|  |  |
| --- | --- |
| 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\_Anthony\_Chan** |
| Date Submitted | September 19, 2011 |
| Source(s) | H Anthony Chan (Huawei), Junghoon Jee (ETRI), Changmin Park (ETRI), and Yoon Young An (ETRI), Dapeng Liu, Charles E. Perkins (Tellabs) |
| Re: | IEEE 802.21c draft |
| Abstract | This document specifies the specification of IEEE 802.21c Single Radio Handover Optimization. |
| 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—**

**Part 21: Media Independent Handover Services**

**Amendment: Optimized Single Radio Handovers**

**Abstract:** This document specifies the single radio handover optimizations to reduce the latency during 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

Control Plane Gateway: A gateway in the control plane to bridge the signaling between the MN and the target network via the source network. To the MN, it acts like a virtual point of attachment (POA) to the target network. It enables such functions as pre-registration and proactive authentication of the MN.

Single radio handover: A handover among different 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

C-GW Control Plane Gateway

SFF Signal Forwarding Function

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 Signal Forwarding Function (SFF) information and the capability for supporting SRHO for each of the available access networks. The SFF information includes SFF 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 |
| **Signal Forwarding Function information elements** | | |
| IE\_SFF\_IP\_ADDR | IP address of SFF | IP\_ADDR |
| IE\_SFF\_TUNN\_MGMT\_PRTO | Type of tunnel management protocol supported. | IP\_TUNN\_MGMT |
| IE\_SFF\_FQDN | FQDN of SFF. | 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\_SFF, is defined for SRHO.

1. **IE\_CONTAINER\_SFF** – contains all the information depicting a SFF as shown in Table 2.

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

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

# Service access point (SAP) and primitives

# Media independent handover protocols

# 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 may 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 for the mobile device.

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

### Relationship to other network standards

Network standards organizations such as WiMAX Forum and 3GPP had both been looking into single radio handover from/to their network. With different 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 in 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 a horizontal handover. While the source and target networks are of the same type of network technology, it is possible that the source and target points of attachment may belong to the same or different access networks, and different access networks may 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 to perform handover.

A multiple-interface device connecting with one interface to a network may change the connection with another 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.

Another requirement with the dual-radio handover is 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 such as when time division duplex is used, there is no interference between the transmitter signal and the receiver signal. If the receiver is receiving signal such as when frequency division duplex is used, the frequency bands for transmission for reception in the same network technology will avoid being 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. A sharper signal filter is therefore needed to avoid interference when one radio is transmitting while another radio is receiving.

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 here. New functions and therefore new functional requirements (Clause 9.2) 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 9.5 and 9.6) whereas the network provides the needed network support with the different network configuration (Clause 9.3) 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 independency 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. These signaling messages are media independent messages. The single radio handover using these media independent messages is a media independent single radio handover. Therefore, a media independent handover may be accomplished in a media independent way, keeping in mind that 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 9.2.

## Requirements of Single Radio Handover

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

General Requirements;

* The defined mechanism shall be general so that it can be applied to the single radio mobile station whether it activates the dual receivers for both access networks or only single receiver for the current access network.
* The defined mechanisms shall be general enough so that they can 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 define the way to deliver radio measurement configuration and report information within a media-independent container for single radio mobile station.
* The mechanism shall define the 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 appropriate target network and the corresponding required information from the access network.
* The following capability shall be communicated between mobile station and single radio enabling entity at the network.

Supported RATs accesses 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 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 network, the communication, or (c) belong to different access networks connecting to different networks. In (a) and (b), the capability to communicate between the source radio and the target network usually does not need new internetwork interfaces. In (c), the two networks should be able to communicate with each other.

## SRHO Reference Model

The reference model for single radio handover networks from a source network to a target network is shown in Figure 9.1. 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 9.1. Reference model for single radio handover from a source network to a target network.

Link configuration before handover:

1. Between 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 signal.
2. Between MN and target network: Not specified.

Link configuration after handover:

1. Between MN and source network: Not specified.
2. Between 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 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 function in MN and in the source network may use this source link to transport control plane messages.

