|  |  |
| --- | --- |
| Project | **IEEE 802.21 Media Independent Handover Services**  **IEEE 802.21c: Single Radio Handover**  **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **TGc\_Proposal\_Charles\_Perkins** |
| Date Submitted | July 19, 2012 |
| Source(s) | H Anthony Chan (Huawei), Junghoon Jee (ETRI), Charles E. Perkins (Futurewei), Hyunho Park (ETRI), Dapeng Liu (China Mobile), Yoshihiro Ohba (Toshiba) |
| Re: | IEEE 802.21c draft |
| Purpose | Task Group Discussion and Acceptance |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.21. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as outlined in [Clause 6.3 of the IEEE-SA Standards Board Operations Manual](http://standards.ieee.org/guides/opman/sect6.html#6.3) <<http://standards.ieee.org/guides/opman/sect6.html#6.3>> and in *Understanding Patent Issues During IEEE Standards Development* <<http://standards.ieee.org/board/pat/guide.html>>. |
|  |  |

**[IEEE Standard for Local and metropolitan area networks —](#_Toc334767864)** [7](#_Toc334767864)

**[Part 21: Media Independent Handover Services](#_Toc334767865)** [7](#_Toc334767865)

**[Amendment: Optimized Single Radio Handovers](#_Toc334767866)** [7](#_Toc334767866)

**[Keywords:](#_Toc334767867)** [8](#_Toc334767867)

**[IEEE Standard for](#_Toc334767868)** [8](#_Toc334767868)

**[Local and metropolitan area networks—](#_Toc334767869)** [8](#_Toc334767869)

**[Amendment: Optimized Single Radio Handovers](#_Toc334767870)** [9](#_Toc334767870)

[1 Overview 10](#_Toc334767871)

[1.1 10](#_Toc334767872)

[1.2 10](#_Toc334767873)

[1.3 General 10](#_Toc334767874)

[2 Normative references 10](#_Toc334767875)

[3 Definitions 10](#_Toc334767876)

[4 Abbreviations and acronyms 11](#_Toc334767877)

[5 General architecture 11](#_Toc334767878)

[6 MIH Services 11](#_Toc334767879)

[6.1 General 11](#_Toc334767880)

[6.2 Service management 11](#_Toc334767881)

[6.3 Media independent event service 11](#_Toc334767882)

[6.4 Media independent command service 11](#_Toc334767883)

[6.5 Media independent information service 11](#_Toc334767884)

[6.5.1 Information Element 11](#_Toc334767885)

**[Table 1 – Information Element](#_Toc334767886)** [11](#_Toc334767886)

[6.5.2 IE Containers 12](#_Toc334767887)

**[Table 2 – IE\_CONTAINER\_PoS definition](#_Toc334767888)** [12](#_Toc334767888)

[7 Service Access Point (SAP) and primitives 12](#_Toc334767889)

[7.1 Introduction 12](#_Toc334767890)

[7.2 SAPs 12](#_Toc334767891)

[7.3 MIH\_LINK\_SAP primitives 12](#_Toc334767892)

[7.4 MIH\_SAP primitives 12](#_Toc334767893)

[7.4.29 MIH\_LL\_Transfer 12](#_Toc334767933)

[CandidateLinkList, 13](#_Toc334767963)

[Nonce 13](#_Toc334767964)

[Parameters: 13](#_Toc334767965)

[MNnetworkaccessid, 17](#_Toc334767966)

[TPoSIdentifier, 17](#_Toc334767967)

[7.4.30 MIH\_N2N\_LL\_Transfer 18](#_Toc334767969)

[MNID, 18](#_Toc334767970)

[CandidateLinkList 18](#_Toc334767971)

**[Parameters:](#_Toc334767972)** [18](#_Toc334767972)

**[Parameters:](#_Toc334767973)** [19](#_Toc334767973)

**[Parameters:](#_Toc334767974)** [21](#_Toc334767974)

**[Parameters:](#_Toc334767975)** [22](#_Toc334767975)

[8 Media independent handover protocols 23](#_Toc334767976)

[8.6 MIH protocol messages 23](#_Toc334767977)

[8.6.3 MIH messages for command service 23](#_Toc334767978)

[Note to editor: Clauses 9.2.2 is defined in IEEE 802.21a-2012. 25](#_Toc334767979)

[9 MIH protocol protection 26](#_Toc334767980)

**[9.2.2 Key derivation and key hierarchy](#_Toc334767981)** [26](#_Toc334767981)

**[9.2.2.1 Derivation of media independent session keys (MISKs)](#_Toc334767982)** [27](#_Toc334767982)

[Output: MIRK 28](#_Toc334767983)

[10 Proactive Authentication 28](#_Toc334767984)

[10.1 Media specific proactive authentication 28](#_Toc334767985)

[ADD NEW FIGURE 29](#_Toc334767986)

**[Figure 47—Protocol Stack for MIH Supported optimized pull key distribution with two PoSes](#_Toc334767987)** [29](#_Toc334767987)

[ADD THE FOLLOWING EXPLANATION 29](#_Toc334767988)

[11 Single Radio Handover 29](#_Toc334767989)

[11.1 Introduction 29](#_Toc334767990)

[11.1.1 Need for single radio handover 29](#_Toc334767991)

[11.1.2 Relationship to other network standards 30](#_Toc334767992)

[11.1.3 Single radio versus dual radio handover 30](#_Toc334767993)

[11.1.4 Media independent single radio handover 31](#_Toc334767994)

[11.2 Requirements of Single Radio Handover 31](#_Toc334767995)

[11.3 Assumptions of Single Radio Handover 32](#_Toc334767996)

[11.4 SRHO Reference Model 33](#_Toc334767997)

[Figure 11.1. Reference model for SRHO from a source network to a target network. 34](#_Toc334767998)

[11.4.1 Link configurations 34](#_Toc334767999)

[11.4.2 Information Repository 35](#_Toc334768000)

[11.4.3 Single Radio Services offered by 802.21 Point of Service 36](#_Toc334768001)

[Figure 11.2 An architecture of distributed mobility management. 37](#_Toc334768002)

[11.4.4 Single Radio handover Control Function 38](#_Toc334768003)

[11.4.5 Transport of L2 network entry PDU of the target radio 39](#_Toc334768004)

[11.4.6 Communication between the MN and the target network 40](#_Toc334768005)

[11.4.7 Communication between the MN and the target PoA 40](#_Toc334768006)

[11.5 Single radio handover overall processes 43](#_Toc334768007)

**[Figure 11.7](#_Toc334768008)** [– Overall Single Radio Handover Procedures 43](#_Toc334768008)

[2. The handover decision may involve the following 43](#_Toc334768009)

[11.6 Securing Single-Radio messages using PoS 44](#_Toc334768010)

[11.6.1 Overview 44](#_Toc334768011)

[Figure 11.8: MN handover signaling for preregistration using SPoS 45](#_Toc334768012)

[Table X : Key notation for PoS-based handover 46](#_Toc334768013)

[Annex A. 49](#_Toc334768014)

**[Data type definition](#_Toc334768015)** [49](#_Toc334768015)

[A.1 Derived data types 49](#_Toc334768016)

**[Table A.1—Data types for information elements](#_Toc334768017)** [49](#_Toc334768017)

[Annex B. 50](#_Toc334768018)

[12 Information element identifiers 50](#_Toc334768019)

**[Table B.1—Information element identifier values](#_Toc334768020)** [50](#_Toc334768020)

[Annex C. 50](#_Toc334768021)

[Annex D. 50](#_Toc334768022)

[Annex E. 50](#_Toc334768023)

[Annex F. 50](#_Toc334768024)

**[F.3 Derived data types](#_Toc334768025)** [50](#_Toc334768025)

**[F.3.16 Data type for security](#_Toc334768026)** [50](#_Toc334768026)

[Note to the editor: Table F.24 is presented in 802.21](#_Toc334768027)*[a](#_Toc334768027)* [document 50](#_Toc334768027)

[ADD FOLLOWING DATA TYPE TO TABLE F.24 50](#_Toc334768028)

[Annex G. 51](#_Toc334768029)

[Annex H. 51](#_Toc334768030)

[Annex I. 51](#_Toc334768031)

[Annex J. 51](#_Toc334768032)

[Annex K. 51](#_Toc334768033)

[Annex L. 51](#_Toc334768034)

***[Insert the following rows to Table L.1](#_Toc334768035)*** [51](#_Toc334768035)

*[Insert the following TLVs to Table L.2](#_Toc334768036)* [52](#_Toc334768036)

[Annex M. 52](#_Toc334768037)

[Annex N. 53](#_Toc334768039)

[Figure N.6 1: Signaling diagram for symmetric key distribution to TPoS and MN from SPoS 54](#_Toc334768040)

[The signaling diagram illustrated in Figure N.6 1 shows the following steps 54](#_Toc334768041)

[Annex O. 58](#_Toc334768042)

[Annex P. MN’s Network Access Identifier Format 58](#_Toc334768043)

[Annex Q. Network discovery for single radio handover 58](#_Toc334768044)

[Annex R. Examples of SRHO 60](#_Toc334768045)

[R.1 WLAN to WiMAX single radio handover 60](#_Toc334768063)

[Figure R.1 WLAN to WiMAX single radio handover reference model. 60](#_Toc334768064)

