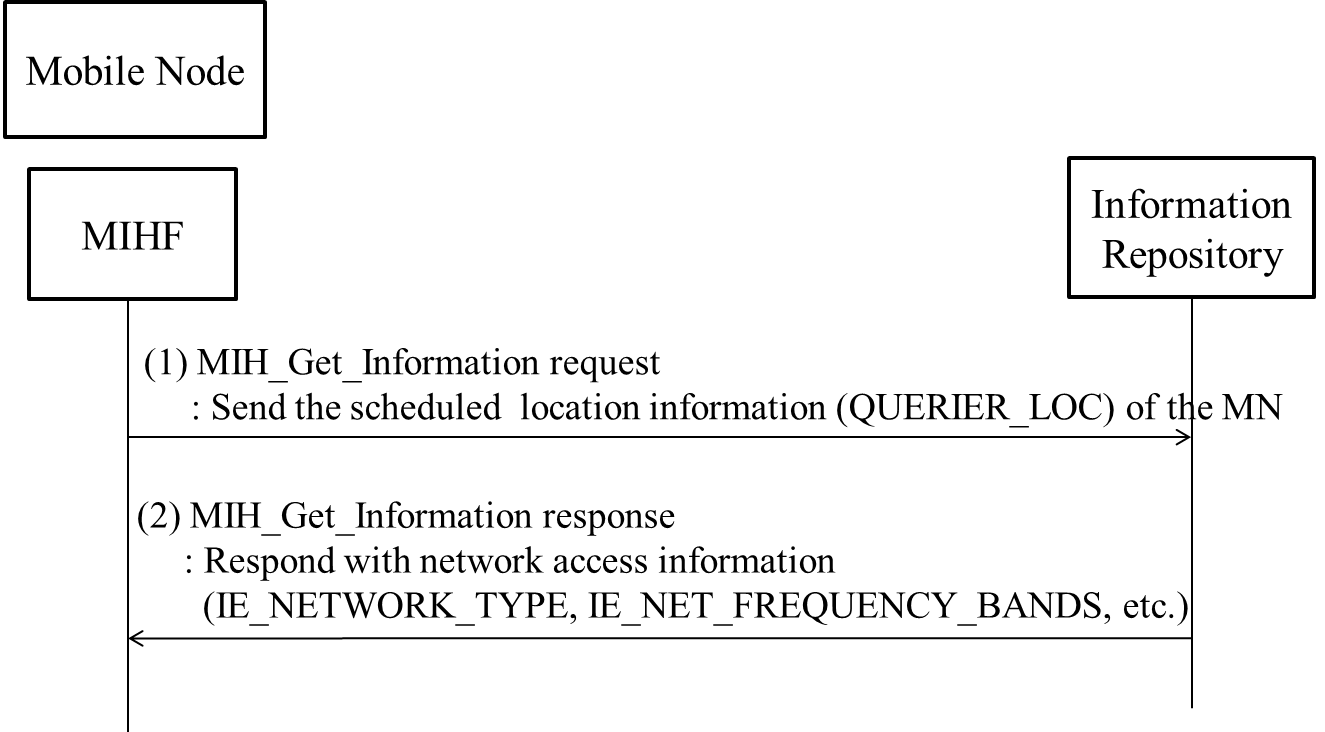
Figure Q.2 shows the case for network discovery using location information of the MN with QUERIER\_LOC. In (1), the MN SR-MIHF sends the location information (QUERIER\_LOC) of the MN through MIH\_Get\_Information request message. In (2), the IR SR-MIHF responds with network access information elements, such as IE\_NETWORK\_TYPE and IE\_NET\_FREQUENCY\_BANDS.

## Network discovery: using user schedule information

The third method is user schedule based network discovery. The multi-radio MN can possess a lightweight software that includes schedule program, e.g., Google calendar, and many users are already managing their schedule through the use of a schedule program such as Google calendar. The schedule program usually shows the user’s location at the dedicated time. Based on user’s location information, the multi-radio MN can determine its available networks and the target radio. For example, if Mr. Sam is scheduled to stay meeting room from 9AM to 11AM, the Mr. Sam’s multi-radio MN can discover a WLAN AP at the meeting room. In order to enhance this network discovery mechanism, the scheduled information can include the network information including information about link type, link identifier, link availability, link quality as defined in this standard. Using the network information, the mobile node can perform network discovery. If the MN knows the network information, it can try to connect to the network using that information.

This method can be supplemented by an information repository that is populated with location and network information. The network discovery is then achieved through use of the information repository combined with schedule of time and location from the MN, which may or may not have GPS information.

In addition, records of user’s network access can enhance network discovery with or without the Information Repository. For example, if Mr. Sam had visited “Room #1” and accessed WLAN at some time. When Mr. Sam is scheduled to visit “Room #1” again, the recorded network information will show that Mr. Sam’s MN can connect the WLAN using the recorded WLAN access information.



**Figure Q.3- Network discovery using user schedule information**

Figure Q.3 shows the case for network discovery using location information of the MN with QUERIER\_LOC. In (1), the MN SR-MIHF sends the scheduled location information (QUERIER\_LOC) of the MN through MIH\_Get\_Information request message. In (2), the IR SR-MIHF responds with network access information elements, such as IE\_NETWORK\_TYPE and IE\_NET\_FREQUENCY\_BANDS.

# Examples of SRHO

(Informative)

*Insert*

## WLAN to WiMAX single radio handover

### Reference model

The general reference model as it applies to WLAN to WiMAX single radio handover is illustrated in Figure R.1.



**Figure R.1 WLAN to WiMAX single radio handover reference model.**

#### Functional entities:

1. The Information Repository function may be implemented in a Media Independent Information Server (MIIS) defined in this specification, or in another information repository defined elsewhere, such as the ANDSF.
2. The WiMAX Signal Forwarding Function (SFF) is defined in a WiMAX Forum standard. It may be co-located at the ASN-GW. Otherwise, SFF may communicate with the ASN-GW using the R6 interface.
3. The Proxy GW function is implemented in the combined functions of ASN-GW and WiMAX SFF, in the WiMAX network. When the MN signals to the Proxy as if signaling to a point of attachment (PoA), the target PoA may correspondingly signal to that Proxy acting in the role of a virtual MN. The Proxy GW may also behave like a virtual PoA to signal with the target PoA.
4. The WiFi Interworking Function (WIF) is defined in WiMAX Forum.

#### Reference Points:

1. W3 interface between the WLAN AP and the WIF is defined in WiMAX Forum [WMF-T37-010-R016v01].
2. Rx interface between the MS and the WiMAX SFF/Proxy is defined in WiMAX Forum [WMF-T37-010-R016v01].
3. R3 interface between the WiMAX CSN and ASN is defined in WiMAX Forum [WMF-T37-010-R016v01].
4. R3+ interface between the WIF and AAA and also DHCP in the WiMAX CSN is defined in WiMAX Forum [WMF-T37-010-R016v01].
5. R6 interface between the WiMAX SFF/Proxy and ASN GW is defined in WiMAX Forum [T33-001-R015].

### Transport of WiMAX L2 control frames between MN and the WiMAX ASN

The single radio handover signal is similar to that of the generalized case described in Clause 5.5. The transport of the WiMAX L2 frame is described below.

#### Transport with MIH-capable devices

Figure R.2 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located Proxy GW/ASN-GW and the target WiMAX BS all support single radio handover in. The WiMAX radio L2 control frame is transported as a payload of a MIH frame between the MN and the WiMAX network via the source WLAN link at the left. The Proxy /ASN-GW combination bridges between the MN and the target WiMAX BS.



**Figure R.2. Transport of WiMAX L2 frame of target interface via the SFF/ASN-GW combination using the logical connection at the MIH.**

The MIHF interfaces with the TCP or UDP / IP layer through the Media Independent Handover Service Access Point (MIH\_SAP). The source WLAN link enables the TCP or UDP / IP connection between the MN and the WLAN network, which may then connect to the WiMAX ASN through the Internet or the WiMAX CSN. Therefore media independent handover (MIH) frames may be exchanged between the MIHF in the MN and the MIHF in the Proxy /ASN-GW and/or the WiMAX BS in the WiMAX network using TCP or UDP / IP transport.

An L2 frame is encapsulated with a MIHF header to constitute a MIH frame, which is exchanged between the MN and the target WiMAX BS or the Proxy /ASN-GW.

The MN will query the Information Repository to find the candidate target WiMAX BS. Based on the information from the Information Repository, the MN will then have some means to identify the target WiMAX BS, such as the link-layer address in order to perform network entry procedure to the WiMAX network using L2 packets.

The Information Repository needs to know the IP address of the Proxy /ASN-GW, so that the MN and the Proxy /ASN-GW can exchange MIH frames using TCP or UDP / IP transport. However, it may or may not be practical for MN to know the IP address of the target WiMAX BS.

If the MN knows the IP address of the target WiMAX BS, it will send the MIH frame to the MIHF in the target WiMAX BS using TCP or UDP / IP transport.

If the MN does not know the IP address of the target WiMAX BS, it will need another identifier, such as the link-layer address, to identify the target WiMAX BS. The MIH frame is first sent as the payload of a TCP or UDP / IP packet destined to the Proxy /ASN-GW as described in Section 12. The SRC frame contains information for the target WiMAX network to identify the target WiMAX BS. The Proxy /ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of a TCP or UDP / IP packet containing the MIH frame as payload to forward to the target WiMAX BS.