1. Between MN and target network: The link between MN and the target network is virtual and communication may happen subject to meeting the constraints given in the assumptions Clause.

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

The Information Repository may reside in the source network or the target network, and is accessible from both networks. It contains network information needed to make handover decision, such as the availability of candidate target network etc. In particular, a media independent information server (IS) is used for information expressed in media independent format. The Information Repository may also be implemented in such a network information repository as part of the Access Network Discovery and Selection Function (ANDSF) defined in 3GPP standard [3GPP TS23.402].

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.

### Control Plane Gateway

The Control Plane Gateway (C-GW) bridges the control plane signaling between the MN and the target network via the source network. When the MN signals to the C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW may also behave like a virtual POA to signal with the target POA. The control frames from the MN tunneled via the source network to the target network are consumed at the C-GW, which processes these control frames. Before replying to the control frames, the C-GW 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 gateway to the target network, and its single radio handover functions may be implemented using the media independent point of service (POS), which are defined in this Clause.

The C-GW 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 C-GW functions may be implemented in the Signal Forwarding Function (SFF) and the existing functions of ASN-GW.

In a target 3GPP network, the C-GW functions may be implemented in the 3GPP-SFF and the existing functions of Mobility Management Entity (MME).

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

A control signal between the MN and the C-GW 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 not defined here is to be used, it can be encapsulated with a media independent control frame header.

### Single Radio handover Control Function

To prepare for handover, the target radio exchanges link-layer network entry PDU’s with the target POA at the target network. These network entry PDU’s can be the same PDU’s 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 PDU’s without depending on the existence of the target radio’s physical channel but with the help of the active source radio.

Figure 9.2 shows the Single Radio handover Control Function (SRCF) in a multiple interface node. The SRCF is a media independent control function (MICF) in the control plane, which is defined in the 802-2010 architecture [IEEE P802-D1.2].



Figure 9.2. Single Radio handover Control Function (SRCF) of a multiple interface mobile node as a Media Independent Control Function (MICF) in the media independent control plane.

The SRCF interfaces with the IP/UDP layer through the Media Independent Control Service Access Point (MICSAP), and the SRCF has 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 IP/UDP connection between these two nodes. The SRC frames are processed by the SRCF in the destination of the IP/UDP 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 IP/UDP connection between the two nodes.

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

The transport of L2 network entry PDU’s of the target radio between the MN and the C-GW in the target network is enabled by the MiCLSAP to the SRCF and the communication between the SRCF in the MN and the SRCF in the C-GW as shown in Figure 9.3.

(a)



(b)



Figure 9.3. Transport of L2 frame of target interface using the communication between the SRCF in the MN and the SRCF in the C-GW. (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 target radio and the target network during a single radio handover, a L2 network entry PDU of the target radio uses the 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 IP/UDP packets to/from the source access network, which has IP connection to the target network through the Internet. There is therefore IP/UDP transport between the source radio and the C-GW of the target network via the source interface. Building on the IP/UDP layer through the MICSAP, the SRCF at the MN may therefore communicate with the SRCF at the C-GW.

### 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 IP/UDP packets to the C-GW, and the MN may query the Information Repository to find the IP address of the C-GW in order to use this IP/UDP 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 9.4.

(a)



(b)



Figure 9.4. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the C-GW via the source radio interface, in the absence of the target link. The C-GW 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, such as by querying the Information Repository.

If MN knows the IP address of the target POA, there is then communication between the SRCF in the MN and the SRCF in the target POA using IP/UDP transport, so that the SRC frames are exchanged between them.

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 IP/UDP packet destined to the C-GW as described in Clause 9.4.3. The SRC frame contains information for the target network to identify the target PoA. The C-GW will find out the IP address of the target PoA and use this address as the destination address of an IP/UDP packet containing the SRC frame as payload to forward to the target PoA. In other words, the C-GW functions 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 IP/UDP transport with an IP address destined to the MN. Yet if the target POA had received the SRC frame from the C-GW, the reply SRC frame will first use IP/UDP transport with an IP address destined to the C-GW. At the C-GW, the IP/UDP header is extracted at the MICSAP at the input interface of the C-GW to retrieve the SRC frame. The SRCF function will pass the SRC frame through the MICSAP at the output interface of the C-GW to form a new IP/UDP packet with an IP address destined to the MN.

