WiFi - WiMAX Interworking

WORK IN PROGRESS DRAFT

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.

The WiMAX Forum™ owns the copyright in this document and reserves all rights therein. Use of this document and any related materials is limited as follows:

A. ***WiMAX Forum members MAY*** use this document for the sole purpose of participating in approved WiMAX Forum activities, including the activities of the Working Group that has produced it.

B. ***Participants in the standards development activities of other organizations*** MAY use this document for reference purposes, namely (i) to review and evaluate the WiMAX Forum's use and implementation of third-party standards in its technical documents, and (ii) to review, evaluate and, in their sole discretion, adapt their standards activities in a manner that encourages, promotes and/or implements enhanced compatibility and/or interoperability between their respective standards and the standards that the WiMAX Forum is promoting.

A user of this document MAY duplicate and distribute copies of the document in connection with the authorized uses described above. Any duplication in whole or in part will include the copyright notice on the first page of this document and all notices and restrictions contained in this Section of the document ("Copyright Notice, Use Restrictions, Disclaimers and Limitation of Liability"). Except for the foregoing or as expressly authorized by the WiMAX Forum in writing, any other use of this document and all other duplication and distribution of this document are prohibited. The WiMAX Forum regards the unauthorized use, duplication or distribution of this document by a member as a material breach of the member's obligations under the organization's rules and regulations, which MAY result in the suspension or termination of its WiMAX Forum membership. Unauthorized use, duplication, or distribution by nonmembers is an infringement of the WiMAX Forum's copyright. Distribution of this document to persons or organizations that are not involved in the standards development process or who are not WiMAX Forum members is prohibited.

Use of this document is subject to the additional disclaimers and limitations described below. By using this document, the user agrees to the following terms and conditions:

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.

The user acknowledges that any products or services provided using technology described in or implemented in connection with this document MAY be subject to various regulatory controls under the laws and regulations of various governments worldwide. The user acknowledges that it is solely responsible for the compliance of its products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products as a result of such regulations within the applicable jurisdiction.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.

The user acknowledges that the WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that MAY be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein MAY therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user acknowledges that it is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, technologies, standards, and specifications, including through the payment of any required license fees.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO ANY OTHER MEMBER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion.

"WiMAX," "WiMAX Forum," "WiMAX Certified," and "WiMAX Forum Certified" are trademarks of the WiMAX Forum. Third-party trademarks contained in this document are the property of their respective owners.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Revision History

March 09, 2009	Initial skeleton draft:
March 16, 2009	Harmonized draft between ZTE and Intel
March 17, 2009	Approved initial baseline after some more comments at F2F
June 23, 2009	Incorporated WiFi_WiMAX_IWK_NRM-Updates.doc 44455_r2 WiFi_WiMAX_Network_Entry-Updates.doc 44456_r2 WiFi_WiMAX_Dual_Radio_HOs-Updates.doc 44457_r2
July 27, 2009	WiFi_WiMAX_Dual_Radio_HOs-Updates(ZTE).doc 44955 r2
Aug 18, 2009	WiFi_WiMAX_Network_Entry-harmonized(ZTE).doc 45967 r2 Editorial Updates
Sep 04, 2009	NWG_Network_Discovery_Selection.doc 46348 r1 NWG_WiFi_WiMAX_IWK_r3_Accounting.doc 46224 r3 NWG_WiFi-to-WiMAX_Single_Radio_HO.doc 46616 r3 NWG_WiMAX_to_WiFi_Single_Radio_HO.doc 46617 r1 Deleted: [Editor's note]: This step needs further study due to the WiMAX MSK being killed.
Oct 24, 2009	NWG_WiMAX_Wifi_IWK_Network_Discovry_Selection_MinorUpdate.doc 47069r0 NWG_WiFi_to_WiMAX_SR_Minor_Update.doc 47068 r0 NWG_WiFi_WiMAX_IWK_SR_Accounting.doc 47549 r1 (TBD Make figures 11-3,11-4,11-5 consistent)
Nov 28, 2009	NWG_WiMAX_to_WiFi_SR_update-r4.doc 48281r4 NWG_Network_Discovery_Selection- r002.doc 48285r1 NWG_Wifi-WiMAX_IWK_Network_Exit-Updated-huawei.doc 48958r0 Baseline_with_added_security_authentication_sections_v3.doc 48758r2
Dec 17, 2009	NWG_WiFi_WiMAX_IWK_Section_8_v4.doc 49891r1 NWG_Wifi-WiMAX_IWK_WIF_Selection_HW-r1.doc 49893r1 NWG_WiFi_WiMAX_Roaming-r1.doc 49895r1

2. Introduction and Document Scope

This document specifies the specification for interworking and/or roaming between WiFi and Mobile WiMAX. The specification will include a network reference model for interworking and/or roaming between WiFi and WiMAX

networks. The purpose of this document is to identify the requirements and impacts to the WiFi access network and the WiMAX network to support the interworking and/or roaming functionality.

3. Abbreviations and Definitions

3.1 Abbreviations

For the purposes of the present document, following abbreviations apply:

AN	Access Network
DM	Dual Mode
IWK	Inteworking
WiFi	Wireless Fidelity
WIF	WiFi Interworking Function
WiMAX SFF	WiMAX Signal Forwarding Function
WiFi SFF	WiFi Signal Forwarding Function
WBA	Wireless Broadband Alliance
WRIX	Wireless Roaming Intermediary eXchange
WISPr	Wireless ISP roaming

3.2 Terms & Definitions

Single Radio Handover: A Dual Mode terminal where *only a single radio is* transmitting "on" at any given time during the handover process. During the handover process one or two receivers may be active.