The reply sent by the target WiMAX BS is transported in a similar manner. If the target WiMAX link were available, the target WiMAX BS would send a L2 message back to the MN using this WiMAX link. Lacking this target link, this L2 message is passed as the payload of an MIH frame.

If the target PoA had received the MIH frame from the MN, the reply MIH frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target WiMAX BS had received the MIH frame from the Proxy /ASN-GW, the reply SRC frame will first use TCP or UDP / IP transport with an IP address destined to the Proxy. At the Proxy /ASN-GW, the TCP or UDP / IP header is extracted at the MIH\_SAP at the input interface of the Proxy /ASN-GW to retrieve the MIH frame. The MIHF will pass the MIH frame through the MIH\_SAP at the output interface of the Proxy /ASN-GW to form a new TCP or UDP / IP packet with an IP address destined to the MN.

#### Transport without MIH-capable target WiMAX BS

Figure R.3 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the Proxy /ASN-GW support single radio handover. Yet the target WiMAX BS are legacy WiMAX BS’s lacking such support. The target radio L2 control frame is transported as a payload of a media independent control frame between the MN and the WiMAX network via the source WLAN link at the left. The SFF/ASN-GW proxies between the MN and the target WiMAX BS using MIH to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS.



**Figure R.3. Transport of WiMAX L2 frame of target interface to the SFF/ASN-GW which proxies between the MN and the target PoA.**

Lacking the single radio handover support in the WiMAX BS, the Proxy /ASN-GW and the target WiMAX BS will need mechanism to communicate with each other. Certain control messages may already exist in the target network for network management purposes. The specific control messages needed may be defined in the specific target network such as an extension (R6+) of the R6 interface and is outside the scope of this standard.

The Proxy /ASN-GW may then proxy between the MN and the target WiMAX BS using MIH to communicate with MN and using some other control messages to communicate with the target network. These control messages need to be comprehensive enough so that the Proxy /ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function.

#### Transport without MIH-capable devices

Figure R.4 shows the packet used in the transport of WiMAX L2 frames between the MN and legacy WiMAX ASN where the single radio handover is supported neither between the MN and the Proxy /ASN-GW nor between the Proxy /ASN-GW and the target WiMAX BS. The Proxy /ASN-GW proxies between the MN and the target WiMAX BS using an extension of Rx interface to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS.



**Figure R.4. Protocol stack showing the transport of WiMAX L2 frame of target interface to the SFF/ASN-GW which proxy between the MN and the target PoA.**

The MN and the co-located Proxy GW/ASN-GW will need certain mechanism to communicate with each other, such as an extension (Rx+) of the Rx interface. The Proxy /ASN-GW and the target WiMAX BS will also need certain mechanism to communicate with each other, such as an extension (R6+) of the R6 interface.

The co-located Proxy GW/ASN-GW may then proxy between the MN and the target WiMAX BS using the Rx+ to communicate with MN and using the R6+ to communicate with the target WiMAX BS.

Both Rx+ and R6+ are outside the scope of this standard.

### WLAN to WiMAX Single Radio Handover processes

The single radio handover processes are: network discovery, preregistration, handover decision, WiMAX link preparation, and these processes are described in the following:

1. Network discovery: The MN queries the Information Repository function, which may be the MIIS. Alternatively, other implementations of the Information Repository function such as the ANDSF may also be used. Then the discovery of ANDSF may be through DHCP according to procedures defined in IETF RFC 6153. These query and reply messages may use the IP connectivity of the source link.

The Information Repository provides the MN with information about available networks and handover policy. It will also inform the MN whether the WiMAX ASN available in the neighborhood supports SRHO, and system information blocks of candidate PoAs to perform radio measurements.

1. Preregistration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the Proxy, the MN can perform network entry procedures towards the target network while retaining its data connection with the source network.

The MN and the target network performs proactive authentication via the source network. The exchange of handshake messages for authentication is communicated as follows:

1. The authentication messages are exchanged between the MN and the ASN-GW, which is the authenticator. These messages are L2 control frame messages in the target (WiMAX) network, which could have been exchanged via the target (WiMAX) link if the target link were available. When the target link is not available, the transport of the L2 control frame between the MN and the Proxy GW/ASN-GW is through the source (WiFi) network as described in Clause 11.2.
2. The ASN-GW/Proxy GW processes the SRC frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.
3. The ASN-GW maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the Proxy /ASN-GW, the preregistration is performed for the ASN network, which may have multiple PoA’s. When the MN attaches to a different target BS, it will use the existing registration context if the Proxy /ASN-GW already has this registration context.
4. The ASN-GW/Proxy combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/Proxy behaves like a virtual WiMAX BS located in the WiMAX network to communicate with the MN. Such control messages are equivalent to those in the handover from one BS to another BS within the same network. Therefore control messages may reuse those messages between the originating PoA and target PoA within the same network to prepare the handover of a MN within the same network.
5. For messages from the ASN-GW/Proxy GW to the MN, they are tunneled to the MN via the WiFi network. To the target WiMAX BS, the ASN-GW/Proxy acts like a virtual WiMAX radio interface.
6. The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.
7. 3: Handover Decision process:
8. The handover may be triggered by a need such as degradation of source link quality or cost considerations.
9. A WiMAX network is selected.
10. A determination is made on whether there is benefit to handover. The decision can be taken by the MN or the network and may be based on the parameters such as signal strength, cost, and operator policy.
11. WiMAX link preparation:

Before L3 handover occurs, the target link may perform preparation processes at L2, such as signal strength measurement and power level adjustment.

A target BS is selected. The MN may use the target interface to check the broadcast messages from the target BS to confirm that there is sufficient signal strength. In addition, limited message exchanges can be made using the target interface subjecting to the assumptions in Clause 1.4.

The WiMAX will check with the target BS and target ASN-GW to reserve the radio channels needed for MN to attach to the WiMAX network. The channels needed for MN to operate in active or idle mode are assigned depending on whether the source radio was in the active or idle mode.

1. SRHO execution process. In this process, the WiFi link is disconnected, the WiMAX radio is activated, and the WiMAX link is established to complete the L3 handover. The association of the network layer address to the link layer address will change from the WiFi link layer address to the WiMAX link layer address, and future incoming packets are then routed to the WiMAX radio.

## 3GPP to WiMAX single radio handover

### Reference model

The general reference model as it applies to 3GPP to WiMAX single radio handover is illustrated in Figure R.5.



**Figure R.5 3GPP to WiMAX single radio handover reference model.**

#### Functional entities:

1. The Information repository function may be implemented in a Media Independent Information Server (MIIS) defined in this specification but may also be other information repository defined elsewhere, such as the ANDSF.
2. The WiMAX Signal Forwarding Function (Proxy GW) is defined in WiMAX Forum standard. It may co-locate at the ASN-GW. Yet in the event that it is not co-located there, it may communicate with the ASN-GW using the R6 interface defined in the WiMAX Forum standard.
3. The Proxy GW function is implemented in the combined functions of ASN-GW and WiMAX Proxy GW, which are defined in the WiMAX network. When the MN signals to the Proxy GW as if signaling to a point of attachment (PoA), the target PoA may signal to the Proxy GW which acts like a virtual MN. The Proxy GW may also behave like a virtual PoA to signal with the target PoA.
4. The PDN Gateway (P-GW) is defined in 3GPP [3GPP TS23.401].

#### Reference Points:

1. S2a reference point between the P-GW and the ASN GW is defined in 3GPP [3GPP TS23.402].
2. R9 interface between the MS and the WiMAX Proxy GW is defined in WiMAX Forum [WMF-T37-011-R016v01].
3. R6 interface between the WiMAX Proxy GW and ASN GW is defined in WiMAX Forum [T33-001-R015].
4. S14 reference point between the MS and the ANDSF is defined in 3GPP [3GPP TS23.402].

### Transport of WiMAX L2 control frames between MN and the WiMAX ASN with MIH-capable devices

The single radio handover signal is similar to that of the generalized case described in Clause 5.5. The transport of the WiMAX L2 frame is described below.

#### Transport with MIH-capable devices

Figure R.6 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located Proxy GW/ASN-GW and the target WiMAX BS all support single radio handover. The WiMAX radio L2 control frame is transported as a payload of a MIH frame between the MN and the WiMAX network via the source 3GPP link at the left. The Proxy /ASN-GW combination bridges between the MN and the target WiMAX BS.



**Figure R.6. Transport of WiMAX L2 frame of target interface via the SFF/ASN-GW using the logical connection at the MIH.**

The MIHF interfaces with the TCP or UDP / IP layer through the Media Independent Handover Service Access Point (MIH\_SAP). The source 3GPP link enables the TCP or UDP / IP connection between the MN and the 3GPP network, which may then connect to the WiMAX ASN through the Internet or the WiMAX CSN. Therefore media independent handover control (MIH) frames may be exchanged between the SR-MIHF in the MN and the MIHF in the Proxy /ASN-GW and/or the WiMAX BS in the WiMAX network using TCP or UDP / IP transport.

An L2 frame is encapsulated with a SR-MIHF header to constitute a MIH frame, which is exchanged between the MN and the target WiMAX BS or the Proxy GW/ASN-GW.