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

Figure 9.5 shows the transport of target radio L2 frames between the MN and the target network when the MN, the C-GW 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 C-GW 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 C-GW 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 C-GW may map the message contents exchanged with the MN with that exchanged with the target POA in performing the proxy function.

(a)



(b)



Figure 9.5. Transport of the target radio L2 control frame as a payload of a media independent control frame between the MN and the C-GW via the source radio interface (if1), in the absence the target link. The C-GW 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 9.8) and messages (Clause 9.9). This Clause describes overall procedures of single radio handover, and examples of handover are described in Clause 9.6. Figure 9.6 shows the single radio handover procedures consisting of 5 processes.



**Figure 9.6** – Overall Single Radio Handover Procedures

1: Network discovery process is to ascertain whether there is a candidate target network available to handover to? In network discovery, the MN queries the Information Repository to discover candidate networks. Information Repository provides the MN with information about available networks and handover policy. Such information includes whether candidate networks and MN support SRHO or not, and the presence of C-GW on the candidate network. Network discovery also allows the MN to acquire the corresponding system information blocks of candidate PoAs to perform the radio measurements.

2. Handover Decision process may involve the following

(1) The handover may be triggered by a need.

(2) A target network is selected and the control plane gateway to that network is discovered.

(3) A determination is made on whether there is benefit to handover? The decision can be taken by the MN or the network. An example of making such a decision is to be based on the parameters such as signal strength, cost, and operator policy. In order to find out whether the target radio is of better signal strength, the MN may use the target interface to listen to the broadcast channels from the target POA in the target network subjecting to the single radio handover assumptions in Clause 9.3.

3: Pre-registration process includes pro-active authentication and establishing context (user identity, security, resource information) at the target network. With the help of C-GW, the MN can perform network entry procedures towards the target network while 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 process. Here, the MN and target network prepare the establishment of the target link. This process ensures whether the target network has enough resources to accommodate the new link and may include performing resource reservation or admission control. It also confirms the signal conditions are favorable enough to establish the target link. In addition, the target radio may perform limited signaling if it can do it 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.

## Examples of SRHO

### WLAN to WiMAX single radio handover

The general reference model as it applies to WLAN to WiMAX single radio handover is illustrated in Figure 9.7.



Figure 9.7 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 but may also be other information repository defined elsewhere, such as the ANDSF.

The C-GW function is implemented in the combined functions of ASN-GW and WiMAX SFF, which are defined in the WiMAX network. When the MN signals to the C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW 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 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 SFF and ASN GW is defined in WiMAX Forum [T33-001-R015].

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

Figure 9.8 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located SFF/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 9.8. 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 SFF/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 IP/UDP layer through the Media Independent Control Service Access Point (MICSAP). The source WLAN link enables the IP/UDP 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 SFF/ASN-GW and/or the WiMAX BS in the WiMAX network using IP/UDP 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 SFF/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 SFF/ASN-GW, so that the MN and the SFF/ASN-GW can exchange SRC frames using IP/UDP 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 IP/UDP 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 IP/UDP packet destined to the collocated SFF/ASN-GW as described in Clause 9.4.3. The SRC frame contains information for the target WiMAX network to identify the target WiMAX BS. The co-located SFF/ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of an IP/UDP 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 IP/UDP transport with an IP address destined to the MN. Yet if the target WiMAX BS had received the SRC frame from the co-located SFF/ASN-GW, the reply SRC frame will first use IP/UDP transport with an IP address destined to the C-GW. At the co-located SFF/ASN-GW, the IP/UDP header is extracted at the MICSAP at the input interface of the co-located SFF/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 SFF/ASN-GW to form a new IP/UDP packet with an IP address destined to the MN.

Figure 9.9 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located SFF/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 9.9. 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 SFF/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 SFF/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 SFF/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 SFF/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 SFF/ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function. Figure 9.10 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 SFF/ASN-GW nor between the SFF/ASN-GW and the target WiMAX BS.