**[Functional entities:](#_Toc334768065)** [60](#_Toc334768065)

[R.1.1 Transport of WiMAX L2 control frames between MN and the WiMAX ASN 61](#_Toc334768066)

[R.1.2 WLAN to WiMAX Single Radio Handover processes 65](#_Toc334768067)

[R.2 3GPP to WiMAX single radio handover 67](#_Toc334768068)

[Figure R.5 3GPP to WiMAX single radio handover reference model. 67](#_Toc334768069)

[R.2.1 Transport of WiMAX L2 control frames between MN and the WiMAX ASN 68](#_Toc334768070)

[R.2.2 3GPP to WiMAX Single Radio Handover processes 72](#_Toc334768071)

[R.3 WiMAX to WLAN single radio handover 74](#_Toc334768072)

[Figure R.9 WiMAX to WLAN single radio handover reference model. 75](#_Toc334768073)

**[Functional entities:](#_Toc334768074)** [75](#_Toc334768074)

[Interfaces: 75](#_Toc334768075)

[R.3.1 Transport of WLAN L2 control frames between MN and the WLAN AN 75](#_Toc334768076)

[R.3.2 WiMAX to WLAN Single Radio Handover processes 79](#_Toc334768077)

[R.4 WiMAX to 3GPP single radio handover 81](#_Toc334768078)

[Figure R.13 WiMax to 3GPP single radio handover reference model. 81](#_Toc334768079)

**[Functional entities:](#_Toc334768080)** [82](#_Toc334768080)

[R.4.1 Transport of 3GPP L2 control frames between MN and the 3GPP network 83](#_Toc334768081)

[R.4.2 WiMAX to 3GPP Single Radio Handover processes 87](#_Toc334768082)

[R.5 WLAN to 3GPP single radio handover 89](#_Toc334768083)

[Figure R.17 Non-trusted WLAN AN to 3GPP single radio handover reference model. 89](#_Toc334768084)

**[Functional entities:](#_Toc334768085)** [89](#_Toc334768085)

[R.5.1 Transport of 3GPP L2 control frames between MN and the 3GPP network 91](#_Toc334768086)

[R.5.2 Non-trusted WLAN AN to 3GPP Single Radio Handover processes 95](#_Toc334768087)

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

**Part 21: Media Independent Handover Services**

**Amendment: Optimized Single Radio Handovers**

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

**Keywords:**

**IEEE Standard for**

**Local and metropolitan area networks—**

**Part 21: Media Independent Handover** **Services**

**Amendment: Optimized Single Radio Handovers**

# Overview

## 

## 

## General

# Normative references

IEEE 802 standard, “IEEE Draft Standard for Local and metropolitan Area Networks: overview and Architecture, P802-D1.2, November 2010.

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.

3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses,” TS23.402

WiMAX Forum Network Architecture: Stage 3 Detailed Protocols and Procedures T33-001-R015

WiMAX Forum, “Single radio interworking,” WMF-T37-011-R016v01.

WiMAX Forum, “WiFi-WiMAX Interworking,” WMF-T37-010-R016v01.

3GPP2, “WiMAX-HRPD Interworking: Core network aspects,” X.S0058.

# Definitions

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

Single Radio handover Control Function (SRCF): 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 SRCF entities through IP transport. The exchanged SRC frames are processed by the SRCF which has the assigned transport layer protocol’s port number. SRCF 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 SRCF entity.

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

# Abbreviations and acronyms

ANDSF Access Network Discovery Selection Functions

SRHO Single Radio Handover

# General architecture

# MIH Services

## General

## Service management

## Media independent event service

## Media independent command service

## Media independent information service

### Information Element

The Information Server provides the Point of Service (PoS) 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.

Table 1 represents the list of Information Elements and their semantics modified and defined SRHO. Each Information Element has an abstract data type (see Annex A for detailed definitions).

**Table 1 – Information Element**

|  |  |  |
| --- | --- | --- |
| **Name of information element** | **Description** | **Data type** |
| **Access network specific information elements** | | |
| IE\_NET\_CAPABILITIES | Bitmap of access network capabilities. | NET\_CAP |
| **802.21 Point of Service information elements** | | |
| IE\_PoS\_IP\_ADDR | IP address of PoS | IP\_ADDR |
| IE\_PoS\_TUNN\_MGMT\_PRTO | Type of tunnel management protocol supported. | IP\_TUNN\_MGMT |
| IE\_PoS\_FQDN | FQDN of PoS. | FQDN |

### IE Containers

In the binary representation method, the Information Element Containers are defined. The containers are used in the type-length-value (TLV) based query method. A new Information Element, namely the IE\_CONTAINER\_PoS, is defined for SRHO.

IE\_CONTAINER\_PoS – contains all the information depicting a PoS as shown in Table 2.

**Table 2 – IE\_CONTAINER\_PoS definition**

|  |  |
| --- | --- |
| Information element ID = (see Table B.1) | Length = *variable* |
| IE\_PoS\_IP\_ADDR | |
| IE\_PoS\_TUNN\_MGMT\_PRTO | |
| IE\_PoS\_FQDN | |

# Service Access Point (SAP) and primitives

## Introduction

## SAPs

## MIH\_LINK\_SAP primitives

## MIH\_SAP primitives



### MIH\_LL\_Transfer



#### MIH\_LL\_Transfer.request

##### Function

This primitive carries link-layer frames between the MN and a possibly non-local MIHF.

##### Semantics of service primitive

MIH\_LL\_Transfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

Nonce

)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | Ias |
|  |  | : included if the target link is knownIa |
|  |  | : included if the target link is known C |
| PoS | PoS | TPoS |
|  | PoA |  |
| Nonce | NONCE | (Optional) Nonce (Nonce TLV) |



##### When generated

This primitive is generated by an MIH user to start an authentication and association process based on link-layer frames.

##### Effect on receipt

After reception of this primitive, the MIHF must generate an MIH\_LL\_Transfer request message towards the MIHF of the serving PoS, which must relay the link-layer frames transported in this message to the target PoS.

#### MIH\_LL\_Transfer.indication

##### **Function**

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

##### **Semantics of service primitive**

MIH\_LL\_Transfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList

)

Parameters:

|  |  |  |
| --- | --- | --- |
| **Name** | **Data type** | **Description** |
| SourceIdentifier | MIHF\_ID | Identifies the invoker, typically a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional)This identifies the remote PoA that is the corresponding peer of the L2 exchange[[1]](#footnote-3). This attribute shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | This carries link layer frames. This attribute shall be included if the target link is known. |
| TPoSIdentifier | TPoS\_ID | (Optional) This identifies the target PoS |
| 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. |

##### When generated

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

##### Effect on receipt

The MIH user must generate an MIH\_LL\_Transfer.response primitive or invoke an MIH\_N2N\_LL\_Transfer.request primitive to send an MIH\_N2N\_LL\_Transfer request message to the MIHF on the target PoS before invoking the MIH\_LL\_Transfer.response primitive.

#### MIH\_LL\_Transfer.response

##### Function

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

##### Semantics of service primitive

MIH\_LL\_Transfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

TPoSIdentifier,

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. [[2]](#footnote-4) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; included if and only if the corresponding MIH\_LL\_Transfer.indication contained LLInformation. |
| MNnetworkaccessid | NAI | (Optional) Carries the MN’s Network Access Identifier in the case optimized pull key distribution is used. |
| TPoSIdentifier | TPoS\_ID | (Optional) This identifies the target PoS |
| Status | STATUS | Status of the operation. |

##### 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.

##### Effect on receipt

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

#### MIH\_LL\_Transfer.confirm

##### Function

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

##### Semantics of service primitive

MIH\_LL\_Transfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

TPoSIdentifier,

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. [[3]](#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 | NAI | (Optional) This carries the MN’s Network Access Identifier in the case optimized pull key distribution is used |
| TPoSIdentifier | TPoS\_ID | (Optional) This identifies the target PoS |
| Status | STATUS | Status of the operation. |

##### When generated

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

##### 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.

### MIH\_N2N\_LL\_Transfer

The primitives defined are to transport media link-layer frames over MIH between the serving PoS and the target PoS. The media specific authentication is conducted with the media specific authenticator deployed in the target PoA.

#### MIH\_N2N\_LL\_Transfer.request

##### Function

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

##### Semantics of Service Primitive

MIH\_N2N\_LL\_Transfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNID,

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; [[4]](#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. |
| 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. |

##### When generated

This primitive is generated by the serving PoS to relay link layer frames to the target PoS when the serving PoS receives an MIH\_LL\_Transfer request message.

##### Effect on receipt

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

#### MIH\_N2N\_LL\_Transfer.indication

##### Function

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

##### Semantics of service primitive

MIH\_N2N\_LL\_Transfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

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. [[5]](#footnote-7) This attribute shall be included if the target link is known. |
| 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 serving PoS. This parameter can be used only if the PoA supports EAP or ERP for media-specific access authentication. |

##### When generated

##### Effect on receipt

The MIH user must generate an MIH\_N2N\_LL\_Transfer.response primitive.

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.