The MN will query the Information Repository to find the candidate target WiMAX BS. Based on the information from the Information Repository, the MN will then have some means to identify the target WiMAX BS, such as the link-layer address in order to perform network entry procedure to the WiMAX network using L2 packets.

The Information Repository need to know the IP address of the Proxy /ASN-GW, so that the MN and the Proxy /ASN-GW can exchange MIH frames using TCP or UDP / IP transport. However, it may or may not be practical for MN to know the IP address of the target WiMAX BS.

If the MN knows the IP address of the target WiMAX BS, it will send the MIH frame to the MIHF in the target WiMAX BS using TCP or UDP / IP transport.

If the MN does not know the IP address of the target WiMAX BS, it will need another identifier, such as the link-layer address, to identify the target WiMAX BS. The MIHMIH frame is first sent as the payload of a TCP or UDP / IP packet destined to the Proxy /ASN-GW as described in Section 12. The MIH frame contains information for the target WiMAX network to identify the target WiMAX BS. The Proxy /ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of a TCP or UDP / IP packet containing the MIH frame as payload to forward to the target WiMAX BS.

The reply sent by the target WiMAX BS is transported in a similar manner. If the target WiMAX link were available, the target WiMAX BS would send a L2 message back to the MN using this WiMAX link. Lacking this target link, this L2 message is passed as the payload of an MIH frame.

If the target PoA had received the MIH frame from the MN, the reply MIH frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target WiMAX BS had received the MIH frame from the Proxy /ASN-GW, the reply MIH frame will first use TCP or UDP / IP transport with an IP address destined to the Proxy /ASN-GW. At the Proxy /ASN-GW, the TCP or UDP / IP header is extracted at the MIH\_SAP at the input interface of the Proxy /ASN-GW to retrieve the MIHrame. The MIHF function will pass the MIH frame through the MIH\_SAP at the output interface of the co-located Proxy GW/ASN-GW to form a new TCP or UDP / IP packet with an IP address destined to the MN.

#### Transport without MIH-capable target WiMAX BS

Figure R.7 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the Proxy /ASN-GW support single radio handover. Yet the target WiMAX BS are legacy WiMAX BS’s lacking such support. The WiMAX target radio L2 control frame is transported as a payload of a media independent control frame between the MN and the WiMAX network via the source 3GPP link at the left. The Proxy GW/ASN-GW proxies between the MN and the target WiMAX BS using MIH to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS.



**Figure R.7. Transport of WiMAX L2 frame of target interface to the SFF/ASN-GW which proxies between the MN and the target PoA.**

Lacking the single radio handover support in the WiMAX BS, the Proxy GW/ASN-GW and the target WiMAX BS will need mechanism to communicate with each other. Certain control messages may already exist in the target network for network management purposes. The specific control messages needed may be defined in the specific target network such as an extension (R6+) of the R6 interface and is outside the scope of this standard.

The Proxy/ASN-GW may then proxy between the MN and the target WiMAX BS using MIHF to communicate with MN and using some other control messages to communicate with the target network. These control messages need to be comprehensive enough so that the Proxy/ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function.

#### Transport without MIH-capable devices

Figure R.8 shows the transport of WiMAX L2 frames between the MN and legacy WiMAX ASN where the single radio handover is supported neither between the MN and the Proxy/ASN-GW nor between the Proxy/ASN-GW and the target WiMAX BS. The Proxy/ASN-GW proxies between the MN and the target WiMAX BS using an extension of R9 interface to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS.



**Figure R.8. Protocol stack showing the transport of WiMAX L2 frame of target interface to the SFF/ASN-GW which proxy between the MN and the target PoA.**

The MN and the Proxy/ASN-GW will need certain mechanism to communicate with each other, such as an extension (R9+) of the R9 interface. The Proxy/ASN-GW and the target WiMAX BS will also need certain mechanism to communicate with each other, such as an extension (R6+) of the R6 interface.

The Proxy/ASN-GW may then proxy between the MN and the target WiMAX BS using the R9+ to communicate with MN and using the R6+ to communicate with the target WiMAX BS.

Both R9+ and R6+ are both outside the scope of this standard.

### 3GPP to WiMAX Single Radio Handover processes

The single radio handover processes are: network discovery, preregistration, handover decision, WiMAX link preparation, and these processes are described in the following:

1. Network discovery: The MN queries the Information Repository function, which may be the MIIS. Alternatively, other implementations of the Information Repository function such as the ANDSF may also be used. Then the discovery of ANDSF may be through DHCP according to procedures defined in IETF RFC 6153. These query and reply messages may use the IP connectivity of the source link. The message exchange between the MN and the ANDSF may use the S14 reference point between the MN and the ANDSF as defined in 3GPP. These messages are carried in IP packets and may therefore use the IP connectivity at the source link.

The ANDSF provides the MN with information about available networks and handover policy. It will also inform the MN whether the WiMAX ASN network available in the neighborhood supports SRHO, the presence of Proxy, and system information blocks of candidate PoAs to perform radio measurements.

1. Preregistration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the Proxy, the MN can perform network entry procedures towards the target network while retaining its data connection with the source network.

The MN and the target network performs proactive authentication via the source network. The exchange of handshake messages for authentication is communicated as follows:

* 1. The authentication messages are exchanged between the MN and the ASN-GW, which is the authenticator. These messages are L2 control frame messages in the target (WiMAX) network, which could have been exchanged via the target (WiMAX) link if the target link were available. When the target link is not available, the transport of the L2 control frame between the MN and the Proxy/ASN-GW is through the source (3GPP) network as described in Clause 11.6.2.1.The ASN-GW/Proxy processes the frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.
  2. The ASN-GW maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the Proxy/ASN-GW, the preregistration is performed for the ASN network, which may have multiple PoA’s. When the MN attaches to a different target BS, it will use the existing registration context if the Proxy/ASN-GW already has this registration context.
  3. The ASN-GW/Proxy combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/Proxy behaves like a virtual WiMAX BS located in the WiMAX network to communicate with the MN. Such control messages are equivalent to those in the handover from one BS to another BS within the same network. Therefore control messages may reuse those between the source PoA and target PoA within the same network to prepare the handover of a MN within the same network.
  4. For messages from the ASN-GW/Proxy to the MN, they are tunneled to the MN via the 3GPP network. To the target WiMAX BS, the ASN-GW/Proxy acts like a virtual WiMAX radio interface.
  5. The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.

1. Handover Decision process:
   1. The handover may be triggered by a need such as degradation of source link quality or cost considerations.
   2. A WiMAX ASN network is selected.
   3. A determination is made on whether there is benefit to handover. The decision can be taken by the MN or the network and may be based on the parameters such as signal strength, cost, and operator policy.
2. WiMAX link preparation:

Before L3 handover occurs, the target link may perform preparation processes at L2, such as signal strength measurement and power level adjustment.

A target BS is selected. The MN may use the target interface to check the broadcast messages from the target BS to confirm that there is sufficient signal strength. In addition, limited message exchanges can be made using the target interface subjecting to the assumptions in Clause 1.4.

The WiMAX will check with the target BS and target ASN-GW to reserve the radio channels needed for MN to attach to the WiMAX network. The channels needed for MN to operate in active or idle mode are assigned depending on whether the source radio was in the active or idle mode.

1. 5: SRHO execution process. In this process, the WiFi link is disconnected, the WiMAX radio is activated, and the WiMAX link is established to complete the L3 handover. The association of the network layer address to the link layer address will change from the 3GPP link layer address to the WiMAX link layer address, and future incoming packets are then routed to the WiMAX radio.

## WiMAX to WLAN single radio handover

### Reference model

The general reference model as it applies to WiMAX to WLAN single radio handover is illustrated in Figure R.9.



**Figure R.9 WiMAX to WLAN single radio handover reference model.**

#### Functional entities:

1. The Information repository function may be implemented in a Media Independent Information Server (MIIS) defined in this specification but may also be other information repository defined elsewhere, such as the ANDSF.
2. The WiFi Interworking Function (WIF) is defined in WiMAX Forum. It may co-locate at the access router (AR). In the event that it is not co-located there, the WIF communicates with the AR through the W3 interface.
3. The Proxy function is implemented in the combined functions of WiFi Interworking Function (WIF) and WiFi Proxy, which are defined in the WiMAX network. When the MN signals to the Proxy as if signaling to a point of attachment (PoA), the target PoA may signal to the Proxy which acts like a virtual MN. The Proxy may also behave like a virtual PoA to signal with the target PoA. The WiFi Signal Forwarding Function (Proxy) is defined in WiMAX Forum standard. It may co-locate at the access router (AR). In the event that it is not there, the WiFi-Proxy communicates with the AR through the W1 interface.

#### Interfaces:

1. W1 interface between the WLAN AR and the WiFi Proxy is defined in WiMAX Forum [WMF-T37-010-R016v01].
2. W3 interface between the WLAN AR and the WIF is defined in WiMAX Forum [WMF-T37-010-R016v01].
3. Ry interface between the MS and the WiFi Proxy is defined in WiMAX Forum [WMF-T37-010-R016v01].
4. R3 interface between the WiMAX CSN and ASN is defined in WiMAX Forum [WMF-T37-010-R016v01].
5. R3+ interface between the WIF and AAA and also DHCP in the WiMAX CSN are defined in WiMAX Forum [WMF-T37-010-R016v01].
6. R6 interface between the WiMAX Proxy and ASN GW is defined in WiMAX Forum [WMF-T37-010-R016v01].