Figure 9.10. 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 SFF/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 SFF/ASN-GW will need certain mechanism to communicate with each other, such as an extension (Rx+) of the Rx interface. The SFF/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 SFF/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.

#### 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 C-GW, 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 SFF/ASN-GW is through the source (WiFi) network as described in Article 9.6.1.1.

b)

The ASN-GW/SFF 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 SFF/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 SFF/ASN-GW already has this registration context.

The ASN-GW/SFF combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/SFF 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/SFF to the MN, they are tunneled to the MN via the WiFi network. To the target WiMAX BS, the ASN-GW/SFF 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 9.3.

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.

### 3GPP to WiMAX single radio handover

The general reference model as it applies to 3GPP to WiMAX single radio handover is illustrated in Figure 9.11.



Figure 9.11 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 C-GW function is implemented in the combined functions of ASN-GW and WiMAX SFF, which are defined in the WiMAX network. When the MN signals to the C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW 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 SFF is defined in WiMAX Forum [WMF-T37-011-R016v01].

R6 interface between the WiMAX SFF 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].

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

Figure 9.12 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located SFF/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 9.12. 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 SFF/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 IP/UDP layer through the Media Independent Control Service Access Point (MICSAP). The source 3GPP link enables the IP/UDP 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 SFF/ASN-GW and/or the WiMAX BS in the WiMAX network using IP/UDP 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 SFF/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 SFF/ASN-GW, so that the MN and the SFF/ASN-GW can exchange SRC frames using IP/UDP 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 IP/UDP 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 IP/UDP packet destined to the collocated SFF/ASN-GW as described in Clause 9.4.3. The SRC frame contains information for the target WiMAX network to identify the target WiMAX BS. The co-located SFF/ASN-GW will find out the IP address of the target WiMAX BS and use this address as the destination address of an IP/UDP 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 IP/UDP transport with an IP address destined to the MN. Yet if the target WiMAX BS had received the SRC frame from the co-located SFF/ASN-GW, the reply SRC frame will first use IP/UDP transport with an IP address destined to the SFF/ASN-GW. At the co-located SFF/ASN-GW, the IP/UDP header is extracted at the MICSAP at the input interface of the co-located SFF/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 SFF/ASN-GW to form a new IP/UDP packet with an IP address destined to the MN.

Figure 9.13 shows the transport of WiMAX L2 frames between the MN and the WiMAX ASN when the MN, the co-located SFF/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 9.13. 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 SFF/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 SFF/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 SFF/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 SFF/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 SFF/ASN-GW may map the message contents exchanged with the MN with that exchanged with the target WiMAX BS in performing proxy function. Figure 9.14 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 SFF/ASN-GW nor between the SFF/ASN-GW and the target WiMAX BS.



Figure 9.14. 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 SFF/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 SFF/ASN-GW will need certain mechanism to communicate with each other, such as an extension (R9+) of the R9 interface. The SFF/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 SFF/ASN-GW may then proxy between the MN and the target WiMAX BS using the R9+ to communicate with MN and using the R6+ to communicate with the target WiMAX BS.

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

#### 3GPP to WiMAX Single Radio Handover processes

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 SFF, 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 C-GW, 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 SFF/ASN-GW is through the source (3GPP) network as described in Article 9.6.2.1.The ASN-GW/SFF 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 SFF/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 SFF/ASN-GW already has this registration context.

The ASN-GW/SFF combination also constructs control messages to communicate with the target WiMAX BS. In terms of exchange of these control messages, the ASN-GW/SFF 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/SFF to the MN, they are tunneled to the MN via the 3GPP network. To the target WiMAX BS, the ASN-GW/SFF 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

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 9.3.

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.

### WiMAX to WLAN single radio handover

The general reference model as it applies to WiMAX to WLAN single radio handover is illustrated in Figure 9.15.



Figure 9.15 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 C-GW function is implemented in the combined functions of WiFi Interworking Function (WIF) and WiFi SFF, which are defined in the WiMAX network. When the MN signals to the C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW 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-SFF 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].