Dual Radio Handover: A Dual Mode terminal where *both* the radios can be transmitting and receiving simultaneously at any given time.

WiFi-WiMAX Roaming: The ability for a WiFi or WiMAX subscriber to function in a visited WiFi or WiMAX network different from the home network.

4. References

[1] WiMAX Forum™ Network Architecture Release 1.3, Nov, 2008.

[2] WiMAX Forum™ Mobile System Profile Release 1.0 (Revision 1.4.0), May 2, 2007.

[3] 3GPP TS 23.234: "3GPP system to WLAN interworking; System description (Release 7)"

[4] WiMAX Forum™ Network Architecture Release 1.5 PMIPv6 Stage 3 Specification

[5] Wireless Broadband Alliance WRIX Standard Service Specification, Umbrella Doc v1.03

[6] Wireless Broadband Alliance WRIX Standard Service Specification, Interconnect Definition v1.04

[7] Wireless Broadband Alliance WISPr 2.0, draft version 0.3

5. General Requirements and Principles

This section defines thehigh level assumptions, architectural principles and requirements for interwoking between WiFi and WiMAX.

5.1 Usage Scenarios

5.2 Assumptions

5.3 Requirements

5.3.1 Requirements for interworking between WiFi and WiMAX

- Common Billing for accessing WiFi and WiMAX networks shall be supported. WiFi and WiMAX may use different credentials but the user may be provided with a consolidated bill.
- WiMAX system based access control and charging mechanism shall be supported.
- Session continuity and seamless handover between WiMAX and WiFi system shall be supported.
- Both single radio and dual radio handovers shall be supported.

5.3.2 Requirements for roaming between WiFi and WiMAX

- WiFi networks shall support EAP based authentication. Non 802.1x based WiFi networks may support EAP based authentication using WISPr 2.0.
- Roaming between WiFi and WiMAX networks is enabled in both directions. The subscriber is always authenticated in the home network.
    - WiFi subscriber roams through a visited WiMAX network and is authenticated by home WiFi AAA based on WiFi credentials.
    - WiMAX subscriber roams through a visited WiFi network and is authenticated by home WiMAX AAA based on WiMAX credentials.
- Common Billing for accessing WiFi and WiMAX networks shall be supported. WiFi and WiMAX may use different credentials but the user may be provided with a consolidated bill.

5.4 Architectural Principles

- No changes to the WiMAX and WiFi air-interface are to be made
- Changes to WiFi access networks should be minimized

6. Architecture Reference Model

6.1 Interworking Reference Model

Figure 6-1 represents the WiFi-WiMAX Interworking Network Reference Model (NRM). The NRM describes the case wherein either the same service provider deploys both WiFi and WiMAX access networks, or these two

networks are deployed by different service providers. In the latter case where WiFi and WiMAX networks are deployed by different service providers, the two service providers are expected to have contractual agreement which enables co-ordinated network access.