### Transport of WLAN L2 control frames between MN and the WLAN AN

The single radio handover signal is similar to that of the generalized case described in Clause 5.5. The transport of the WLAN L2 frame is described below.

#### Transport with MIH-capable devices

Figure R.10 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the Proxy/WIF/AR and the target WLAN AP all support single radio handover. The WLAN radio L2 control frame is transported as a payload of a media independent control frame between the MN and the WLAN network via the source WiMAX link at the left. The Proxy/WIF/AR bridges between the MN and the target WLAN AP.



**Figure R.10. Transport of WLAN L2 frame of target interface via the SFF/WIF/AR using the logical connection at the MIH.**

The SR-MIHF interfaces with the TCP or UDP / IP layer through the Media Independent Handover Service Access Point (MIH\_SAP). The source WiMAX link enables the TCP or UDP / IP connection between the MN and the WiMAX network, which may then connect to the WLAN AN through the Internet or the WiMAX CSN. Therefore media independent handover control (MIH) frames may be exchanged between the MIHF in the MN and the MIHF in the Proxy/WIF/AR and/or the WLAN AP in the WLAN network using TCP or UDP / IP transport.

An L2 frame is encapsulated with a SR-MIHF header to constitute a MIH frame, which is exchanged between the MN and the target WLAN AP or the Proxy/WIF/AR.

The MN will query the Information Repository to find the candidate target WLAN AP. Based on the information from the Information Repository, the MN will then have some means to identify the target WLAN AP, such as the link-layer address in order to perform network entry procedure to the WLAN network using L2 packets.

The Information Repository need to know the IP address of the Proxy/WIF/AR, so that the MN and the Proxy/WIF/AR can exchange MIH frames using TCP or UDP / IP transport. However, it may or may not be practical for MN to know the IP address of the target WLAN AP.

If the MN knows the IP address of the target WLAN AP, it will send the MIH frame to the SR-MIHF in the target WLAN AP using TCP or UDP / IP transport.

If the MN does not know the IP address of the target WLAN AP, it will need another identifier, such as the link-layer address, to identify the target WLAN AP. The MIH frame is first sent as the payload of a TCP or UDP / IP packet destined to the Proxy/WIF/AR as described in Section 12. The MIH frame contains information for the target WLAN network to identify the target WLAN AP. The Proxy/WIF/AR will find out the IP address of the target WLAN AP and use this address as the destination address of a TCP or UDP / IP packet containing the MIH frame as payload to forward to the target WLAN AP.

The reply sent by the target WLAN AP is transported in a similar manner. If the target WLAN link were available, the target WLAN AP would send a L2 message back to the MN using this WLAN link. Lacking this target link, this L2 message is passed as the payload of an MIH frame.

If the target PoA had received the MIH frame from the MN, the reply MIH frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target WLAN AP had received the MIH frame from the Proxy/WIF/AR, the reply MIH frame will first use TCP or UDP / IP transport with an IP address destined to the Proxy/WIF/AR. At the Proxy/WIF/AR, the TCP or UDP / IP header is extracted at the MICSAP at the input interface of the Proxy/WIF/AR to retrieve the MIH frame. The SR-MIHF function will pass the MIH frame through the MICSAP at the output interface of the Proxy/WIF/AR to form a new TCP or UDP / IP packet with an IP address destined to the MN.

#### Transport without MIH-capable target WLAN AP

Figure R.11 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the Proxy/WIF/AR support single radio handover. Yet the target WLAN AP are legacy WLAN AP’s lacking such support. The WLAN target radio L2 control frame is transported as a payload of a media independent control frame between the MN and the WLAN network via the source WiMAX link at the left. The Proxy/WIF/AR proxies between the MN and the target WLAN AP using MICF to communicate with the MN and using an extension of R6 interface to communicate with the target WLAN AP.



**Figure R.11. Transport of WLAN L2 frame of target interface to the SFF/WIF-AR which proxy between the MN and the target PoA.**

Lacking single radio handover support in the WLAN AP, the Proxy/WIF/AR and the target WLAN AP will need mechanism to communicate with each other. Certain control messages may already exist in the target network for network management purposes. The specific control messages needed may be defined in the specific target network and is outside the scope of this standard.

The Proxy/WIF/AR may then proxy between the MN and the target WLAN AP using SR-MIHF to communicate with MN and using some other control messages to communicate with the target network. These control messages need to be comprehensive enough so that the Proxy/WIF/AR may map the message contents exchanged with the MN with that exchanged with the target WLAN AP in performing proxy function.

#### Transport without MIH-capable devices

Figure R.12 shows the transport of WLAN L2 frames between the MN and legacy WLAN AN where the single radio handover is supported neither between the MN and the Proxy/WIF/AR nor between the Proxy/WIF/AR and the target WLAN AP. The Proxy/WIF/AR proxies between the MN and the target WLAN AP using an extension of R9 interface to communicate with the MN and using an extension of R6 interface to communicate with the target WLAN AP.



**Figure R.12. Protocol stack showing the transport of WLAN L2 frame of target interface to the SFF/ASN-GW which proxy between the MN and the target PoA.**

The MN and the Proxy/WIF/AR will need certain mechanism to communicate with each other, such as an extension (Ry+) of the Ry interface. The Proxy/WIF/AR and the target WLAN AP will also need certain mechanism to communicate with each other.

The Proxy/WIF/AR may then proxy between the MN and the target WLAN AP using the Ry+ to communicate with MN and using some mechanism to communicate with the target WLAN AP.

Ry+ is outside the scope of this standard.

### WiMAX to WLAN Single Radio Handover processes

The single radio handover processes are: network discovery, handover decision, preregistration, WLAN link preparation, and these processes are described in the following:

1. Network discovery: The MN queries the Information Repository function, which may be the MIIS. Alternatively, other implementations of the Information Repository function such as the ANDSF may also be used. Then the discovery of ANDSF may be through DHCP according to procedures defined in IETF RFC 6153. These query and reply messages may use the IP connectivity of the source link.

The Information Repository provides the MN with information about available networks and handover policy. It will also inform the MN whether the WiFi access network (AN) available in the neighborhood supports SRHO, and channel and frequency information of the candidate APs to perform radio measurements.

1. Handover Decision process:
   1. The handover may be triggered by a need such as degradation of source link quality or cost considerations.
   2. A WLAN network is selected.
   3. A determination is made on whether there is benefit to handover. The decision can be taken by the MN or the network and may be based on the parameters such as signal strength, cost, and operator policy.
2. Preregistration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the Proxy, the MN can perform network entry procedures towards the target network while retaining its data connection with the source network.

The MN and the target network performs proactive authentication via the source network. The exchange of handshake messages for authentication is communicated as follows:

* 1. The authentication messages are exchanged between the MN and the WLAN AP, which is the authenticator. These messages are L2 control frame messages in the target (WLAN) network, which could have been exchanged via the target (WLAN) link if the target link were available. When the target link is not available, the transport of the L2 control frame is through the source (WiMAX) network as described in Clause 11.2.
  2. The Proxy (WIF/AR/WiFi-Proxy) processes the MIH frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.
  3. The Proxy (WIF/AR/WiFi-Proxy) maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the Proxy, the preregistration is performed for the WiFi access network, which may have multiple AP’s. When the MN attaches to a different target AP, it will use the existing registration context if the Proxy already has this registration context.
  4. The Proxy (WIF/AR/WiFi-Proxy combination) also constructs control messages to communicate with the target WLAN AP. In terms of exchange of these control messages, the WIF/AR/WiFi-Proxy behaves like a virtual WiFi AP located in the WiFi network to communicate with the MN. Such control messages are equivalent to those in the handover from one AP to another AP within the same network. Therefore control messages may reuse those between the source PoA and target PoA within the same network to prepare the handover of a MN within the same network.
  5. For messages from the WIF/AR/WiFi-Proxy to the MN, they are tunneled to the MN via the WiMAX network. To the target WiFi AP, the WIF/AR/WiFi-Proxy acts like a virtual WLAN radio interface.
  6. The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.

1. WLAN link preparation:

Before L3 handover occurs, the target link may perform preparation processes at L2, such as signal strength measurement and power management.

A target AP is selected. The MN may use the target interface to check the beacon messages from the target AP to confirm that there is sufficient signal strength.

1. SRHO execution process. In this process, the WiMAX link is disconnected, the WLAN radio is activated, and the WLAN link is established to complete the L3 handover. The association of the network layer address to the link layer address will change from the WiMAX link layer address to the WLAN link layer address, and future incoming packets are then routed to the WLAN radio.

## WiMAX to 3GPP single radio handover

### Reference model

The general reference model as it applies to WiMAX to 3GPP single radio handover is illustrated in Figure R.13.



**Figure R.13 WiMAX to 3GPP single radio handover reference model.**

#### Functional entities:

1. The Information Repository function may be implemented in a Media Independent Information Server (MIIS) defined in this specification, or in another information repository defined elsewhere, such as the ANDSF.
2. The Proxy function is implemented in the 3GPP-Proxy and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-Proxy and MME may co-locate. In the event that they are not co-located, they communicate with each other using interface X202. When the MN signals to the Proxy as if signaling to a point of attachment (PoA), the target PoA may signal to the Proxy which acts like a virtual MN. The Proxy may also behave like a virtual PoA to signal with the target PoA.