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

Figure 9.16 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the co-located SFF/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 9.16. 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 SFF/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 IP/UDP layer through the Media Independent Control Service Access Point (MICSAP). The source WiMAX link enables the IP/UDP 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 SFF/WIF/AR and/or the WLAN AP in the WLAN network using IP/UDP 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 SFF/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 SFF/WIF/AR, so that the MN and the SFF/WIF/AR can exchange SRC frames using IP/UDP 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 IP/UDP 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 IP/UDP packet destined to the collocated SFF/WIF/AR as described in Clause 9.4.3. The SRC frame contains information for the target WLAN network to identify the target WLAN AP. The co-located SFF/WIF/AR will find out the IP address of the target WLAN AP and use this address as the destination address of an IP/UDP 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 IP/UDP transport with an IP address destined to the MN. Yet if the target WLAN AP had received the SRC frame from the co-located SFF/WIF/AR, the reply SRC frame will first use IP/UDP transport with an IP address destined to the SFF/WIF/AR. At the co-located SFF/WIF/AR, the IP/UDP header is extracted at the MICSAP at the input interface of the co-located SFF/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 SFF/WIF/AR to form a new IP/UDP packet with an IP address destined to the MN.

Figure 9.17 shows the transport of WLAN L2 frames between the MN and the WLAN AN when the MN, the co-located SFF/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 9.17. 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 SFF/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 SFF/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 SFF/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 SFF/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 SFF/WIF/AR may map the message contents exchanged with the MN with that exchanged with the target WLAN AP in performing proxy function. Figure 9.18 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 SFF/WIF/AR nor between the SFF/WIF/AR and the target WLAN AP.



Figure 9.18. 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 SFF/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 SFF/WIF/AR will need certain mechanism to communicate with each other, such as an extension (Ry+) of the Ry interface. The SFF/WIF/AR and the target WLAN AP will also need certain mechanism to communicate with each other.

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

Ry+ is outside the scope of this standard.

#### WiMAX to WLAN Single Radio Handover processes

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 C-GW, 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 9.6.3.1.

(a)

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

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

The C-GW (WIF/AR/WiFi-SFF combination) also constructs control messages to communicate with the target WLAN AP. In terms of exchange of these control messages, the WIF/AR/WiFi-SFF 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-SFF to the MN, they are tunneled to the MN via the WiMAX network. To the target WiFi AP, the WIF/AR/WiFi-SFF 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.

### WiMAX to 3GPP single radio handover

The general reference model as it applies to WiMAX to 3GPP single radio handover is illustrated in Figure 9.19.



Figure 9.19 WiMax to 3GPP single radio handover reference model.

**Functional entities:**

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

The C-GW function is implemented in the 3GPP-SFF and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-SFF 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 C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW 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].

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

Figure 9.20 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-SFF/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 9.20. 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-SFF/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 IP/UDP layer through the Media Independent Control Service Access Point (MICSAP). The source WiMAX link enables the IP/UDP 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-SFF/MME and/or the 3GPP eNB in the 3GPP network using IP/UDP 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-SFF/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-SFF/MME, so that the MN and the 3GPP-SFF/MME can exchange SRC frames using IP/UDP 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 IP/UDP 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 IP/UDP packet destined to the collocated 3GPP-SFF/MME as described in Clause 9.4.3. The SRC frame contains information for the target 3GPP network to identify the target 3GPP eNB. The co-located 3GPP-SFF/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of an IP/UDP 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 IP/UDP 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-SFF/MME, the reply SRC frame will first use IP/UDP transport with an IP address destined to the 3GPP-SFF/MME. At the co-located 3GPP-SFF/MME, the IP/UDP header is extracted at the MICSAP at the input interface of the co-located 3GPP-SFF/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-SFF/MME to form a new IP/UDP packet with an IP address destined to the MN.

Figure 9.21 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-SFF/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 9.21. 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-SFF/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-SFF/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-SFF/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-SFF/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-SFF/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function. Figure 9.22 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-SFF/MME nor between the 3GPP-SFF/MME and the target 3GPP eNB.