#### MIH\_N2N\_LL\_Transfer.response

##### Function

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

##### Semantics of service primitive

MIH\_N2N\_LL\_Auth.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNnetworkaccessid,

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. [[6]](#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 | NAI | (Optional) Carries the MN’s Network Access Identifier when optimized pull key distribution is used. |
| Status | STATUS | Status of the operation. |

##### When generated

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

##### Effect on receipt

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

#### MIH\_N2N\_LL\_Transfer.confirm

##### Function

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

##### 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. [[7]](#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 | NAI | (Optional) This carries the MN’s Network Access Identifier when optimized pull key distribution is used |
| Status | STATUS | Status of the operation. |

##### When generated

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

##### Effect on receipt

The MIH user invokes an MIH\_LL\_Transfer.response primitive with the information obtained from this primitive.

# Media independent handover protocols

## MIH protocol messages

### MIH messages for command service

#### MIH\_LL\_Transfer request

This message is used by an MIHF to carry link layer frames to conduct 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 serving PoS.

|  |
| --- |
| **MIH Header Fields (SID=1, Opcode=1, AID=9)** |
| 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) |
| 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.)

#### MIH\_LL\_Transfer response

This message is used for an MIHF to carry link layer frames to conduct an authentication. 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=9)** |
| **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) |
| SALifeTime (optional)  (Lifetime TLV) |
| Status  (Status TLV) |

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

#### MIH\_N2N\_LL\_Auth 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 Ktpos. -. 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 Ktpos 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=9)** |
| **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) |
| SALifeTime (optional) (Lifetime TLV) |

#### MIH\_N2N\_LL\_Auth response

This message is used for an MIHF to carry link layer frames to conduct an authentication. The corresponding primitive is defined in Section 7.4.30.3

|  |
| --- |
| **MIH Header Fields (SID=1, Opcode=2, AID=9)** |
| **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) |
| Status  (Status TLV) |

# MIH protocol protection

Note to editor: Modify section 9.2.2 (defined in IEEE 802.21a) as follows:

**9.2.2 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 Serving 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 Serving PoS via MIH service access authentication using EAP. In the second option (i.e., non-EAP-based MIRK), an MIRK is generated by the Serving PoS independently of the MIH SA established between the MN and Serving 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.

**9.2.2.1 Derivation of media independent session keys (MISKs)**

**9.2.2.2 EAP-based MIRK**

During an optimized pull key distribution process that involves the MN, the serving PoS and a target PoS, the serving 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*).

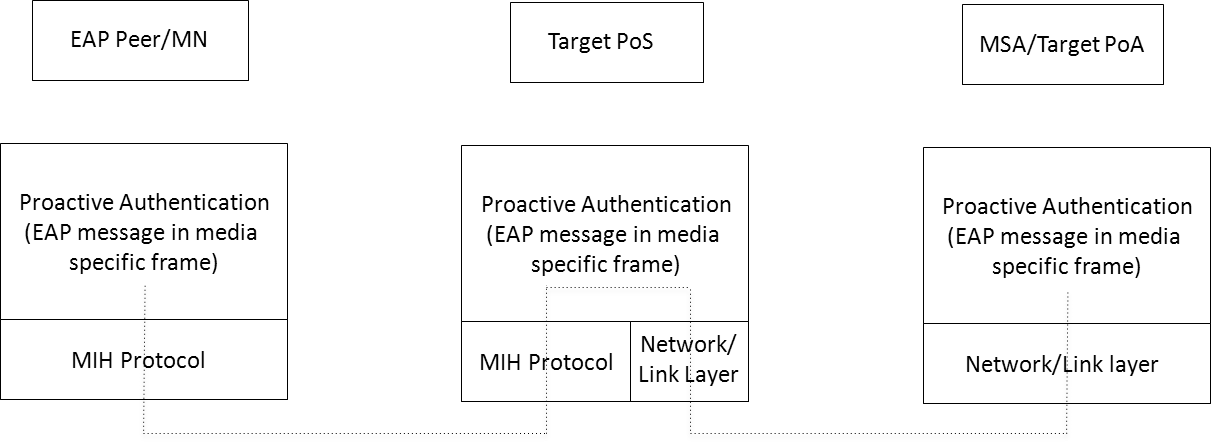
Output: MIRK

It is important to note that the key distribution of a MIRK from the Serving PoS to the target PoS may produce a security weakness so-called “domino effect” [rfc4962]. This weakness implies that the compromise of the serving 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.

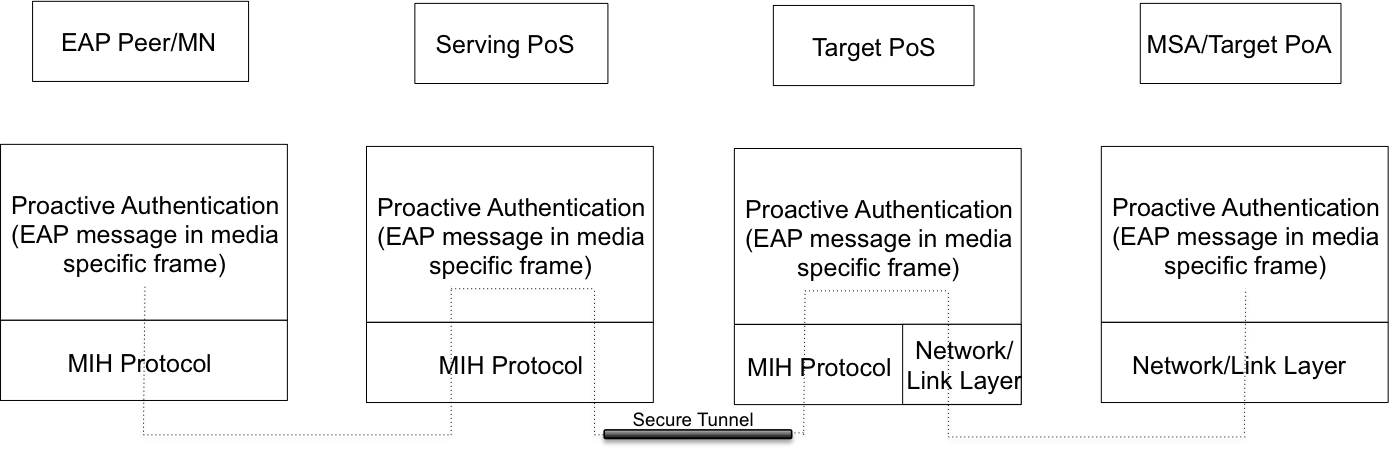
# Proactive Authentication

## Media specific proactive authentication

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



ADD NEW FIGURE



**Figure 47—Protocol Stack for MIH Supported optimized pull key distribution with two PoSes**

ADD THE FOLLOWING EXPLANATION

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

# Single Radio Handover

## Introduction

### Need for single radio handover

In a single radio handover, a mobile node can transmit on only one radio at a time. The needed peak transmission power capability for the mobile node is therefore smaller than if the mobile node were to transmit on both the source radio and the target radio simultaneously. In addition, the design of signal filter at the radio receiver is simpler if one radio is not transmitting when another radio is receiving. The lower peak power transmission and the simpler filter design for the mobile device both contribute to lower cost and longer battery life for the mobile device.

Such a lower cost design is appealing especially to the consumer market which is experiencing a proliferation of multiple radio interface devices using different network technologies.

### Relationship to other network standards

Network standards organizations such as WiMAX Forum and 3GPP have considered single radio handover from/to their networks. With heterogeneous networks involved in a single radio handover, a media independent single radio handover standard can avoid duplicating the technology for the different networks and achieve higher volume production using the same technology. The resulting economy of scale can benefit both network service providers and vendors. This standard provides such a media independent single radio handover optimization and explains how the individual network standards may tailor it to the needs of their specific networks.

### Single radio versus dual radio handover

A mobile device switches its link to the network during a handover process. The link is between a radio interface of the device and a point of attachment in a network. In the handover process, the radio interface may or may not change, whereas the point of attachment in the network also may or may not change to a different network technology.

If the radio interface remains the same, the handover is from one point of attachment to another point of attachment in the same network technology. This type of handover is sometimes called a horizontal handover. While the source and target networks are of the same type of network technology, the source and target points of attachment may belong to the same or to different access networks, and different access networks may themselves connect through the same or different networks to the Internet. An example of the handover involving only one radio interface is the handover with one WiMAX interface from one WiMAX base station to another WiMAX base station. A single interface device can only perform a single radio handover, whereas a multiple-interface device has more options.

A multiple-interface device connecting with one interface to a network may change the connection using an interface to another network of a different network technology. This type of handover is a heterogeneous network handover, with which the multiple-interface device is able to exploit the availability of the different networks to enjoy more opportunities and choices of network connectivity.

When the multiple-interface device performs handover from a source radio interface to a target radio interface, it is possible to perform a dual-radio handover which has an overlap period utilizing both radios simultaneously. Such a make-before-break handover, in which there is an overlap period during which both radios are fully on, has the advantage of avoiding handover delay and packet loss. Yet the device must then possess the functional capability for both radios to operate simultaneously during the dual-radio handover. The resulting requirements to the device are higher peak power consumption and more demanding filtering of receiver signals.

An alternative is to perform a single radio handover, in which the mobile device is allowed to transmit on only one radio at any time. Because the power consumption of the transmitter is high compared with that of the rest of the radio, limiting to only one radio transmission at a time will reduce the peak power consumption of the device.

A dual-radio handover also typically requires a sharper receiver signal filter. When a radio is transmitting, the receiver of the same radio may or may not be receiving signals. If the receiver is not receiving signal (e.g., when time division duplex is used) there is no interference between the transmitter signal and the receiver signal. If the receiver is receiving signal (e.g., when frequency division duplex is used) the frequency bands for transmission for reception in the same network technology must not be too close to each other. Yet with two different network technologies, there is generally no coordination to sufficiently separate the transmission frequency of one technology from the receiver frequency of another technology.