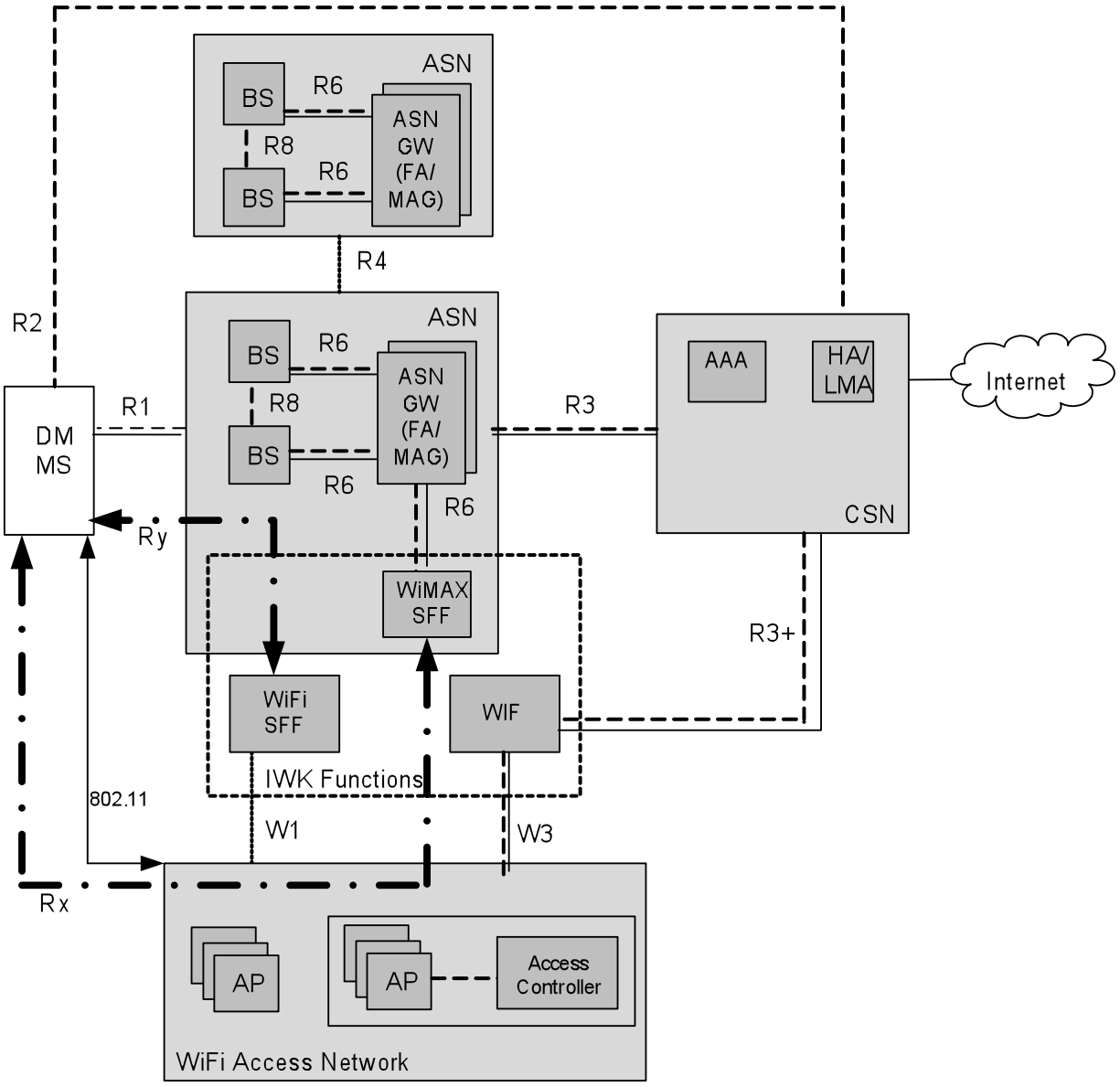

Figure 6-1 WiFi-WiMAX Interworking Network Reference Model

The reference model introduces new logical entities called WiMAX SFF, WiFi SFF and WIF, collectively labeled "Interworking Functions". The functional dcomposition of the IWK Functions is shown in figure 6-2. The IWK Functions consist of the following independent logical entities:

1. WiFi Interworking Function (WIF).
2. WiMAX Signal Forwarding Function (SFF) used to support single radio handovers from WiFi to WiMAX.

3. WiFi Signal Forwarding Function (SFF) used to support single radio handovers from WiMAX to WiFi.

These independent logical entities may be physically co-located in a single network entity or separately located in the network as per the specific deployment scenario.

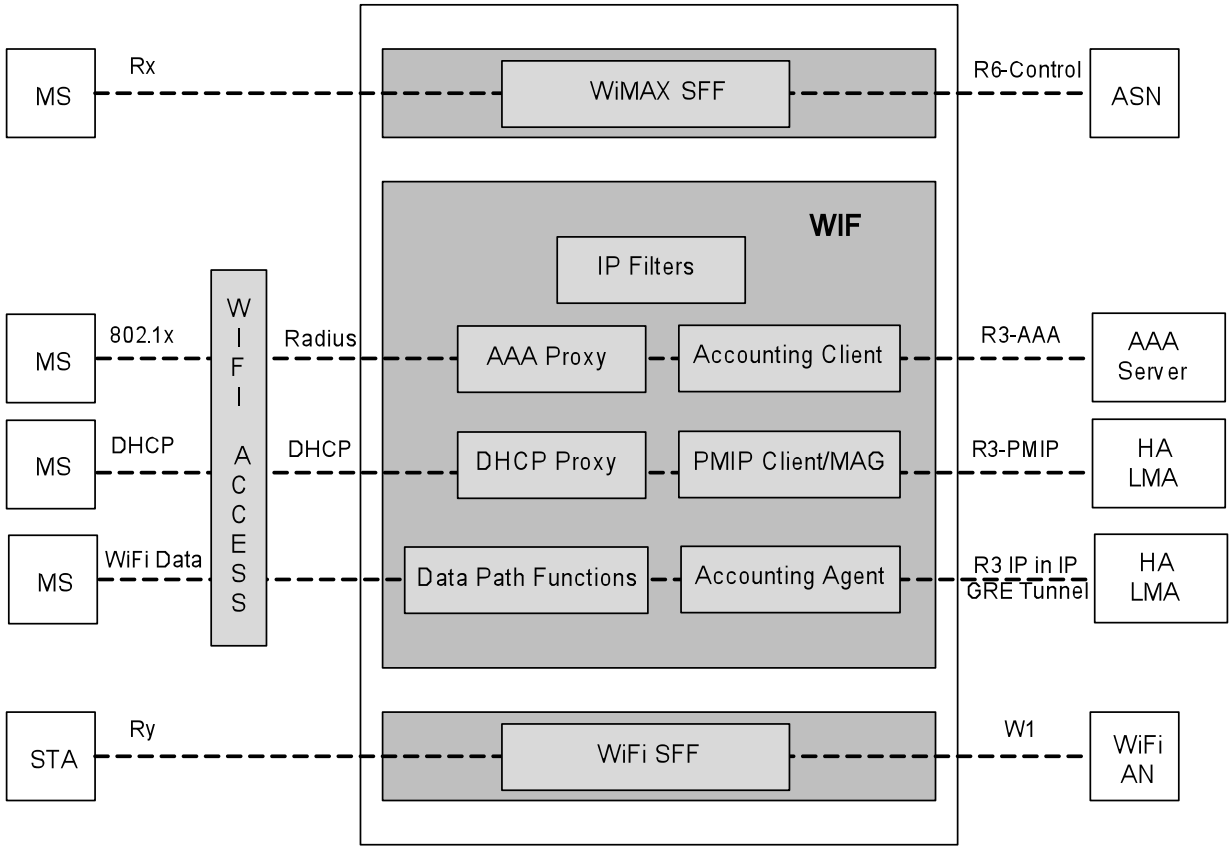

Figure 6-2 Interworking Functions Decomposition

6.1.1 WiFi Interworking Function (WIF)

The WiFi Interworking Function enables the moble device connected to the WiFi AN to access the core functionality of the WiMAX CSN. The WIF supports the following functions.