Figure 9.22. 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-SFF/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-SFF/MME will need certain mechanism to communicate with each other, such as an extension (X200+) of the X200 interface. The 3GPP-SFF/MME and the target 3GPP eNB will also need certain mechanism to communicate with each other.

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

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

#### WiMAX to 3GPP Single Radio Handover processes

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 C-GW, 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-SFF/MME combination is through the source (WiMAX) network as described in Article 9.6.4.1.

The 3GPP-SFF/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-SFF/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-SFF/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-SFF/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-SFF/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 9.3.

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.

### 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 9.23.



Figure 9.23 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 C-GW function is implemented in the 3GPP-SFF and the existing functions of Mobility Management Entity (MME) in the 3GPP EPS network. The 3GPP-SFF 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 C-GW as if signaling to a point of attachment (POA), the target POA may signal to the C-GW which acts like a virtual MN. The C-GW 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-SFF.

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

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

Figure 9.24 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-SFF/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 9.24. 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-SFF/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 IP/UDP layer through the Media Independent Control Service Access Point (MICSAP). The source WLAN link enables the IP/UDP 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-SFF/MME and/or the 3GPP eNB in the 3GPP network using IP/UDP 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-SFF/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-SFF/MME, so that the MN and the 3GPP-SFF/MME can exchange SRC frames using IP/UDP 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 IP/UDP 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 IP/UDP packet destined to the collocated 3GPP-SFF/MME as described in Clause 9.4.3. The SRC frame contains information for the target 3GPP network to identify the target 3GPP eNB. The co-located 3GPP-SFF/MME will find out the IP address of the target 3GPP eNB and use this address as the destination address of an IP/UDP 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 IP/UDP 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-SFF/MME, the reply SRC frame will first use IP/UDP transport with an IP address destined to the 3GPP-SFF/MME. At the co-located 3GPP-SFF/MME, the IP/UDP header is extracted at the MICSAP at the input interface of the co-located 3GPP-SFF/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-SFF/MME to form a new IP/UDP packet with an IP address destined to the MN.

Figure 9.25 shows the transport of 3GPP L2 frames between the MN and the 3GPP network when the MN, the co-located 3GPP-SFF/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 9.25. 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-SFF/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-SFF/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-SFF/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-SFF/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-SFF/MME may map the message contents exchanged with the MN with that exchanged with the target 3GPP eNB in performing proxy function. Figure 9.26 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-SFF/MME nor between the 3GPP-SFF/MME and the target 3GPP eNB.



Figure 9.26. 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-SFF/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-SFF/MME will need certain mechanism to communicate with each other, such as an extension (RPmi+) of the RPmi interface. The 3GPP-SFF/MME and the target 3GPP eNB will also need certain mechanism to communicate with each other.

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

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

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

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 C-GW, 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 9.6.5.1.

The 3GPP-SFF/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-SFF/MME combination also constructs control messages to communicate with the target 3GPP eNB. In terms of exchange of these control messages, the 3GPP-SFF/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-SFF/MME to the MN, they are tunneled to the MN via the WiMAX network. To the target 3GPP eNB, the 3GPP-SFF/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 9.3.

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

## Securing Single-Radio messages using SFF

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. Using the SFF along with some signaling to transmit security information between roaming partners enables a low-latency, optimized single-radio handover 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 SFF 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 SFFs in partner networks. It is expected that in many cases the SFFs 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 SFFs. It is out of scope for this document to specify exactly how the partner SFFs 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 1: MN handover signaling for preregistration using OSFF FIX THIS BAD DIAGRAM.

Except for the initial network attach, by the time a MN enters a network, it also has a security relationship with the SFF in that network. For a visited network, this security relationship is created on demand, enabled by signaling from another SFF. The SFF creating the visited security relationship can either be the MN's home SFF (HSFF, a SFF in MN's home network), or the SFF 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 HSFF; 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 SFF in the network at its current point of attachment (PoA); the current network is termed the "originating" network, and the SFF in the originating network is abbreviated as the OSFF. 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 SFF in the target network (i.e., the "TSFF"). When handover is completed, the TSFF naturally becomes the local SFF (OSFF).