An additional requirement may therefore be imposed on single radio handover, to disallow one radio from transmitting when another radio is receiving. This restriction will result in simpler filter design and therefore further reduction in the cost of the device.

Other than the above requirements, a single radio handover does not exclude both radios to be receiving simultaneously when no radio is transmitting.

With the restrictions on the single radio handover, certain operations that are possible in the dual-radio handover will not be possible. New functions and therefore new functional requirements (Clause 11.2) are needed in single radio handover. The single radio handover therefore differs from the dual-radio handover in that the device follows a different signaling procedure (Clause 11.5 and 11.6) whereas the network provides the needed network support with the different network configuration (Clause 11.3) to optimize the handover performance.

As with a dual-radio handover, a single radio handover among different access technologies also includes a L2 handover and a L3 handover. At the link layer, a handover involves a change of the layer 2 network link.

The L2 handover related signaling messages, which terminate at the L2 endpoints of the radio link, involve L2 interfaces in the different network technologies. It is also possible to use IP packets to deliver signaling messages, which are then independent of the network medium.

### Media independent single radio handover

The concept of media independence applies to the single radio handover as it does to the dual-radio handover: Although the network technologies involving the two different L2 radio interfaces differ, it is possible to define generic signaling messages which are the same for different radio interfaces. 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 handover.

In a single radio handover using the media independent messages, the same transport possibilities as MIHF may apply. The requirements for single radio handover are described next in Clause 11.2.

## Requirements of Single Radio Handover

The following are the lists of requirements to assist and facilitate the single radio handover among different radio access technology networks.

General Requirements:

* The defined mechanisms shall be applicable to the single radio mobile station whether the station activates the dual receivers for both access networks or only a single receiver for the current access network.
* The defined mechanisms shall be applicable to various interworking scenarios (e.g., WiMAX-3GPP, WiMAX-WiFi, 3GPP-WiFi, etc.)
* The impact on existing access network architectures (3GPP, 3GPP2, WiMAX, WiFi) shall be minimized

Functional Requirements:

* The mechanism shall enable delivery of radio measurement configuration and report information within a media-independent container for a single radio mobile station.
* The mechanism shall define a tunneling mechanism to deliver the pre-registration messages.
* The defined mechanism shall provide a way to control pre-registered states and deliver pre-registered contexts to enable single-radio operation.
* The mechanism shall assist the mobile station to detect the presence of single radio enabling entity at the network before attaching to the target access network.
* The mechanism shall assist the mobile station to select an appropriate target network and to obtain the corresponding required information from the access network.
* The following capabilities shall be communicated between mobile station and single radio enabling entity at the network.

Supported radio access technologies (RATs) types on mobile station (3GPP, WiMAX, WiFi, 3GPP2, etc.)

Whether it supports single radio handover or dual radio handover

Applicable frequencies bands per access technology

Transmit Configuration (Single/Dual)

Receive Configuration (Single/Dual)

Measurement Gaps (UL/DL)

Whether the networks is allowing pre-registration

## Assumptions of Single Radio Handover

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. If sufficiently sharp signal filtering is lacking, then 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. If sufficiently sharp signal filtering is lacking, then while the source radio is transmitting, the target radio shall not receive at a frequency close to the frequency of the source radio transmitter.
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.

## SRHO Reference Model

The reference model for single radio handover from a source network to a target network is shown in Figure 11.1. Before handover, the MN uses its source interface to attach to the source point of attachment (PoA) in the source network through a source link. After handover, the MN will use its target interface to attach to the target PoA in the target network through a target link.

Figure 11.1. Reference model for SRHO from a source network to a target network.

### Link configurations

Link configuration before handover:

1. Between the MN and source network: The source (radio) interface is connected to a source PoA in a source (access) network through a source link. This source link can exchange both data and signaling.
2. Between the MN and target network: Not specified.

Link configuration after handover:

1. Between the MN and source network: Not specified.
2. Between the MN and target network: The target (radio) interface is connected to a target PoA in a target (access) network through a target link. This target link can exchange both data and signal.

Link configuration during handover:

1. Between the MN and source network: The source (radio) interface remains connected to the source PoA in the source network. This source link can exchange both data and signal.

The control plane function in the MN and in the source network may use this source link to transport control messages.

1. Between the MN and target network: The link between the MN and the target network has a lower priority than the source link and communication may happen subject to meeting the constraints given in section 11.3.

The MN’s target radio can only transmit during the time when both the following conditions are met:

1. the source radio is not transmitting
2. its transmission will not interfere with the source radio receiver such as by selecting frequencies sufficiently far from the frequencies at which the source radio is receiving or when sufficient signaling filter is available.

The MN’s target radio can expect to receive valid signals from the target PoA under any one of the following conditions:

* 1. the source radio is not transmitting, or
  2. there is sufficient filtering from the source radio transmitter, or
  3. the MN can select frequencies to avoid interference from its source transmitter.

The control plane function in the MN and in the target network may use this link to transport control messages only under the above conditions.

The source network and the target network may communicate with each other. For example, shortly after handover, packets delivered to the source network may be forwarded or tunneled to the target network.

### Information Repository

The Information Repository comprises a distributed database with location management and network service information. It must therefore be accessible from both the source and target networks with appropriate authorization. This authorization may, for roaming partners, require additional authentication and secure communication channels.

Location management requires location information for the networks and the MN. The location information for networks at a geographic location could be included as a list of the access networks or base stations that are within range at that geographic location. The location of the MN in the network would include the network location to which the MN is currently attached. That enables the network to estimate the geographic location of the MN when its exact location is not known. In addition to this location there may be an identity or a network address of the MN, which enables global reachability.

The network service information indicates the availability of candidate target networks and may be based on network operator service policy, roaming agreement between network service operators, the existing load versus capacity of the network, etc.

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 distributed components of the Information Repository may be further organized to include localized database caches for improved performance. These localized caches may include information originally obtained from the Information Repository components of several roaming partners, or any other local information acquired by other means.

While location information and network service information are needed to enable handover decisions, some location information may also be needed in a mobility management protocol. It is then convenient to co-locate the location information for the mobility management protocol with the information needed for handover decision in the same database referred to as the distributed database of Information Repository in this reference model.

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.

### Single Radio Services offered by 802.21 Point of Service

The Point of Service in this design bridges the mobility signaling between the MN and the target network via the source network. When the MN signals to the PoS as if signaling to a point of attachment (PoA), the target PoA may respond by signaling to the PoS which acts like a virtual MN. The PoS 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 PoS, which processes these control frames. Before replying to the control frames, the PoS may communicate with the appropriate network entities in the target network to enable conducting any needed functions requested in the control frame, such as as pre-registration and proactive authentication of the MN. It resides in the Point of Service in the target network, and its single radio handover functions may be implemented using the media independent point of service (PoS), as defined in this Clause.

The PoS often needs some location management and network service information to perform its function. It may cache the needed information.

Some PoS 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 PoS 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 PoS functions may be implemented as an extension of the Mobility Management Entity (MME).

In a target 3GPP2 network, the PoS 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 PoS should be provided in a media independent manner. Such signaling may take advantage of the Media Independent messages defined in this specification. If a new message is to be used that is not defined here, it can be encapsulated with a media independent control frame header.

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 PoS may be co-located. The PoS at the home network, source network, and target network are respectively hPoS, sPoS, and tPoS. The distributed mobility management architecture is then shown in Figure 11.2 Figure 11.8in which the Information Repository contains the logical function of location management information only and the PoS contains the logical function of mobility routing only.



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.

### Single Radio handover Control Function

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 (SRCF) 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.

Figure 11.3 shows the Single Radio handover Control Function (SRCF) in a multiple interface node. The SRCF is part of the media independent control function (MICF) in the control plane, which is defined in the 802-2010 architecture [IEEE P802-D1.2].



Figure 11.3. Single Radio handover Control Function (SRCF) of a multiple interface mobile node within the Media Independent Control Function (MICF).

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP), and the SRCF uses an assigned transport layer protocol’s port number. Therefore, the SRCF in this local node may exchange single radio handover control (SRC) frames with the SRCF of a remote node as long as there is TCP or UDP / IP connection between these two nodes. The SRC frames are processed by the SRCF in the destination of the TCP or UDP / IP packets carrying the SRC frames. The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame of a deactivated link (e.g., interface 2) may therefore be encapsulated with a SRCF header to constitute a SRC frame, which is then exchanged via an active link between the SRCF’s of a local and a remote node using the TCP or UDP / IP connection between the two nodes.

### Transport of L2 network entry PDU of the target radio

The transport of L2 network entry PDUs of the target radio between the MN and the PoS in the target network is enabled by the MiCLSAP to the SRCF. The communication between the SRCF in the MN and the SRCF in the PoS is shown in Figure 11.4.

(a)



(b)

Figure 11.4. Transport of L2 frame of target interface using the communication between the SRCF in the MN and the SRCF in the PoS. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking physical connection between the MN’s target radio and the target network during a single radio handover, a L2 network entry PDU of the target radio requires service from SRCF. Passing to the SRCF via the MiCLSAP, the L2 PDU becomes the payload of an SRC frame in the media independent control function of the MN. Only the source radio is fully capable of transmitting and receiving TCP or UDP / IP packets to/from the source access network, which has IP connection to the target network through the Internet. There is therefore TCP or UDP / IP transport between the source radio and the PoS of the target network via the source interface. Building on the TCP or UDP / IP layer through the MICSAP, the SRCF at the MN may therefore communicate with the SRCF at the PoS.