- AAA Proxy to provide support for authentication and authorization using the CSN AAA server
- PMIP client to provide support for mobility management and IP session continuity using HA/LMA from the WiMAX CSN
- DHCP Proxy to serve the DHCP Requests/Replies
- Accounting Client for generating UDRs and sending the accounting messages to the CSN AAA
- Accounting Agent for metering the WiFitraffic traversing the CSN
- Data Path Functions to create IP in IP or GRE tunnel
- IP Filters for filtering out IP packets from unauthorized WiFi STAs

6.1.2 WiMAX SFF

The WiMAX Signal Forwarding Function enables single radio handovers from WiFi to WiMAX. The WiMAX SFF acts as a virtual WiMAX BS and is connected via R6 reference point to the ASN-GW. . The WiMAX SFF can connect to any of the ASN-GW located in the ASN. Upon handoff the WiMAX SFF may be collocated in the new serving ASN or may not.

6.1.3 WiFi SFF

The WiFi Signal Forwarding Function enables single radio handovers from WiMAX to WiFi. The WiFi SFF acts as an entity forwarding the WiFi signaling and uses the W1 reference point to perform handovers from WiMAX to the WiFi access network.

6.2 Interworking Reference Points

Figure 6-1 shows the reference points that are used in WiFi – WiMAX interworking.

6.2.1 Reference Point R3+

Reference Point R3+ consists of the set of control plane protocols between the WIF and the WiMAX CSN to support AAA and mobility management capabilities. It also encompasses bearer plane methods to transfer user data between the WIF and the WiMAX CSN.

Note: Reference Point R3+ is similar in functionality to Reference Point R3. It is FFS if R3+ is same as R3 or not.

6.2.2 Reference Point Rx

Reference Point Rx consists of control plane messages at the IP layer from MS to WiMAX SFF that enable single radio handover from WiFi to WiMAX. These messages are transfered over the WiFi access network and maybe routed through the WiMAX CSN...

6.2.3 Reference Point Ry

Reference Point Ry consists of control plane messages at the IP layer from STA to WiFi SFF that enable single radio handover from WiMAX to WiFi. These messages are transferred over the WiMAX access network and maybe routed through the WiMAX CSN. .

6.2.4 Reference Point W1

Reference Point W1 consists of control plane messages between the WiFi SFF and the WiFi access network.

Note: The protocol definition for Reference Point W1 is TBD.

6.2.5 Reference Point W3

Reference Point W3 consists of control plane protocols between WiFi access network and WiFi Interworking Function to support AAA, mobility management and data path functions. It also encompasses bearer plane methods to support transfer of user data between the WiFi access network and WIF.

6.3 Roaming Scenarios

6.3.1 Visited WiFi Access Network (802.1X enabled) to Home WiMAX CSN

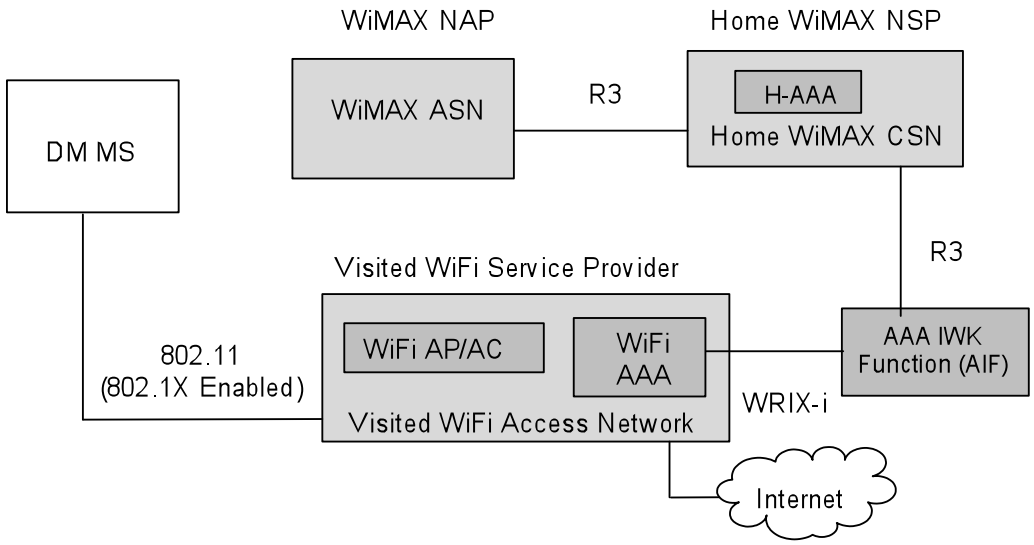

Figure 6-3 Roaming from Visited WiFi Access Network (802.1X enabled) to Home WiMAX CSN

In this case, a WiMAX subscriber gains access to the internet using his WiMAX subscription via a 802.1X enabled WiFi access network. The visited WiFi service provider has a roaming agreement with the home WiMAX Network Service Provider. The WiMAX H-AAA authenticates the user. The AAA IWK unction (AIF) converts the WRIX-i RADIUS protocol to WiMAX R3 protocol.