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 SFF 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 is naturally dependent on the requirements of the target network, and typically quite independent of the nature of the network (as above, the "originating 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; thus preregistration signaling could be exposed to attack.

In order to enable wider application of high-performance handovers and in particular preregistration signaling, we need to provide a guarantee of security for the control traffic. From above, we see that this signaling traffic is mediated by the SFF 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 SFF. The process of establishing such a security association is, in general, 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 SFF in any target network within the networks covered by the roaming partners.

### Key distribution for SFF-based handover

The following terminology and abbreviations will be used for keys and key distribution functions:

Table 1: Terminology for SFF Key Distribution

|  |  |
| --- | --- |
| *K\_hsff* | key between MN and HSFF |
| *K\_osff* | key between MN and OSFF |
| *K\_tsff* | key between MN and TSFF |
| *K\_hosff* | key between HSFF and OSFF |
| *K\_htsff* | key between HSFF and TSFF |
| *K\_otsff* | key between OSFF and TSFF |
| *KDF\_hosff* | key distribution function between HSFF and OSFF |
| *KDF\_otsff* | key distribution function between OSFF and TSFF |

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 SFF (HSFF), based on a key *K\_hsff*. Because of previous protocol operations, the MN has a current security association with the SFF in the originating network (OSFF).

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 SFF in target network (TSFF). Before it can do this, it needs to discover the address of TSFF and establish a security association with TSFF using *K\_tsff*.

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

To send *K\_tsff* to TSFF, OSFF provides the following payload as part of an appropriate extension payload:

Payload\_tsff = MNaddr, RAND, [*K\_tsff* ⊕ *KDF\_otsff* (MNaddr, RAND)]

To send *K\_tsff* to MN, OSFF provides the following payload as part of payload in a new 802.21(c) message:

Payload\_mn = TSFFaddr, RAND, [*K\_tsff* ⊕ *KDF\_osff* (TSFFaddr, RAND)]

Upon TSFF receiving Payload\_tsff, TSFF calculates *KDF\_otsff* (MNaddr, RAND) and XORs the result to the third parameter of Payload\_tsff to recover *K\_tsff*. Similarly, upon receiving Payload\_mn, MN calculates *KDF\_osff* (TSFFaddr, RAND) and applies that to the third parameter of Payload\_mn to recover *K\_tsff*.

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

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

It is possible for OSFF to take a more active role to promote smooth handover. When the MN determines the need for handover, but does not already know the address of the TSFF for the intended target network, the MN can start the preregistration sequence by sending all the known information to the OSFF. Subsequently, the OSFF will provide the address of the TSFF to the MN along with *K\_tsff*, just as described above. The exact nature of the information about TSFF 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 Information Repository software, detailed information about TSFF, and the other entities within the target network can be easily be made available. Note, however, that discovery and secure communication with Information Repository may not be any easier than discovery and secure communication with TSFF.

### SFF-based Key Distribution -- Integration with Mobile IP

When the MN makes its initial attachment to a network other than its home network, as mentioned above, it can use its HSFF to bootstrap a security association with the SFF in the visited network. For this case, which is will not be uncommon, the HSFF can be beneficially integrated with the MN’s home agent. Then, the home agent can include the desired key material as part of the Mobile IP registration signaling. For IPv6, this would be the MIPv6 Binding Update and Binding Acknowledgement exchange [RFC 6275]. There are multiple advantages of this approach. One is that the MN does not have to manage yet another security association with yet another trusted agent in its home network. Another is that the MN, when it receives the Binding Acknowledgement, will already be assured of IPv6 address continuity in the visited network.

Furthermore, in the frequent case when the MN returns to its home network, it will always have the proper security association with HSFF being utilized as TSFF when the home network is the same as the target network.

See [http://tools.ietf.org/id/draft-perkins-mext-sffexts-01.txt] for further details.

**Annex A**

(normative)

**Data type definition**

**A.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 | Represents an IP address. The Address Type is either 1  (IPv4) or 2 (IPv6). |
| IP\_TUNN\_MGT | BITMAP(16) | Indicates the supported tunnel management protocol on SFF.  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. |

**Annex B**

(normative)

# Information element identifiers

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

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