### Communication between the MN and the target network

The MN may only communicate with the target PoA subject to restrictions explained in Session 11.4.1 above. When it is not possible to use the target radio link, the source link can be used to provide (via SRCF) a reliable means of communication with the target network.

(1) The MN may signal directly with the target network PoS if the MN knows the IP address of the target PoS and does not need the help of the source network PoS. In particular, the target network PoS may proxy between the MN and the target PoA.

(2) The MN may signal first with the source network PoS, which will assist the MN to communicate with the target network PoS. In particular, the source network PoS may relay between the MN and the target PoS.

### Communication between the MN and the target PoA

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 the PoS, and the MN may query the Information Repository to find the IP address of the PoS in order to use this TCP or UDP / IP transport. The second part of this communication depends on whether the target PoA supports MICF in the 802-architecture or whether it is a legacy PoA lacking such support.

If the target PoA supports MICF, the network entry L2 frame is encapsulated into SRC frames to forward to the target radio as shown in Figure 11.5.

(a)



(b)



Figure 11.5. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the PoS via the source radio interface, in the absence of the target link. The PoS bridges between the MN source link and the target PoA. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The MN will need to acquire information of the candidate target PoA, e.g. by querying the Information Repository.

If MN knows the IP address of the target PoA, SRC frames may be exchanged between the SRCF in the MN and the SRCF in the target PoA using TCP or UDP / IP transport.

If MN does not know the IP address of the target PoA, it will need to have some means, such as the link-layer identification, of the target PoA in order to perform network entry procedure. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the PoS as described in Clause 11.4.3. The SRC frame contains information for the target network to identify the target PoA. The PoS will find out the IP address of the target PoA and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target PoA. In other words, the PoS can function like a proxy for the MN to send the target radio L2 network entry packets to the target PoA.

The reply by the target PoA is transported in a similar manner. If the target link were available, the target PoA will send a L2 message back to the target radio of the MN. Lacking this target link, this L2 message is passed through the MiCLSAP to become the payload of an SRC frame.

If the target PoA had received the SRC frame from the MN, this reply SRC frame uses TCP or UDP / IP transport with an IP address destined to the MN. Yet if the target PoA had received the SRC frame from the PoS, the reply SRC frame will first use TCP or UDP / IP transport with an IP address destined to the PoS. At the PoS, the TCP or UDP / IP header is extracted at the MICSAP at the input interface of the PoS to retrieve the SRC frame. The SRCF function will pass the SRC frame through the MICSAP at the output interface of the PoS to form a new TCP or UDP / IP packet with an IP address destined to the MN.

If the target PoA’s are legacy PoA’s lacking MICF support, the PoS will need other communication mechanism in order to proxy between the MN and the target PoA.

Figure 11.6 shows the transport of target radio L2 frames between the MN and the target network when the MN, the PoS support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? Architecture, but the target PoA are legacy PoA’s lacking MICF support.

Lacking MICF support in the target PoA, the PoS and the target PoA 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 PoS may then proxy between the MN and the target PoA using SRCF 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 PoS may map the message contents exchanged with the MN with that exchanged with the target PoA in performing the proxy function.

(a)



(b)



Figure 11.6. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the PoS via the source radio interface (if1), in the absence the target link. The PoS communicates with the target PoA using other control messages in order to proxy between the MN and the target PoA. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

## Single radio handover overall processes

A single radio handover following the above reference model may consists of different handover processes and involve different information elements (Clause 11.8) and messages (Clause 11.9). Examples of handover are described in Clause 11.6. Figure 11.7 shows the single radio handover procedures consisting of 5 processes as described below.



**Figure 11.7** – Overall 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 PoS 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.

2. The handover decision may involve the following

1. A handover trigger.
2. Target network selection
3. 802.21 Point of Service 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: Pre-registration includes pro-active authentication and establishing context (user identity, security, resource information) at the target network. With the help of PoS, the MN can perform network entry procedures towards the target network while still retaining its data connection with the source network. Optionally, the pre-registration process may occur before the network selection process as in the case of WiMAX network.

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. The MN’s target radio may perform limited signaling if possible within the constraints of peak power and signaling interface defined for single radio handover in this standard.

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.

## Securing Single-Radio messages using PoS

There is a need for a simplified yet secure method for enabling movement between the network domains of roaming partners for single-radio smartphones and Internet enabled wireless devices. The proposal outlined in this document makes effective use of the Point of Service (PoS) as defined in numerous recent documents developed in the WiMAX Forum, 3GPP2, and IEEE. 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 of interest in 802.21c.

### Overview

Security is indispensable to mobility management, but it is also 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. 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 PoSs in partner networks. It is expected that in many cases the PoSs 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 partner PoSs. It is out of scope for this document to specify exactly how the partner PoSs should establish secure communications, 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 [RFC 5996].

Figure 11.8: MN handover signaling for preregistration using SPoS

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 SPoS. 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 (SPoS).

For optimized handovers, a single-radio MN must perform as many protocol steps as possible for attachment to the target network, before actually tuning its radio to the access point of the target network. The entire reason for the existence of the PoS is to mediate signaling between the MN and a new target network while the MN is still radio contact with its current access network (i.e., to mediate "pre-registration"). The exact signaling steps included in the pre-registration 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.

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 retuned 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.

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.

Key notation for PoS-based handover is listed in Table X.

Table X : Key notation for PoS-based handover

|  |  |
| --- | --- |
| *K*hpos | key between MN and HPoS |
| *K*spos | key between MN and SPoS |
| *K*tpos | key between MN and TPoS; Ktpos is also referred to as the Media Independent Root Key (MIRK). |
| *K*hspos | key between HPoS and SPoS |
| *K*htpos | key between HPoS and TPoS |
| *K*stpos | key between SPoS and TPoS |
| PNGspos | pseudo-random number generator between MN and SPoS |
| PNGhspos | pseudo-random number generator between HPoS and SPoS |
| PNGstpos | pseudo-random number generator between SPoS 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 its home PoS (HPoS), based on a key *K*spos. Because of previous protocol operations, the MN has a current security association with the PoS in the originating network (SPoS).

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 SPoS, because SPoS either already has, or can readily establish, a security association with TPoS. Suppose SPoS already has the required security association with TPoS. Then, when MN begins forwarding preregistration traffic to TPoS via SPoS, SPoS 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 SPoS would thus forward the initial traffic to TPoS on behalf of the MN; the SPoS uses its own security relationship with TPoS to protect this initial preregistration signaling, and it also supplies the value of *K*tposto TPoS by adding a new extension to the preregistration traffic.

To send *K*tposto TPoS, SPoS provides the following payload within the TLVs of a new 802.21(c) message:

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

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

Similarly, to send Ktposto MN, SPoS provides the following payload within the TLVs of a new 802.21(c) message:

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

Upon receiving the payload, MN calculates *PNG*spos (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 SPoS using the keys it has available with TPoS and MN respectively. MN is allowed to send more signaling information to TPoS via SPoS even after SPoS distributes the keys; SPoS 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 SPoS, MN and TPoS should begin to use direct signaling as soon as possible and thus bypass SPoS. Other structures for the message payloads are also possible, depending on requirements.

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

It is possible for SPoS 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 SPoS. Subsequently, the SPoS 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 be easily be made available. Note, however, that discovery and secure communication with TPoS may be easier than discovery and secure communication with ANDSF.

**11.7.2 Protecting communications between serving PoS and target PoS**  
MIH\_N2N\_LL\_Transfer messages exchanged between the serving PoS and the target PoS may require security protection. Also, the target PoS may only accept these messages from an authenticated and authorized serving PoS. To protect the link between the serving 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 serving PoS and the target PoS. In this case, the serving 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 serving PoS and the target PoS. Details on such mechanisms are outside the scope of this standard.

(normative)

**Data type definition**

* + - 1. Derived data types

**Table A.1—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 11–31: (Reserved) |
| IP\_ADDR | TRANSPORT\_ADDR | Indicates the IP address family, either 1 (for IPv4) or 2 (for IPv6). |
| IP\_TUNN\_MGT | BITMAP(16) | Indicates the supported tunnel management protocol on PoS.  Bitmap Values:  Bit 0: IPsec  Bit 1–15: (Reserved) |
| FQDN | OCTET\_STRING | The fully qualified domain name of a host as described in IETF RFC 2181. |



(normative)

# Information element identifiers

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

|  |  |
| --- | --- |
| **Name of information element or container** | **IE Identifier** |
| IE\_NET\_CAPABILITIES | 0x1000010A |
| IE\_PoS\_IP\_ADDR | 0x10000206 |
| IE\_PoS\_TUNN\_MGMT\_PRTO | 0x10000207 |
| IE\_PoS\_FQDN | 0x10000208 |
| IE\_CONTAINER\_PoS | 0x10000303 |



**F.3 Derived data types**

**F.3.16 Data type for security**

Note to the editor: Table F.24 is presented in 802.21*a* document

ADD FOLLOWING DATA TYPE TO TABLE F.24

|  |  |  |
| --- | --- | --- |
| **Data** | **Derived from** | **Definition** |
| NAI | OCTET\_STRING | Represents a Network Access Identifier as in IETF RFC 4282 |
| TPoS\_ID | CHOICE(IP\_ADDR, MIHF\_ID) | Represents the identifier of the target PoS |



***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 |

*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 |
| Network Access Identifier | 80 | NAI |
| TPoS Identifier TLV | 81 | TPoS\_ID |



**N.6 Use of MIH\_LL\_Transfer for the exchange of L2 frames, including Optimized Pull Key Distribution**

This first call flow shows how the identity is bootstrapped by TPoS, how the MIRK[[8]](#footnote-10) is sent by the SPoS to the TPoS and how the MSPMK[[9]](#footnote-11) 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 SPoS are transmitted through the SPoA.