6.3.2 Visited WiFi Access Network (non-802.1X enabled) to Home WiMAX CSN

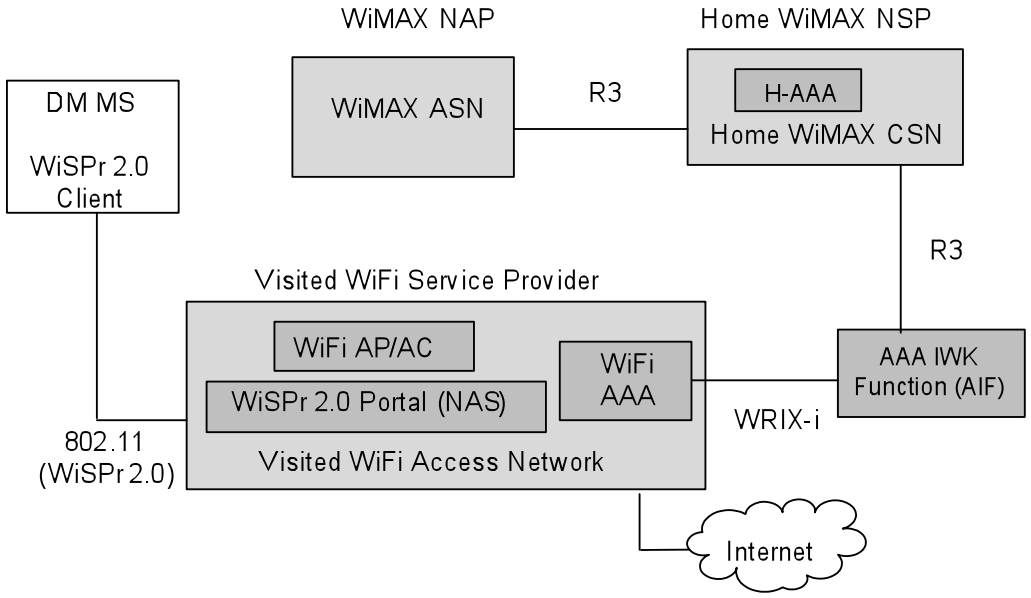

Figure 6-4 Roaming from Visited WiFi Access Network (WISPr 2.0 enabled) to Home WiMAX CSN

In this case, a WiMAX subscriber gains access to the internet using his WiMAX subscription via a WISPr 2.0 enabled WiFi access network. WISPr 2.0 provides mechanism to transport EAP messages over HTTP. The visited

WiFi service provider has a roaming agreement with the home WiMAX Network Service Provider. The WiMAX H-AAA authenticates the user. The AAA IWK unction (AIF) converts the WRIX-i RADIUS protocol to WiMAX R3 protocol.

6.3.3 Visited WiFi Access Network (non-802.1X enabled) to Home WiMAX CSN (via Visited WiMAX CSN)

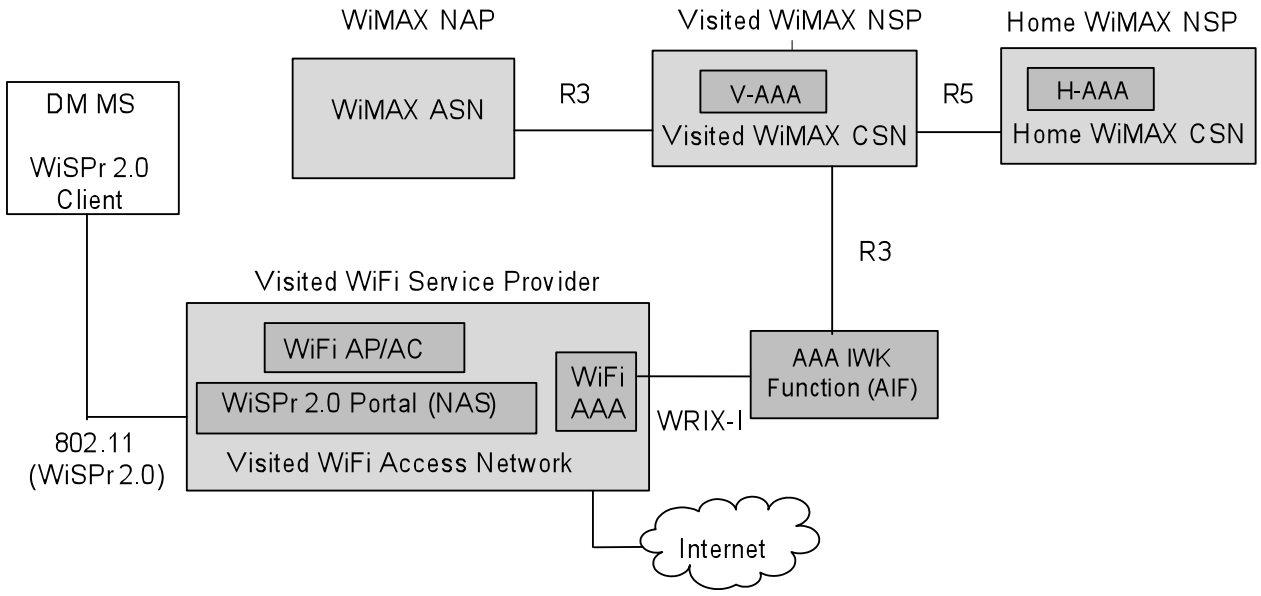

Figure 6-5 Roaming from Visited WiFi Access Network (WISPr 2.0 enabled) to Home WiMAX CSN (via Visited WiMAX CSN)

In this case the WiFi subscriber has a roaming relationship with a Visited WiMAX NSP which in turn has a relationship with the Home WiMAX NSP. The WiMAX H-AAA authenticates the user.