#### Reference Points:

1. S2a reference point between P-GW in the 3GPP EPS network and ASN GW in the WiMAX network is defined in the 3GPP network [3GPP TS23.402].
2. S14 reference points between UE and ANDSF is defined in the 3GPP network [3GPP TS23.402].
3. S5/8 reference point between P-GW and S-GW is defined in the 3GPP network [3GPP TS23.401].
4. S11 reference point between S-GW and MME is defined in the 3GPP network [3GPP TS23.401].
5. S1-U reference point between UE and S-GW is defined in the 3GPP network [3GPP TS23.401].
6. S1-MME reference point between UE and MME is defined in the 3GPP network [3GPP TS23.401].
7. S6a reference point between P-GW and AAA is defined in the 3GPP network [3GPP TS23.401].
8. S6b reference point between MME and HSS is defined in the 3GPP network [3GPP TS23.401].
9. SWx reference point between HSS and AAA is defined in the 3GPP network [3GPP TS23.401].
10. STa reference point between WiMAX ASN and AAA is defined in the 3GPP network [3GPP TS23.402].
11. Gx reference point between P-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].
12. Gxa reference point between WiMAX ASN and PCRF is defined in the 3GPP network [3GPP TS23.402].
13. Gxc reference point between S-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].
14. R6 interface between the WiMAX Proxy and ASN GW is defined in WiMAX Forum [WMF-T37-010-R016v01].
15. X200 interface between MN and 3GPP-Proxy is defined in WiMAX Forum [WMF-T37-011-R016v01].
16. X202 interface between MME and 3GPP-Proxy is defined in WiMAX Forum [WMF-T37-011-R016v01].

### Transport of 3GPP L2 control frames between MN and the 3GPP network with MIH-capable devices

The single radio handover signal is similar to that of the generalized case described in Clause 5.5. The transport of the 3GPP L2 frame is described below.

#### Transport with MIH-capable devices

Figure R.14 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the 3GPP-Proxy/MME and the target 3GPP eNB all support single radio handover. The 3GPP radio L2 control frame is transported as a payload of a media independent control frame between the MN and the 3GPP network via the source WiMAX link at the left. The 3GPP-Proxy/MME bridges between the MN and the target 3GPP eNB.



**Figure R.14. Transport of 3GPP L2 frame of target interface via the 3GPP-SFF/MME using the logical connection at the MIH.**

The SR-MIHF interfaces with the TCP or UDP / IP layer through the Media Independent Handover Service Access Point (MIH\_SAP). The source WiMAX link enables the TCP or UDP / IP connection between the MN and the WiMAX network, which may then connect to the 3GPP network through the Internet or the WiMAX CSN. Therefore media independent handover (MIH) frames may be exchanged between the MIHF in the MN and the MIHF in the 3GPP-Proxy/MME and/or the 3GPP eNB in the 3GPP network using TCP or UDP / IP transport.

An L2 frame is encapsulated with a SR-MIHF header to constitute a MIH frame, which is exchanged between the MN and the target 3GPP eNB or the 3GPP-Proxy/MME.

The MN will query the Information Repository to find the candidate target 3GPP eNB. Based on the information from the Information Repository, the MN will then have some means to identify the target 3GPP eNB, such as the link-layer address in order to perform network entry procedure to the 3GPP network using L2 packets.

The Information Repository need to know the IP address of the 3GPP-Proxy/MME, so that the MN and the 3GPP-Proxy/MME can exchange MIH frames using TCP or UDP / IP transport. However, it may or may not be practical for MN to know the IP address of the target 3GPP eNB.

If the MN knows the IP address of the target 3GPP eNB, it will send the MIH frame to the SR-MIHF in the target 3GPP eNB using TCP or UDP / IP transport.

If the MN does not know the IP address of the target 3GPP eNB, it will need another identifier, such as the link-layer address, to identify the target 3GPP eNB. The MIH frame is first sent as the payload of a TCP or UDP / IP packet destined to the 3GPP-Proxy/MME as described in Section 12. The MIH frame contains information for the target 3GPP network to identify the target 3GPP eNB. The 3GPP-Proxy/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of a TCP or UDP / IP packet containing the MIH frame as payload to forward to the target 3GPP eNB.

The reply sent by the target 3GPP eNB is transported in a similar manner. If the target 3GPP link were available, the target 3GPP eNB would send a L2 message back to the MN using this 3GPP link. Lacking this target link, this L2 message is passed as the payload of an MIH frame.

If the target PoA had received the MIH frame from the MN, the reply MIH frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target 3GPP eNB had received the MIH frame from the 3GPP-Proxy/MME, the reply MIH frame will first use TCP or UDP / IP transport with an IP address destined to the 3GPP-Proxy/MME. At the 3GPP-Proxy/MME, the TCP or UDP / IP header is extracted at the MICSAP at the input interface of the 3GPP-Proxy/MME to retrieve the MIH frame. The SR-MIHF function will pass the MIH frame through the MICSAP at the output interface of the 3GPP-Proxy/MME to form a new TCP or UDP / IP packet with an IP address destined to the MN.

#### Transport without MIH-capable target 3GPP eNB

Figure R.15 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the 3GPP-Proxy/MME support single radio handover. Yet the target 3GPP eNB are legacy 3GPP eNB’s lacking such support. The 3GPP target radio L2 control frame is transported as a payload of a media independent control frame between the MN and the 3GPP network via the source WiMAX link at the left. The 3GPP-Proxy/MME proxies between the MN and the target 3GPP eNB using MIH to communicate with the MN and using an extension of R6 interface to communicate with the target 3GPP eNB.



**Figure R.15. Transport of 3GPP L2 frame of target interface to the 3GPP-SFF/MME which proxy between the MN and the target PoA, showing (a) the MICLSAP and MICSAP, and (b) the resulting protocol stack.**

Lacking the single radio handover support in the 3GPP eNB, the 3GPP-Proxy/MME and the target 3GPP eNB will need mechanism to communicate with each other. Certain control messages may already exist in the target network for network management purposes. The specific control messages needed may be defined in the specific target network such as an extension (S1-MME+) of the S1-MME reference point and is outside the scope of this standard.

The 3GPP-Proxy/MME may then proxy between the MN and the target 3GPP eNB using SR-MIHF to communicate with MN and using some other control messages to communicate with the target network. These control messages need to be comprehensive enough so that the 3GPP-Proxy/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function.

#### Transport without MIH-capable devices

Figure R.16 shows the transport of 3GPP L2 frames between the MN and legacy 3GPP network where the single radio handover is supported neither between the MN and the 3GPP-Proxy/MME nor between the 3GPP-Proxy/MME and the target 3GPP eNB. The 3GPP-Proxy/MME proxies between the MN and the target 3GPP eNB using an extension of R9 interface to communicate with the MN and using an extension of R6 interface to communicate with the target 3GPP eNB.



**Figure R.16. Protocol stack showing the transport of 3GPP L2 frame of target interface to the SFF/ASN-GW which proxy between the MN and the target PoA.**

The MN and the 3GPP-Proxy/MME will need certain mechanism to communicate with each other, such as an extension (X200+) of the X200 interface. The 3GPP-Proxy/MME and the target 3GPP eNB will also need certain mechanism to communicate with each other.

The 3GPP-Proxy/MME may then proxy between the MN and the target 3GPP eNB using the X200+ to communicate with MN and using S1-MME+ to communicate with the target 3GPP eNB.

Both X200+ and S1-MME+ are outside the scope of this standard.

### WiMAX to 3GPP Single Radio Handover processes

The single radio handover processes are: network discovery, handover decision, preregistration, 3GPP link preparation, and these processes are described in the following:

1. Network discovery: The MN queries the Information Repository function, which may be the MIIS. Alternatively, other implementations of the Information Repository function such as the ANDSF may also be used. Then the discovery of ANDSF may be through DHCP according to procedures defined in IETF RFC 6153. The message exchange between the MN and the ANDSF may use the S14 reference point between the MN and the ANDSF as defined in 3GPP. These messages are carried in IP packets and may therefore use the IP connectivity at the source link.

The ANDSF provides the MN with information about available networks and handover policy. It will also inform the MN whether the 3GPP EPS network available in the neighborhood supports SRHO, the presence of P-GW, and system information blocks of candidate PoAs to perform radio measurements.

While ANDSF may be present in the 3GPP network, the WiMAX network may also have ANDSF in its CSN.

1. Handover Decision process:
   1. The handover may be triggered by a need such as degradation of source link quality or cost considerations.
   2. A 3GPP EPS network is selected.
   3. A determination is made on whether there is benefit to handover. The decision can be taken by the MN or the network and may be based on the parameters such as signal strength, cost, and operator policy.
2. Preregistration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the ProxyProxy, the MN can perform network entry procedures towards the target network while retaining its data connection with the source network.