Figure N.6 1: Signaling diagram for symmetric key distribution to TPoS and MN from SPoS

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

1. MIH\_LL\_Transfer.request: the MN application asks to initiate preregistration to a suitable target PoS (TPoS)
2. MIH\_LL\_Transfer.request: MN’s MIHF relays request to Serving PoS (SPoS)
3. MIH\_LL\_Transfer.indication: SPoS’s MIHF presents MN’s request to SPoS MIH application.
4. MIH\_N2N\_LL\_Transfer.request: issued by MIHSPoS containing information to enable TPoS to compute MIRK (i.e., *K*tpos)
5. MIH\_N2N\_LL\_Transfer.request: relayed by MIHFSPoS to MIHFTPoS, possibly encapsulated with IPsec
6. MIH\_ N2N\_LL\_Transfer.indication: presented to MIHTPoS for extraction of *K*tpos and computation of MNmsrk
7. MIHTPoS provides MIRK to AAA for future authentication purposes
8. MIHTPoS computes MNmsrk from MIRK and sends appropriate LL frames to TPoA for key distribution and any other preregistration tasks.
9. MIH\_N2N\_LL\_Transfer.response: MIHTPoS initiates message for MIHSPoS containing MNnetworkaccessid.
10. MIH\_N2N\_LL\_Transfer.response: MIHFTPoS relays message to MIHFSPoS containing MNnetworkaccessid.
11. MIH\_N2N\_LL\_Transfer.confirm: MIHFSPoS presents message to MIHSPoS containing MNnetworkaccessid.
12. MIH\_LL\_Transfer.response: MIHSPoS initiates message to MIHMN via MIHFSPoS containing MNnetworkaccessid, MIRK.
13. MIH\_LL\_Transfer.response: MIHFSPoS relays message to MIHFMN containing MNnetworkaccessid, MIRK.
14. MIH\_LL\_Transfer. confirm: MIHFMN relays message to MIHMN containing MNnetworkaccessid, MIRK.
15. MIHMN 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 SPoS and TPoS are the same entity) the following example diagram applies for authentication at the TPoA:



Finally when the SPoS 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:



2. MN’s Network Access Identifier Format

(informative)

An MNnetworkaccessid attribute (of type NAI), 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 NAI 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 NAI may contain a Fully Qualified Domain Name of the target PoS.

1. Network discovery for single radio handover

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:

1. 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 shall follow the assumptions in Section 11.3.

1. 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.

1. With 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.

1. Examples of SRHO















18. * + 1. WLAN to WiMAX single radio handover

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:**

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.

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.

The PoS function is implemented in the combined functions of ASN-GW and WiMAX SFF, in the WiMAX network. When the MN signals to the PoS as if signaling to a point of attachment (PoA), the target PoA may correspondingly signal to that PoS acting in the role of a virtual MN. The PoS may also behave like a virtual PoA to signal with the target PoA.

The WiFi Interworking Function (WIF) is defined in WiMAX Forum.

Reference Points:

W3 interface between the WLAN AP and the WIF is defined in WiMAX Forum [WMF-T37-010-R016v01].

Rx interface between the MS and the WiMAX SFF/PoS is defined in WiMAX Forum [WMF-T37-010-R016v01].

R3 interface between the WiMAX CSN and ASN is defined in WiMAX Forum [WMF-T37-010-R016v01].

R3+ interface between the WIF and AAA and also DHCP in the WiMAX CSN is defined in WiMAX Forum [WMF-T37-010-R016v01].

R6 interface between the WiMAX PoS and ASN GW is defined in WiMAX Forum [T33-001-R015].

* + 1. Transport of WiMAX L2 control frames between MN and the WiMAX ASN

Figure R.2 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located PoS/ASN-GW and the target WiMAX BS all support single radio handover control function (SRCF), which is a media independent control function (MICF) in the 802-2010 architecture [IEEE P802-D1.2].

(a)



(b)



Figure R.2. Transport of WiMAX radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source WLAN link at the left and in the absence of the target WiMAX link at the right. The co-located PoS/ASN-GW bridges between the MN and the target WiMAX BS. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP). 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 single radio handover control (SRC) frames may be exchanged between the SRCF in the MN and the SRCF in the PoS/ASN-GW and/or the WiMAX BS in the WiMAX network using TCP or UDP / IP transport.

The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame is encapsulated with a SRCF header to constitute a SRC frame, which is exchanged between the MN and the target WiMAX BS or the co-located PoS/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.

It is required that the Information Repository need to know the IP address of the PoS/ASN-GW, so that the MN and the PoS/ASN-GW can exchange SRC 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 SRC frame to the SRCF 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 at least something, such as the link-layer address, to identify the target WiMAX BS. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the collocated PoS/ASN-GW as described in Clause 11.4.3. The SRC frame contains information for the target WiMAX network to identify the target WiMAX BS. The co-located PoS/ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target WiMAX BS.

The reply 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 through the MiCLSAP to become the payload of an SRC frame.

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

Figure R.3 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located PoS/ASN-GW support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? architecture. Yet the target WiMAX BS are legacy WiMAX BS’s lacking MICF support.

(a)



(b)



Figure R.3. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source WLAN link at the left and in the absence of the target WiMAX link at the right. The co-located PoS/ASN-GW proxies between the MN and the target WiMAX BS using MICF to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS. (a) shows the transport between MN and the co-located PoS/ASN-GW through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking MICF support in the WiMAX BS, the co-located PoS/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 co-located PoS/ASN-GW may then proxy between the MN and the target WiMAX BS using SRCF 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 co-located PoS/ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function. 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 control function (SRCF) is supported neither between the MN and the PoS/ASN-GW nor between the PoS/ASN-GW and the target WiMAX BS.



Figure R.4. Packet used in the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source WLAN link and in the absence of the target WiMAX link. The co-located PoS/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.

The MN and the co-located PoS/ASN-GW will need certain mechanism to communicate with each other, such as an extension (Rx+) of the Rx interface. The PoS/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 PoS/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 both outside the scope of this standard.

* + 1. WLAN to WiMAX Single Radio Handover processes

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 RFC6153. 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.

(In OMA, the target radio has to be in idle mode when OMA is utilized to push neighboring information of the target network. There is no such restriction with 802.21c.)

2: Pre-registration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the PoS, 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:

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 PoS/ASN-GW is through the source (WiFi) network as described in Article 11.6.1.1.

The ASN-GW/PoS processes the SRC frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.

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 PoS/ASN-GW, the pre-registration 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 PoS/ASN-GW already has this registration context.

The ASN-GW/PoS combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/PoS behaves like a virtual WiMX 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 source PoA and target PoA within the same network to prepare the handover of a MN within the same network.

For messages from the ASN-GW/PoS to the MN, they are tunneled to the MN via the WiFi network. To the target WiMAX BS, the ASN-GW/PoS acts like a virtual WiMAX radio interface.

The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.

3: 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 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.

4: 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 11.3.

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.

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 WiFi link layer address to the WiMAX link layer address, and future incoming packets are then routed to the WiMAX radio.

* + - 1. 3GPP to WiMAX single radio handover

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.

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.

The WiMAX Signal Forwarding Function (PoS) 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.

The PoS function is implemented in the combined functions of ASN-GW and WiMAX PoS, which are defined in the WiMAX network. When the MN signals to the PoS as if signaling to a point of attachment (PoA), the target PoA may signal to the PoS which acts like a virtual MN. The PoS may also behave like a virtual PoA to signal with the target PoA.

The PDN Gateway (P-GW) is defined in 3GPP [3GPP TS23.401].

Reference Points:

S2a reference point between the P-GW and the ASN GW is defined in 3GPP [3GPP TS23.402].

R9 interface between the MS and the WiMAX PoS is defined in WiMAX Forum [WMF-T37-011-R016v01].

R6 interface between the WiMAX PoS and ASN GW is defined in WiMAX Forum [T33-001-R015].

S14 reference point between the MS and the ANDSF is defined in 3GPP [3GPP TS23.402].

* + 1. Transport of WiMAX L2 control frames between MN and the WiMAX ASN

Figure R.6 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located PoS/ASN-GW and the target WiMAX BS all support single radio handover control function (SRCF), which is a media independent control function (MICF) in the 802-2010 architecture [IEEE P802-D1.2].

(a)



(b)



Figure R.6. Transport of WiMAX radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source 3GPP link at the left and in the absence of the target WiMAX link at the right. The co-located PoS/ASN-GW bridges between the MN and the target WiMAX BS. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP). 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 single radio handover control (SRC) frames may be exchanged between the SRCF in the MN and the SRCF in the PoS/ASN-GW and/or the WiMAX BS in the WiMAX network using TCP or UDP / IP transport.