6.3.4 Visited WiMAX Access Network to Home WIFi

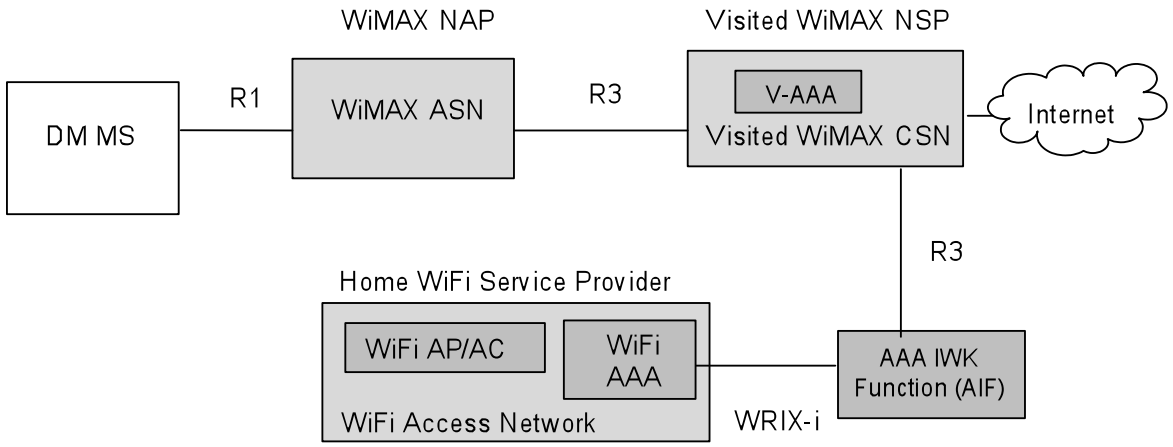

Figure 6-6 Roaming from Visited WiMAX Access Network to Home WiFi Network

In this case, a WiFi subscriber gains access to the internet using his WiFi subscription via a WiMAX access network. The visited WiMAX Network Service Provider has a roaming agreement with the home WiFi service provider. The WiFi AAA authenticates the user. The AAA IWK unction (AIF) converts the WiMAX R3 protocol to WRIX-i RADIUS protocol.

6.4 Roaming Reference Model

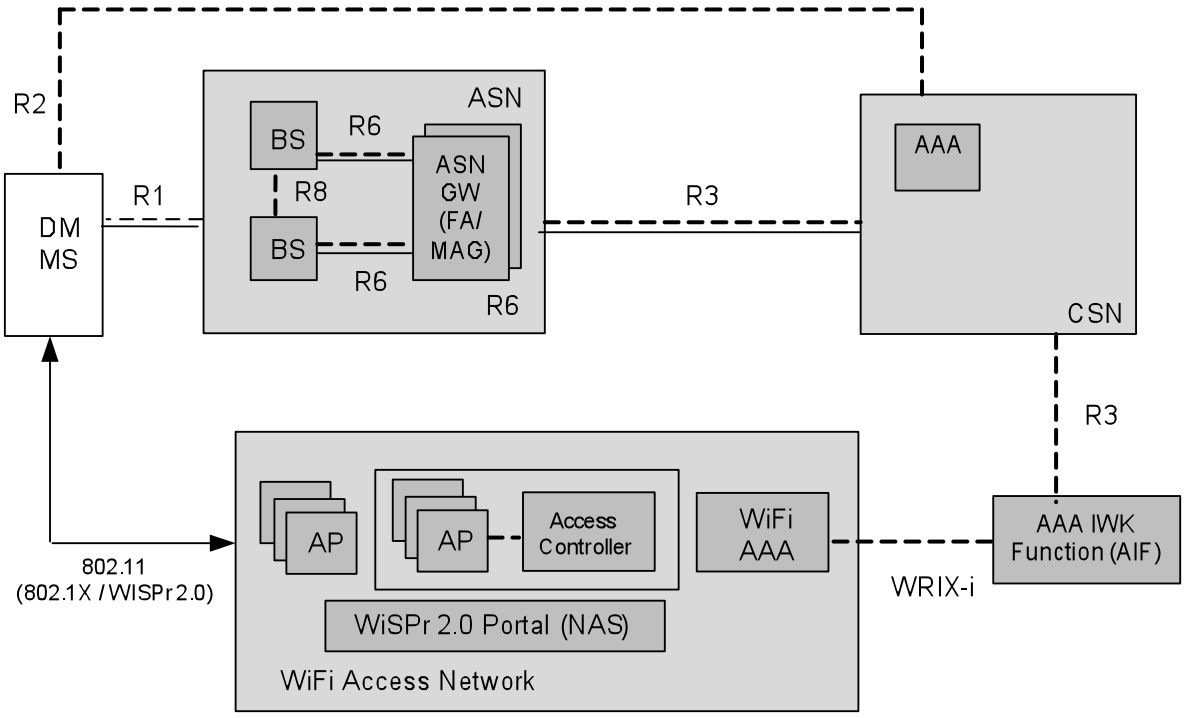

Figure 6-7 WiFi-WiMAX Roaming Network Reference Model

Figure 6-7 represents the WiFi-WiMAX Roaming Network Reference Model (NRM). The NRM describes the case wherein the WiFi and WiMAX networks are deployed by different service providers and the two service providers

have roaming agreement between them. The WiFi access network supports EAP based authentication and is 802.1X or WISPr 2.0 enabled. The reference model introduces a new logical entity called AAA Interworking Function (AIF).

6.4.1 AAA Interworking Function (AIF)

The AAA IWK unction (AIF) is a logical entity and converts the WiMAX R3 protocol to WRIX-i RADIUS protocol and from the WRIX-i RADIUS protocol to WiMAX R3 protocol.

6.4.2 Wireless ISP Roaming (WISPr 2.0)

The WISPr 2.0 specification developed by WBA transports EAP messages over HTTP and enables (non 802.1X based) WiFi networks to perform EAP based authentication. The dual mode mobile device needs a WISPr2.0 client implementation ad the WiFi access network has a WISPr 2.0 NAS portal. WISPr transactions are always initiated by the client. The client passes parameters to the WISPr portal via the parameters of an HTTP Request. The WISPr portal responds to these requests by passing XML parameters in the HTTP response. Further details about WISPr can be found in [3]. WISPr 2.0 has no impact on WiMAX networks.