The MN and the target network performs proactive authentication via the source network. The exchange of handshake messages for authentication is communicated as follows:

* 1. The authentication messages are exchanged between the MN and the MME, which is the authenticator. These messages are L2 control frame messages in the target (3GPP) network, which could have been exchanged via the target (3GPP) link if the target link were available. When the target link is not available, the transport of the L2 control frame between the MN and the 3GPP-ProxyProxy/MME combination is through the source (WiMAX) network as described in Clause 11.6.4.1.
  2. The 3GPP-ProxyProxy/MME processes the MIH frame containing the L2 authentication message. The MME may consult the HSS in the 3GPP EPS network through the S6a reference point.
  3. The MME maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the MME, the preregistration is performed for the 3GPP access network, which may have multiple eNB’s. When the MN attaches to a different target eNB, it will use the existing registration context if the MME already has this registration context.
  4. The 3GPP-ProxyProxy/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-Proxy/MME behaves like a virtual 3GPP eNB located in the 3GPP network to communicate with the MN. Such control messages are equivalent to those in the handover from one eNB to another eNB within the same network. Therefore control messages may reuse those between the originating PoA and target PoA within the same network to prepare the handover of a MN within the same network.
  5. For messages from the 3GPP-Proxy/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-Proxy/MME acts like a virtual 3GPP radio interface.
  6. The MN may pre-register with the 3GPP network, using the same interface and transport mechanism as that in proactive authentication.

1. Target 3GPP link preparation:

Before L3 handover occurs, the target link may perform preparation processes at L2, such as signal strength measurement and power level adjustment.

A target eNB is selected. The MN may use the target interface to check the broadcast messages from the target eNB to confirm that there is sufficient signal strength. In addition, limited message exchanges can be made using the target interface subjecting to the assumptions in Clause 1.4.

The 3GPP will check with the target eNB to reserve the radio channels needed for MN to attach to the 3GPP network. The channels needed for MN to operate in active or idle mode are assigned depending on whether the source radio was in the active or idle mode.

1. SRHO execution process. In this process, the WiMAX link is disconnected, the 3GPP radio is activated, and the 3GPP link is established to complete the L3 handover. The association of the network layer address to the link layer address will change from the WiMAX link layer address to the 3GPP link layer address, and future incoming packets are then routed to the 3GPP radio.

## WLAN to 3GPP single radio handover

### Reference model

The general reference model as it applies to Non-trusted WLAN to 3GPP single radio handover is illustrated in Figure R.17.



**Figure R.17 Non-trusted WLAN AN to 3GPP single radio handover reference model.**

#### Functional entities:

1. The Information Repository function may be implemented in a Media Independent Information Server (MIIS) defined in this specification, or in another information repository defined elsewhere, such as the ANDSF.
2. The Proxy function is implemented in the 3GPP-Proxy and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-Proxy and MME may co-locate. In the event that they are not co-located, they communicate with each other using interface X202. When the MN signals to the Proxy as if signaling to a point of attachment (PoA), the target PoA may signal to the Proxy which acts like a virtual MN. The Proxy may also behave like a virtual PoA to signal with the target PoA.

#### Reference points:

1. S2c reference point between MN and the P-GW is defined in the 3GPP EPS network [3GPP TS23.402].
2. S2b reference point between ePDG and the P-GW is defined in the 3GPP EPS network [3GPP TS23.402].
3. S14 reference point between UE and ANDSF is defined in the 3GPP network [3GPP TS23.402].
4. S5/8 reference point between P-GW and S-GW is defined in the 3GPP network [3GPP TS23.401].
5. S11 reference point between S-GW and MME is defined in the 3GPP network [3GPP TS23.401].
6. S1-U reference point between UE and S-GW is defined in the 3GPP network [3GPP TS23.401].
7. S1-MME reference point between UE and MME is defined in the 3GPP network [3GPP TS23.401].
8. S6a reference point between P-GW and AAA is defined in the 3GPP network [3GPP TS23.401].
9. S6b reference point between MME and HSS is defined in the 3GPP network [3GPP TS23.401].
10. SWa reference point between the non-trusted WLAN AN and AAA is defined in the 3GPP network [3GPP TS23.402].
11. SWn reference point between the non-trusted WLAN AN and ePDG is defined in the 3GPP network [3GPP TS23.402].
12. SWm reference point between ePDG and P-GW is defined in the 3GPP network [3GPP TS23.402].
13. SWx reference point between HSS and AAA is defined in the 3GPP network [3GPP TS23.401].
14. Gx reference point between P-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].
15. Gxb reference point between ePDG and PCRF is defined in the 3GPP network [3GPP TS23.401].
16. Gxc reference point between S-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].
17. RPmi interface between MN and 3GPP-Proxy.
18. X202 interface between MME and 3GPP-Proxy is defined in WiMAX Forum [WMF-T37-010-R016v01].

### Transport of 3GPP L2 control frames between MN and the 3GPP network

The single radio handover signal is similar to that of the generalized case described in Clause 5.5. The transport of the 3GPP L2 frame is described below.

#### Transport with MIH-capable devices

Figure R.18 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the 3GPP-Proxy/MME and the target 3GPP eNB all support single radio handover. The 3GPP radio L2 control frame is transported as a payload of a MIH frame between the MN and the 3GPP network via the source WLAN link at the left. The 3GPP-Proxy/MME bridges between the MN and the target 3GPP eNB.



**Figure R.18. Transport of 3GPP L2 frame of target interface via the 3GPP-SFF/MME using the logical connection at the MIH.**

The SR-MIHF interfaces with the TCP or UDP / IP layer through the Media Independent Handover Service Access Point (MIH\_SAP). The source WLAN link enables the TCP or UDP / IP connection between the MN and the WLAN network, which may then connect to the 3GPP network through the Internet or the 3GPP EPC. Therefore media independent handover control (MIH) frames may be exchanged between the SR-MIHF in the MN and the SR-MIHF in the 3GPP-Proxy/MME and/or the 3GPP eNB in the 3GPP network using TCP or UDP / IP transport.

An L2 frame is encapsulated with a SR-MIHF header to constitute a MIH frame, which is exchanged between the MN and the target 3GPP eNB or the 3GPP-Proxy/MME.

The MN will query the Information Repository to find the candidate target 3GPP eNB. Based on the information from the Information Repository, the MN will then have some means to identify the target 3GPP eNB, such as the link-layer address in order to perform network entry procedure to the 3GPP network using L2 packets.

The Information Repository need to know the IP address of the 3GPP-Proxy/MME, so that the MN and the 3GPP-Proxy/MME can exchange MIH frames using TCP or UDP / IP transport. However, it may or may not be practical for MN to know the IP address of the target 3GPP eNB.

If the MN knows the IP address of the target 3GPP eNB, it will send the MIH frame to the SR-MIHF in the target 3GPP eNB using TCP or UDP / IP transport.

If the MN does not know the IP address of the target 3GPP eNB, it will need another identifier, such as the link-layer address, to identify the target 3GPP eNB. The MIH frame is first sent as the payload of a TCP or UDP / IP packet destined to the 3GPP-Proxy/MME as described in Section 12. The MIH frame contains information for the target 3GPP network to identify the target 3GPP eNB. The 3GPP-Proxy/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of a TCP or UDP / IP packet containing the MIH frame as payload to forward to the target 3GPP eNB.

The reply sent by the target 3GPP eNB is transported in a similar manner. If the target 3GPP link were available, the target 3GPP eNB would send a L2 message back to the MN using this 3GPP link. Lacking this target link, this L2 message is passed as the payload of an MIH frame.

If the target PoA had received the MIH frame from the MN, the reply MIH frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target 3GPP eNB had received the MIH frame from the 3GPP-Proxy/MME, the reply MIH frame will first use TCP or UDP / IP transport with an IP address destined to the 3GPP-Proxy/MME. At the 3GPP-Proxy/MME, the TCP or UDP / IP header is extracted at the MICSAP at the input interface of the 3GPP-Proxy/MME to retrieve the MIH frame. The SR-MIHF function will pass the MIH frame through the MICSAP at the output interface of the 3GPP-Proxy/MME to form a new TCP or UDP / IP packet with an IP address destined to the MN.

#### Transport without MIH-capable target 3GPP eNB

Figure R.19 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the 3GPP-Proxy/MME support single radio handover. Yet the target 3GPP eNB are legacy 3GPP eNB’s lacking MICF support. The 3GPP target radio L2 control frame is transported as a payload of a media independent control frame between the MN and the 3GPP network via the source WLAN link at the left. The 3GPP-Proxy/MME proxies between the MN and the target 3GPP eNB using MICF to communicate with the MN and using an extension of R6 interface to communicate with the target 3GPP eNB.



**Figure R.19. Transport of 3GPP L2 frame of target interface to the 3GPP-SFF/MME which proxies between the MN and the target PoA.**

Lacking the single radio handover support in the 3GPP eNB, the 3GPP-Proxy/MME and the target 3GPP eNB will need mechanism to communicate with each other. Certain control messages may already exist in the target network for network management purposes. The specific control messages needed may be defined in the specific target network such as an extension (S1-MME+) of the S1-MME reference point and is outside the scope of this standard.

The 3GPP-Proxy/MME may then proxy between the MN and the target 3GPP eNB using SR-MIHF to communicate with MN and using some other control messages to communicate with the target network. These control messages need to be comprehensive enough so that the 3GPP-Proxy/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function.

#### Transport without MIH-capable devices

Figure R.20 shows the transport of 3GPP L2 frames between the MN and legacy 3GPP network where the single radio handover is supported neither between the MN and the 3GPP-Proxy/MME nor between the 3GPP-Proxy/MME and the target 3GPP eNB. The 3GPP-Proxy/MME proxies between the MN and the target 3GPP eNB using an extension of RPmi interface to communicate with the MN and using an extension of S1-MME reference point to communicate with the target 3GPP eNB.