The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame is encapsulated with a SRCF header to constitute a SRC frame, which is exchanged between the MN and the target WiMAX BS or the co-located PoS/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.

It is required that the Information Repository need to know the IP address of the PoS/ASN-GW, so that the MN and the PoS/ASN-GW can exchange SRC 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 SRC frame to the SRCF 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 at least something, such as the link-layer address, to identify the target WiMAX BS. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the collocated PoS/ASN-GW as described in Clause 11.4.3. The SRC frame contains information for the target WiMAX network to identify the target WiMAX BS. The co-located PoS/ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target WiMAX BS.

The reply 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 through the MiCLSAP to become the payload of an SRC frame.

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

Figure R.7 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located PoS/ASN-GW support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? architecture. Yet the target WiMAX BS are legacy WiMAX BS’s lacking MICF support.

(a)



(b)



Figure R.7. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source 3GPP link at the left and in the absence of the target WiMAX link at the right. The co-located PoS/ASN-GW proxies between the MN and the target WiMAX BS using MICF to communicate with the MN and using an extension of R6 interface to communicate with the target WiMAX BS. (a) shows the transport between MN and the co-located PoS/ASN-GW through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking MICF support in the WiMAX BS, the co-located PoS/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 co-located PoS/ASN-GW may then proxy between the MN and the target WiMAX BS using SRCF 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 co-located PoS/ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function. Figure R.8 shows the transport of WiMAX L2 frames between the MN and legacy WiMAX ASN where the single radio handover control function (SRCF) is supported neither between the MN and the PoS/ASN-GW nor between the PoS/ASN-GW and the target WiMAX BS.



Figure R.8. Packet used in the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WiMAX network via the source 3GPP link and in the absence of the target WiMAX link. The co-located PoS/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.

The MN and the co-located PoS/ASN-GW will need certain mechanism to communicate with each other, such as an extension (R9+) of the R9 interface. The PoS/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 PoS/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.

* + 1. 3GPP to WiMAX Single Radio Handover processes

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 RFC6153. 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 PoS, and system information blocks of candidate PoAs to perform radio measurements.

2: Pre-registration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the PoS, 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:

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 PoS/ASN-GW is through the source (3GPP) network as described in Article 11.6.2.1.The ASN-GW/PoS processes the frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.

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 PoS/ASN-GW, the pre-registration 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 PoS/ASN-GW already has this registration context.

The ASN-GW/PoS combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/PoS behaves like a virtual WiMX 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.

For messages from the ASN-GW/PoS to the MN, they are tunneled to the MN via the 3GPP network. To the target WiMAX BS, the ASN-GW/PoS acts like a virtual WiMAX radio interface.

The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.

3: 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.

4: 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 11.3.

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.

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.

* + - 1. WiMAX to WLAN single radio handover

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:**

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.

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.

The PoS function is implemented in the combined functions of WiFi Interworking Function (WIF) and WiFi PoS, which are defined in the WiMAX network. When the MN signals to the PoS as if signaling to a point of attachment (PoA), the target PoA may signal to the PoS which acts like a virtual MN. The PoS may also behave like a virtual PoA to signal with the target PoA.The WiFi Signal Forwarding Function (SFF) is defined in WiMAX Forum standard. It may co-locate at the access router (AR). In the event that it is not co-located there, the WiFi-PoS communicates with the AR through the W1 interface.

Interfaces:

W1 interface between the WLAN AR and the WiFi SFF is defined in WiMAX Forum [WMF-T37-010-R016v01].

W3 interface between the WLAN AR and the WIF is defined in WiMAX Forum [WMF-T37-010-R016v01].

Ry interface between the MS and the WiFi SFF is defined in WiMAX Forum [WMF-T37-010-R016v01].

R3 interface between the WiMAX CSN and ASN is defined in WiMAX Forum [WMF-T37-010-R016v01].

R3+ interface between the WIF and AAA and also DHCP in the WiMAX CSN are defined in WiMAX Forum [WMF-T37-010-R016v01].

R6 interface between the WiMAX SFF and ASN GW is defined in WiMAX Forum [WMF-T37-010-R016v01].

* + 1. Transport of WLAN L2 control frames between MN and the WLAN AN

Figure R.10 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the co-located PoS/WIF/AR and the target WLAN AP all support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2010 architecture [IEEE P802-D1.2].

(a)



(b)



Figure R.10. Transport of WLAN radio L2 control frame as a payload of a media independent control frame between the MN and the WLAN network via the source WiMAX link at the left and in the absence of the target WLAN link at the right. The co-located PoS/WIF/AR bridges between the MN and the target WLAN AP. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP). 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 single radio handover control (SRC) frames may be exchanged between the SRCF in the MN and the SRCF in the PoS/WIF/AR and/or the WLAN AP in the WLAN network using TCP or UDP / IP transport.

The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame is encapsulated with a SRCF header to constitute a SRC frame, which is exchanged between the MN and the target WLAN AP or the co-located PoS/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.

It is required that the Information Repository need to know the IP address of the PoS/WIF/AR, so that the MN and the PoS/WIF/AR can exchange SRC 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 SRC frame to the SRCF 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 at least something, such as the link-layer address, to identify the target WLAN AP. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the collocated PoS/WIF/AR as described in Clause 11.4.3. The SRC frame contains information for the target WLAN network to identify the target WLAN AP. The co-located PoS/WIF/AR will find out the IP address of the target WLAN AP and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target WLAN AP.

The reply 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 through the MiCLSAP to become the payload of an SRC frame.

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

Figure R.11 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the co-located PoS/WIF/AR support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? architecture. Yet the target WLAN AP are legacy WLAN AP’s lacking MICF support.

(a)



(b)



Figure R.11. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WLAN network via the source WiMAX link at the left and in the absence of the target WLAN link at the right. The co-located PoS/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. (a) shows the transport between MN and the co-located PoS/WIF/AR through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking MICF support in the WLAN AP, the co-located PoS/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 co-located PoS/WIF/AR may then proxy between the MN and the target WLAN AP using SRCF 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 co-located PoS/WIF/AR may map the message contents exchanged with the MN with that exchanged with the target WLAN AP in performing proxy function. Figure R.12 shows the transport of WLAN L2 frames between the MN and legacy WLAN AN where the single radio handover control function (SRCF) is supported neither between the MN and the PoS/WIF/AR nor between the PoS/WIF/AR and the target WLAN AP.



Figure R.12. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the WLAN network via the source WiMAX link at the left and in the absence of the target WLAN link at the right. The co-located PoS/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.

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

The co-located PoS/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.

* + 1. WiMAX to WLAN Single Radio Handover processes

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 RFC6153. 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.

2: 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.

3: Pre-registration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the PoS, 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:

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 Article 11.6.3.1.

(a)

The PoS (WIF/AR/WiFi-PoS) processes the SRC frame containing the L2 authentication message and may consult the AAA in the WiMAX CSN through the R3 interface.

The PoS (WIF/AR/WiFi-PoS) maintains the higher layer registration context including the security keys and the data path information to maintain the IP session. By registering with the PoS, the pre-registration 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 PoS already has this registration context.

The PoS (WIF/AR/WiFi-PoS combination) also constructs control messages to communicate with the target WLAN AP. In terms of exchange of these control messages, the WIF/AR/WiFi-PoS 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.

For messages from the WIF/AR/WiFi-PoS to the MN, they are tunneled to the MN via the WiMAX network. To the target WiFi AP, the WIF/AR/WiFi-PoS acts like a virtual WLAN radio interface.

The MN may pre-register with the WiMAX network, using the same interface and transport mechanism as that in proactive authentication.

4: 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.

5: 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.

* + - 1. WiMAX to 3GPP single radio handover

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:**

The Information repository function is implemented in the ANDSF in the 3GPP network.

The PoS function is implemented in the 3GPP-PoS and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-PoS 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 PoS as if signaling to a point of attachment (PoA), the target PoA may signal to the PoS which acts like a virtual MN. The PoS may also behave like a virtual PoA to signal with the target PoA.

Reference Points:

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].

S14 reference points between UE and ANDSF is defined in the 3GPP network [3GPP TS23.402].

S5/8 reference point between P-GW and S-GW is defined in the 3GPP network [3GPP TS23.401].

S11 reference point between S-GW and MME is defined in the 3GPP network [3GPP TS23.401].

S1-U reference point between UE and S-GW is defined in the 3GPP network [3GPP TS23.401].

S1-MME reference point between UE and MME is defined in the 3GPP network [3GPP TS23.401].

S6a reference point between P-GW and AAA is defined in the 3GPP network [3GPP TS23.401].

S6b reference point between MME and HSS is defined in the 3GPP network [3GPP TS23.401].

SWx reference point between HSS and AAA is defined in the 3GPP network [3GPP TS23.401].

STa reference point between WiMAX ASN and AAA is defined in the 3GPP network [3GPP TS23.402].

Gx reference point between P-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].

Gxa reference point between WiMAX ASN and PCRF is defined in the 3GPP network [3GPP TS23.402].

Gxc reference point between S-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].

R6 interface between the WiMAX SFF and ASN GW is defined in WiMAX Forum [WMF-T37-010-R016v01].

X200 interface between MN and 3GPP-SFF is defined in WiMAX Forum [WMF-T37-011-R016v01]..