6.4.3 Wireless Roaming Intermediary Exchange (WRIX)

The WiFi access network supports the WBA WRIX specifications. WRIX provides an independent functional module to provide centralized aggregation adaptation between WiFi roaming partners. WRIX provides several interfaces. The WRIX-i interface is used for RADIUS interconnection.

6.5 Interworking and Roaming Reference Model

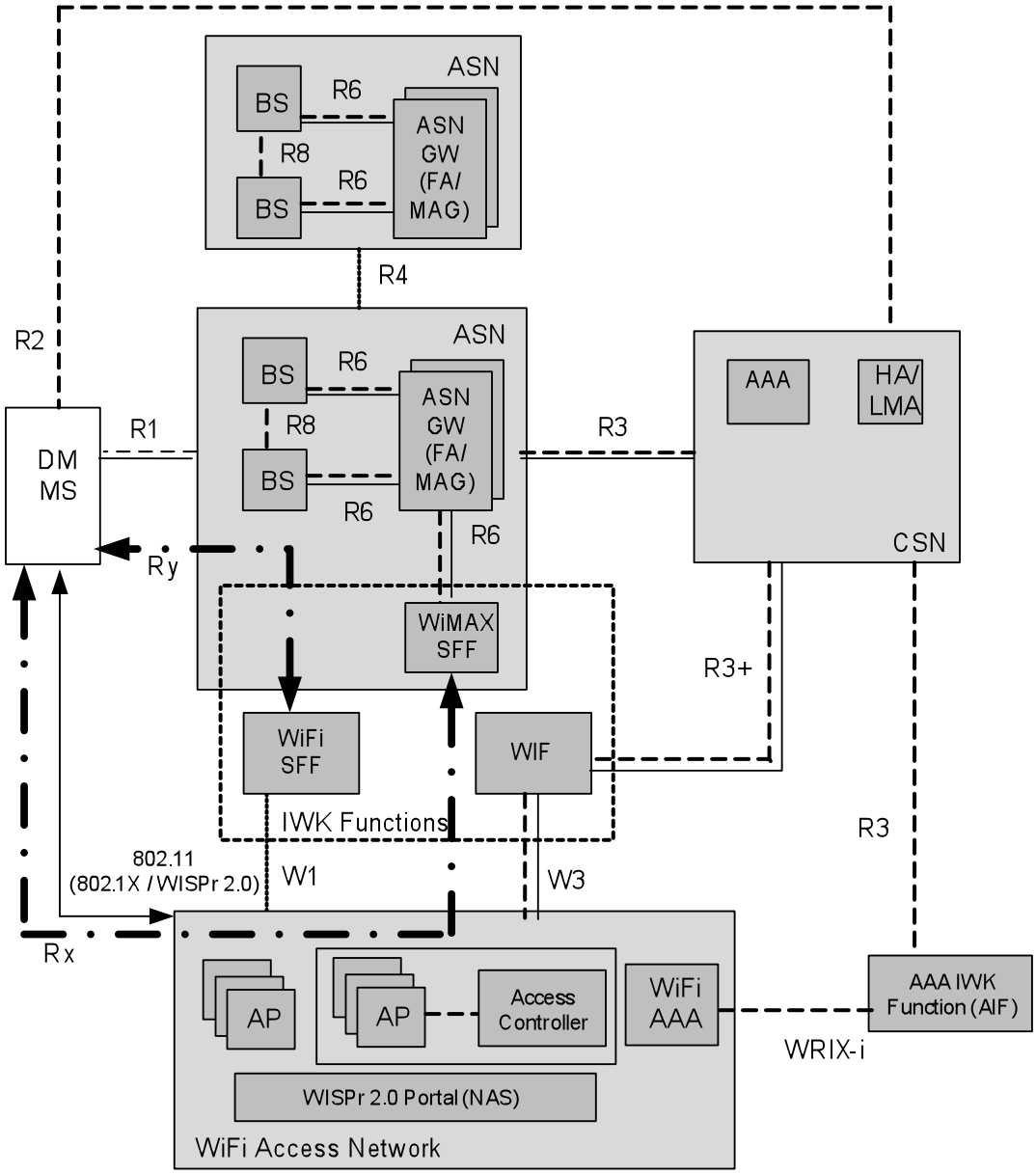

Figure 6-8 WiFi-WiMAX Interworking and Roaming Network Reference Model

Figure 6-8 represents the combined WiFi-WiMAX Interworking and Roaming Network Reference Model (NRM). The NRM describes the case wherein the WiFi and WiMAX networks are deployed by different service providers and the two service providers have roaming agreement between them. The service providers also have a contractual agreement between them which allows for co-ordinated access between them. The IWK Function provides IP Session continuity during handovers. The Roaming functionality by itself only provides nomadic access (no IP session continuity). The mobile device cannot be both roaming and interworking at the same time.

7. Access Network Discovery and Selection

7.1 Access Network Discovery and Selection Principles

The following principles apply for network discovery and selection when the dual mode WiFi-WiMAX terminal is registered with WiMAX CSN.

- WiMAX CSN may provide the MS/STA with information to assist with access network discovery and selection. This includes information about available accesses in vicinity of MS/STA and operator policies which may influence network selection.
- The assistance information provided to MS/STA may depend on the operator policies, information from MS/STA (e.g. location information) or network (e.g. user subscription, network load).
- This information can be used by both single radio and dual radio terminals.

7.2 Architecture for Access Network Discovery and Selection

The Access Network Discovery and Selection is based on the Media Independent Information Service (MIIS) defined in [IEEE 802.21]. Below figure 7.2.1 shows the architecture for Access Network Discovery and Selection.