**Figure R.20. Protocol stack showing the transport of 3GPP L2 frame of target interface to the SFF/ASN-GW which proxy between the MN and the target PoA.**

The MN and the 3GPP-Proxy/MME will need certain mechanism to communicate with each other, such as an extension (RPmi+) of the RPmi interface. The 3GPP-Proxy/MME and the target 3GPP eNB will also need certain mechanism to communicate with each other.

The 3GPP-Proxy/MME may then proxy between the MN and the target 3GPP eNB using the RPmi+ to communicate with MN and using S1-MME+ to communicate with the target 3GPP eNB.

Both RPmi+ and S1-MME+ are outside the scope of this standard.

### Non-trusted WLAN AN to 3GPP Single Radio Handover processes

The single radio handover processes are: network discovery, handover decision, preregistration, 3GPP link preparation, and these processes are described in the following:

1. Network discovery: The MN queries the Information Repository function, which may be the MIIS. Alternatively, other implementations of the Information Repository function such as the ANDSF may also be used. Then the discovery of ANDSF may be through DHCP according to procedures defined in IETF RFC 6153. The message exchange between the MN and the ANDSF may use the S14 reference point between the MN and the ANDSF as defined in 3GPP. These messages are carried in IP packets and may therefore use the IP connectivity at the source link.

The MIIS or ANDSF provides the MN with information about available networks and handover policy. It will also inform the MN whether the 3GPP EPS network available in the neighborhood supports SRHO, the presence of ePDG, P-GW, and system information blocks of candidate PoAs to perform radio measurements.

1. Handover Decision process:
   1. The handover may be triggered by a need such as degradation of source link quality or cost considerations.
   2. A 3GPP EPS network is selected.
   3. A determination is made on whether there is benefit to handover. The decision can be taken by the MN or the network and may be based on the parameters such as signal strength, cost, and operator policy.
2. Preregistration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the Proxy, the MN can perform network entry procedures towards the target network while retaining its data connection with the source network.

The MN and the target network performs proactive authentication via the source network. The exchange of handshake messages for authentication is communicated as follows:

* 1. The authentication messages are exchanged between the MN and the MME, which is the authenticator. These messages are L2 control frame messages in the target (3GPP) network, which could have been exchanged via the target (3GPP) link if the target link were available. When the target link is not available, the transport of the L2 control frame is through the originating (WLAN) network as described in Clause 11.2.
  2. The 3GPP-Proxy/MME processes the frame containing the L2 authentication message. The MME may consult the HSS in the 3GPP EPS network through the S6a reference point.
  3. The MME maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the MME, the preregistration is performed for the 3GPP access network, which may have multiple eNB’s. When the MN attaches to a different target eNB, it will use the existing registration context if the MME already has this registration context.
  4. The 3GPP-Proxy/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-Proxy/MME behaves like a virtual 3GPP eNB located in the 3GPP network to communicate with the MN. Such control messages are equivalent to those in the handover from one eNB to another eNB within the same network. Therefore control messages may reuse those between the originating PoA and target PoA within the same network to prepare the handover of a MN within the same network.
  5. For messages from the 3GPP-Proxy/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-Proxy/MME acts like a virtual 3GPP radio interface.
  6. The MN may pre-register with the 3GPP network, using the same interface and transport mechanism as that in proactive authentication.

1. Target 3GPP link preparation:

Before L3 handover occurs, the target link may perform preparation processes at L2, such as signal strength measurement and power level adjustment.

A target eNB is selected. The MN may use the target interface to check the broadcast messages from the target eNB to confirm that there is sufficient signal strength. In addition, limited message exchanges can be made using the target interface subjecting to the assumptions in Clause 1.4.

The 3GPP will check with the target eNB and target 3GPP-Proxy/MME to reserve the radio channels needed for MN to attach to the 3GPP network. The channels needed for MN to operate in active or idle mode are assigned depending on whether the source radio was in the active or idle mode.

1. SRHO execution process. In this process, the WLAN link is disconnected, the 3GPP radio is activated, and the 3GPP link is established to complete the L3 handover. The association of the network layer address to the link layer address will change from the WLAN link layer address to the 3GPP link layer address, and future incoming packets are then routed to the 3GPP radio.

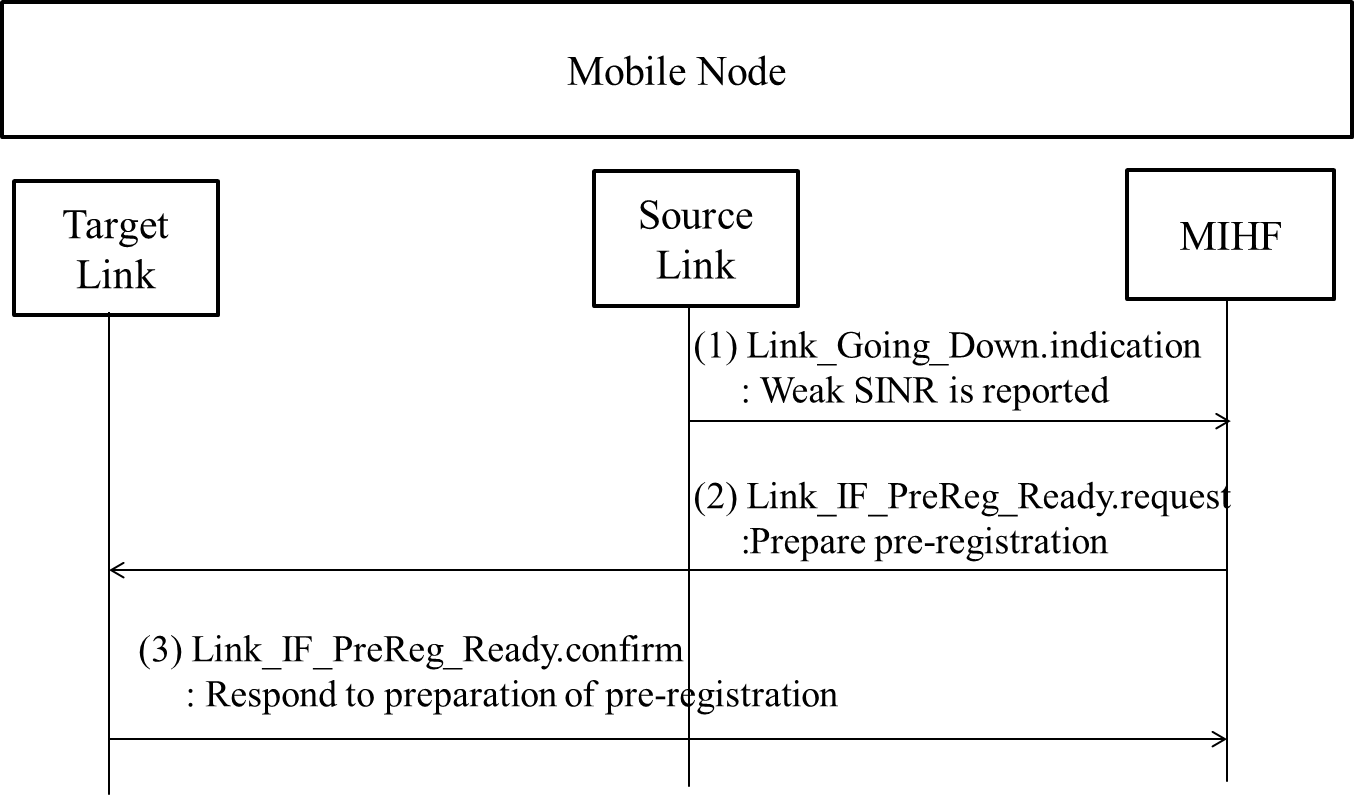
*Insert new Annex S*

# Handover Decision

(Informative)

To decide handover, three representative criteria are considerable for handover decision. Criteria to decide handover can be weak SINR (Signal to Interference plus Noise Ratio), QoS and/or cost, and the power consumption of the source link.