X202 interface between MME and 3GPP-SFF is defined in WiMAX Forum [WMF-T37-011-R016v01].

* + 1. Transport of 3GPP L2 control frames between MN and the 3GPP network

Figure R.14 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-PoS/MME and the target 3GPP eNB all support single radio handover control function (SRCF), which is a media independent control function (MICF) in the 802-2010 architecture [IEEE P802-D1.2].

(a)



(b)



Figure R.14. Transport of 3GPP radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WiMAX link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/MME bridges between the MN and the target 3GPP eNB. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP). 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 single radio handover control (SRC) frames may be exchanged between the SRCF in the MN and the SRCF in the 3GPP-PoS/MME and/or the 3GPP eNB in the 3GPP network using TCP or UDP / IP transport.

The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame is encapsulated with a SRCF header to constitute a SRC frame, which is exchanged between the MN and the target 3GPP eNB or the co-located 3GPP-PoS/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.

It is required that the Information Repository need to know the IP address of the 3GPP-PoS/MME, so that the MN and the 3GPP-PoS/MME can exchange SRC 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 SRC frame to the SRCF 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 at least something, such as the link-layer address, to identify the target 3GPP eNB. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the collocated 3GPP-PoS/MME as described in Clause 11.4.3. The SRC frame contains information for the target 3GPP network to identify the target 3GPP eNB. The co-located 3GPP-PoS/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target 3GPP eNB.

The reply 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 through the MiCLSAP to become the payload of an SRC frame.

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

Figure R.15 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-PoS/MME support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? architecture. Yet the target 3GPP eNB are legacy 3GPP eNB’s lacking MICF support.

(a)



(b)



Figure R.15. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WiMAX link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/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. (a) shows the transport between MN and the co-located 3GPP-PoS/MME through using MiCLSAP and MICSAP. (b) show shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking MICF support in the 3GPP eNB, the co-located 3GPP-PoS/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 co-located 3GPP-PoS/MME may then proxy between the MN and the target 3GPP eNB using SRCF 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 co-located 3GPP-PoS/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function. Figure R.16 shows the transport of 3GPP L2 frames between the MN and legacy 3GPP network where the single radio handover control function (SRCF) is supported neither between the MN and the 3GPP-PoS/MME nor between the 3GPP-PoS/MME and the target 3GPP eNB.



Figure R.16. Packet used in the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WiMAX link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/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.

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

The co-located 3GPP-PoS/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.

* + 1. WiMAX to 3GPP Single Radio Handover processes

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 RFC6153. 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.

2: 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.

3: Pre-registration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the PoS, 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:

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-PoS/MME combination is through the source (WiMAX) network as described in Article 11.6.4.1.

The 3GPP-PoS/MME processes the SRC frame containing the L2 authentication message. The MME may consult the HSS in the 3GPP EPS network through the S6a reference point.

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 pre-registration 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.

The 3GPP-PoS/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-PoS/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 source PoA and target PoA within the same network to prepare the handover of a MN within the same network.

For messages from the 3GPP-PoS/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-PoS/MME acts like a virtual 3GPP radio interface.

The MN may pre-register with the 3GPP network, using the same interface and transport mechanism as that in proactive authentication.

4: 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 11.3.

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.

5: 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.

* + - 1. WLAN to 3GPP single radio handover

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:**

The Information repository function is implemented in the ANDSF in the 3GPP network.

The PoS function is implemented in the 3GPP-PoS and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-PoS 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 PoS as if signaling to a point of attachment (PoA), the target PoA may signal to the PoS which acts like a virtual MN. The PoS may also behave like a virtual PoA to signal with the target PoA.

Reference points:

S2c reference point between MN and the P-GW is defined in the 3GPP EPS network [3GPP TS23.402].

S2b reference point between ePDG and the P-GW is defined in the 3GPP EPS network [3GPP TS23.402].

S14 reference point between UE and ANDSF is defined in the 3GPP network [3GPP TS23.402].

S5/8 reference point between P-GW and S-GW is defined in the 3GPP network [3GPP TS23.401].

S11 reference point between S-GW and MME is defined in the 3GPP network [3GPP TS23.401].

S1-U reference point between UE and S-GW is defined in the 3GPP network [3GPP TS23.401].

S1-MME reference point between UE and MME is defined in the 3GPP network [3GPP TS23.401].

S6a reference point between P-GW and AAA is defined in the 3GPP network [3GPP TS23.401].

S6b reference point between MME and HSS is defined in the 3GPP network [3GPP TS23.401].

SWa reference point between the non-trusted WLAN AN and AAA is defined in the 3GPP network [3GPP TS23.402].

SWn reference point between the non-trusted WLAN AN and ePDG is defined in the 3GPP network [3GPP TS23.402].

SWm reference point between ePDG and P-GW is defined in the 3GPP network [3GPP TS23.402].

SWx reference point between HSS and AAA is defined in the 3GPP network [3GPP TS23.401].

Gx reference point between P-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].

Gxb reference point between ePDG and PCRF is defined in the 3GPP network [3GPP TS23.401].

Gxc reference point between S-GW and PCRF is defined in the 3GPP network [3GPP TS23.401].

RPmi interface between MN and 3GPP-PoS.

X202 interface between MME and 3GPP-PoS is defined in WiMAX Forum [WMF-T37-010-R016v01].

* + 1. Transport of 3GPP L2 control frames between MN and the 3GPP network

Figure R.18 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-PoS/MME and the target 3GPP eNB all support single radio handover control function (SRCF), which is a media independent control function (MICF) in the 802-2010 architecture [IEEE P802-D1.2].

(a)



(b)



Figure R.18. Transport of 3GPP radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WLAN link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/MME bridges between the MN and the target 3GPP eNB. (a) shows the transport through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

The SRCF interfaces with the TCP or UDP / IP layer through the Media Independent Control Service Access Point (MICSAP). 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 single radio handover control (SRC) frames may be exchanged between the SRCF in the MN and the SRCF in the 3GPP-PoS/MME and/or the 3GPP eNB in the 3GPP network using TCP or UDP / IP transport.

The SRCF also interfaces with the link-layer (L2) through the media independent control link-layer service access point (MiCLSAP). An L2 frame is encapsulated with a SRCF header to constitute a SRC frame, which is exchanged between the MN and the target 3GPP eNB or the co-located 3GPP-PoS/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.

It is required that the Information Repository need to know the IP address of the 3GPP-PoS/MME, so that the MN and the 3GPP-PoS/MME can exchange SRC 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 SRC frame to the SRCF 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 at least something, such as the link-layer address, to identify the target 3GPP eNB. The SRC frame is first sent as the payload of an TCP or UDP / IP packet destined to the collocated 3GPP-PoS/MME as described in Clause 11.4.3. The SRC frame contains information for the target 3GPP network to identify the target 3GPP eNB. The co-located 3GPP-PoS/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of an TCP or UDP / IP packet containing the SRC frame as payload to forward to the target 3GPP eNB.

The reply 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 through the MiCLSAP to become the payload of an SRC frame.

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

Figure R.19 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-PoS/MME support single radio handover control function (SRCF), which is a media independent control function (MICF) in the IEEE 802-2012?? architecture. Yet the target 3GPP eNB are legacy 3GPP eNB’s lacking MICF support.

(a)



(b)



Figure R.19. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WLAN link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/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. (a) shows the transport between MN and the co-located 3GPP-PoS/MME through using MiCLSAP and MICSAP. (b) shows the resulting packets with cross-layer encapsulation after passing through these two SAP’s.

Lacking MICF support in the 3GPP eNB, the co-located 3GPP-PoS/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 co-located 3GPP-PoS/MME may then proxy between the MN and the target 3GPP eNB using SRCF 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 co-located 3GPP-PoS/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function. Figure R.20 shows the transport of 3GPP L2 frames between the MN and legacy 3GPP network where the single radio handover control function (SRCF) is supported neither between the MN and the 3GPP-PoS/MME nor between the 3GPP-PoS/MME and the target 3GPP eNB.



Figure R.20. Packet used in the transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the 3GPP network via the source WLAN link at the left and in the absence of the target 3GPP link at the right. The co-located 3GPP-PoS/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.

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

The co-located 3GPP-PoS/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.

* + 1. Non-trusted WLAN AN to 3GPP Single Radio Handover processes

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 RFC6153. 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.

2: 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.

3: Pre-registration includes proactive authentication and establishing context (user identity, security, resource information) at the target network. With the help of the PoS, 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:

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 source (WLAN) network as described in Article 11.6.5.1.

The 3GPP-PoS/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.

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 pre-registration 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.

The 3GPP-PoS/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-PoS/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 source PoA and target PoA within the same network to prepare the handover of a MN within the same network.

For messages from the 3GPP-PoS/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-PoS/MME acts like a virtual 3GPP radio interface.

The MN may pre-register with the 3GPP network, using the same interface and transport mechanism as that in proactive authentication.

4: 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 11.3.

The 3GPP will check with the target eNB and target 3GPP-PoS/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.

5: 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.

1. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-3)
2. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-4)
3. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-5)
4. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-6)
5. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-7)
6. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-8)
7. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-9)
8. Note to the editor, this footnote should not appear in the final version. MIRK stands for MN´s media independent root key. [↑](#footnote-ref-10)
9. Note to editor, this footnote should not appear in the final version. MSPMK stands for MN´s media specific root key. [↑](#footnote-ref-11)