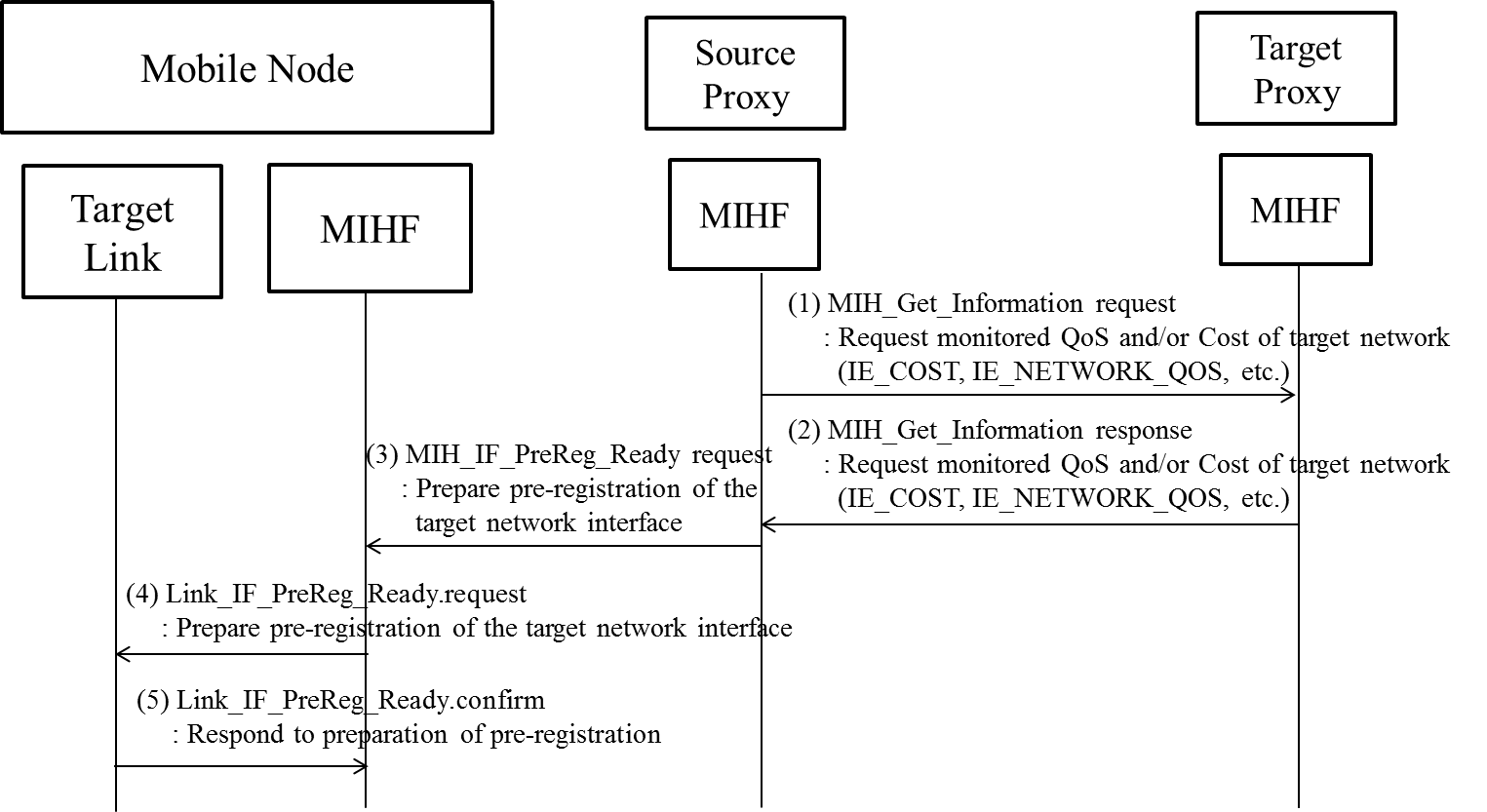
## Weak SINR of the source link



**Figure S.1- HO decision caused by weak SINR of the source link**

Figure S.1 shows the case for weak SINR of the source link. Through Link\_Going\_Down.indication, the source link interface reports its weak SINR. Afterwards, the SR-MIHF orders the target link interface to initiate preregistration through Link\_IF\_PreReg\_Ready.req. Link\_IF\_PreReg\_Ready is needed, because preregistration is different from regular registration. While the L2 messages for regular registration are transmitted through the target link, the L2 messages for preregistration are transmitted through higher layer (TCP or UDP/IP) and the source link. After the target link interface prepares preregistration, the target link interface responds with Link\_IF\_PreReg\_Ready.confirm.

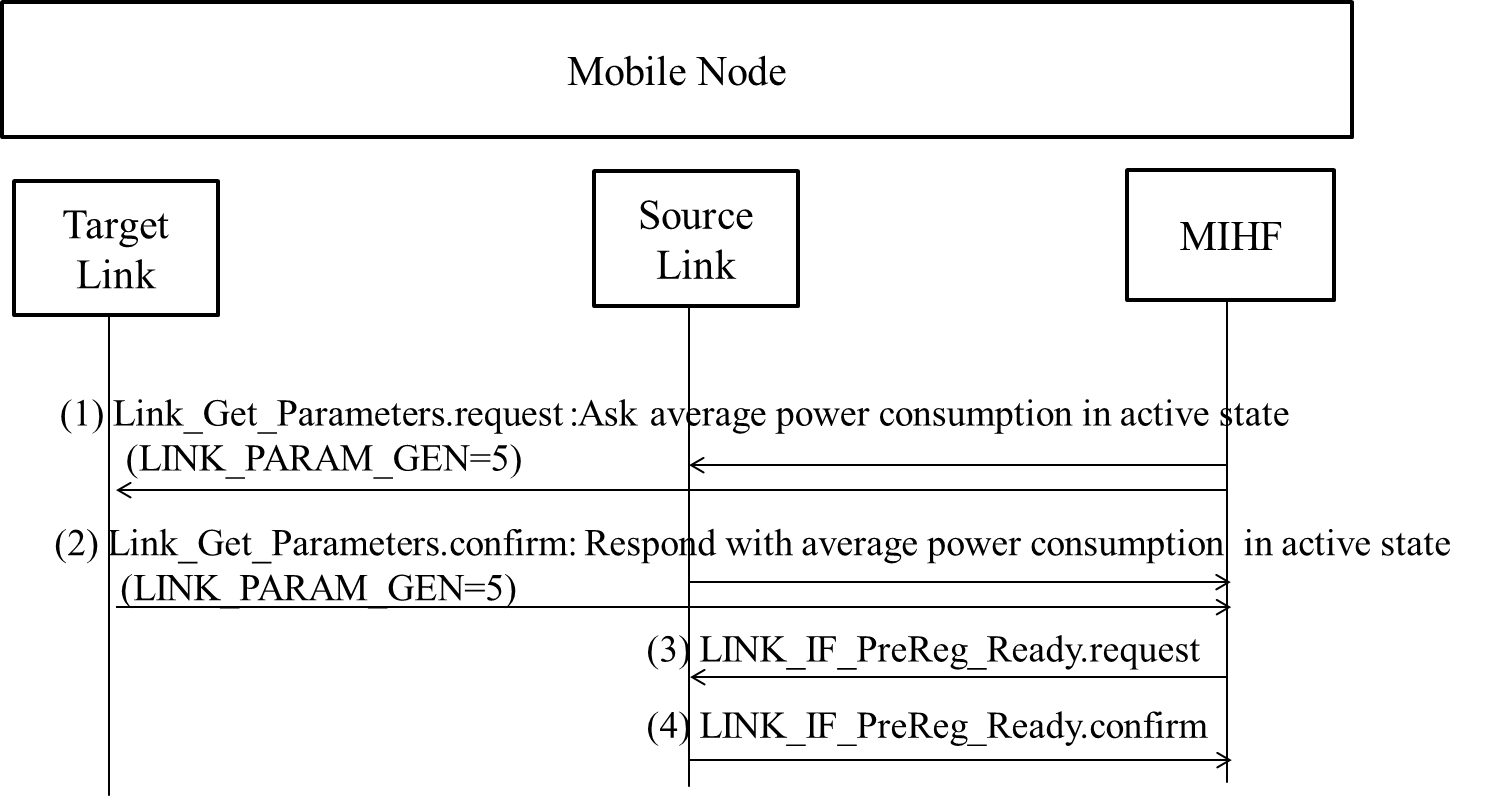
## QoS and/or cost check



**Figure S.2- HO decision caused by QoS and/or cost**

Figure S.2 shows the case of QoS and/or cost check for HO decision. The source Proxy GW consults the QoS and/or cost with target Proxy GW through MIH\_Get\_Information. After source Proxy GW recommends the MN to perform handover, the source Proxy GW transmits MIH\_IF\_PreReg\_Ready request message. The SR-MIHF of the MN orders the target link to pre-register through Link\_IF\_PregReg\_Ready.

## Power consumption comparison of the link interfaces



**Figure S.3- HO decision caused by power consumption comparison**

Figure S.3 shows the HO decision to reduce power consumption of the MN. The SR-MIHF of the MN ask power consumption of each link interface through Link\_Get\_Parameters.request with new LINK\_PARAM\_GEN value, which is 5, and thus the source link interface and the target link interface answers its average power consumption through Link\_Get\_Parameters.confirm. Afterwards, the SR-MIHF of the MN decides to perform handover through Link\_IF\_PreReg\_Ready.request, and then the target link interface responds with Link\_IF\_PreReg\_Ready.confirm.

1. The Institute of Electrical and Electronics Engineers, Inc.

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

   Copyright © 20XX by the Institute of Electrical and Electronics Engineers, Inc.

   All rights reserved. Published <XX MONTH 20XX>. Printed in the United States of America.

   IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics   
   Engineers, Incorporated.

   **PDF: ISBN 978-0-XXXX-XXXX-X STDXXXXX**

   **Print: ISBN 978-0-XXXX-XXXX-X STDPDXXXXX**

   *IEEE prohibits discrimination, harassment and bullying. For more information, visit* [*http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html*](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.*  [↑](#footnote-ref-1)
2. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-2)
3. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-3)
4. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-4)
5. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-5)
6. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-6)
7. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-7)
8. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-8)
9. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-9)
10. Note to the editor, this footnote should not appear in the final version. MIRK stands for MN´s media independent root key. [↑](#footnote-ref-14)
11. Note to editor, this footnote should not appear in the final version. MSPMK stands for MN´s media specific root key. [↑](#footnote-ref-15)