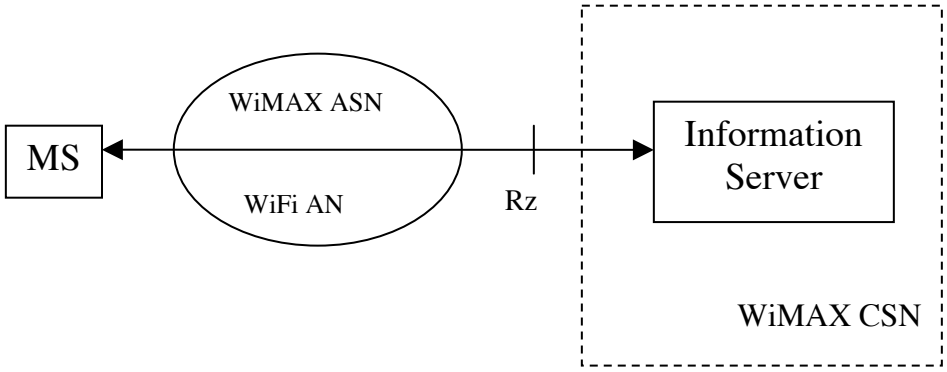

Figure 7.2.1: Architecture for Access Network Discovery and Selection

7.2.1 Information server

The Information Server provides a set of Information Elements for data management and control functionality that is required for network discovery and selection assistance. It provides the ANs as well as inter-system mobility policy such as preferred HO access network type to the MS for the preparation of HO, the SFF information. This is as per operator policies. The Informaton Server initiates data transfer based on requests from the MS or from the network. The Information server is discovered using DNS or DHCP. The address of Information Server may also be pre-provisioned in the MS/STA.

7.2.2 Reference Point

Rz: This reference point is for communication between MS/STA and the Information Server. This interface is realized at or above IP level. The data transfer is initiated based on requests from the MS/STA or from the network..

MS sends MIH information request (and other such messages) and receives the response messages from the Information server over this reference point. The transport protocol for information exchange between MS/STA and

the Information Server is described in the IETF document draft-ietf-mipshop-mstp-solution titled “IEEE 802.21 Mobility Services Framework Design (MSFD)”. The MS and the Information Srver may use UDP transport protocol for information exchange.

7.3 Access Network Discovery and Selection procedure

The Network Discovery and Selection procedure is based on MIH protocol defined in [802.21]. The messages can be sent by using a suitable transport mechanism at layer 3. The Information Elements are represented in TLV format.The call flow is described as follow:

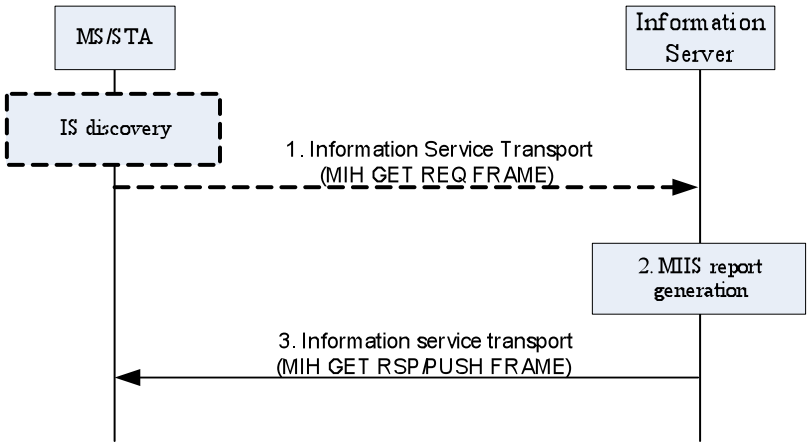

Figure 7-2 Call flow of network discovery and selection

As indicated in figure 7.2.1 the Is is located in the WiMAx CSN. The MS/STA can access the IS either from the WIMAX network or from the visited WiFi network. The MS may use DHCP or DNS mechanisms for discovering the IS server. The address of the IS server can also be preprovisioned in the MS/STA or discovered as part of the initial network attachment.

Step1: MS/STA may send a MIH_Get_Information request to IS to query the information of access networks. This message may include the MS/STA’s location information, a list of link types or identities of access networks.

Step2: IS determines access network information after receiving a request from MS or trigger from network. The information may include access network discovery information (e.g. Network availability), inter-system mobility policies and SFF(s) addresses. IS may determines these information based on the operator policy, user subscription from AAA, or current user location.

Step3: IS sends the generated access network information to MS/STA by MIH_Get_Information response or MIH_Push_Information request message.

7.4 Interworking Function Discovery

The MS/STA may need to discover the availability of WiFi-WiMAX interworking functionality before attaching to a particular access network.

The WiFi access network may provide multiple connectivtiy options. One of the options may be to use WiMAX interworking while there may be other options to connect to WiFi network in conventional ways. The WiFi access network can provide this distinction by the use of suitable SSIDs. The WiFi network may deploy virtual APs with multiple SSIDs. If the WiFi operator supports WiMAX interworking it may configure one of the SSIDs as “WiMAX IWK” (or some such user distinguishable identifier) to enable the user to select the appropriate WiFi access. If the WiFi access provides WiMAX interworking by default (as the only option to connect) then there is no need for virtual APs or multiple SSIDs. The WiFi access network may also include suitable Information Elements (IEs) in beacon to indicate support for WiMAX IWK. The IEs can also indicate support for single radio handovers (presence of WiMAX SFF) from the network.

The WiMAX access network may advertise support for WiFi Interworking by use of suitable parameters in system information broadcast. This can also be used to indicate support for single rado handovers (presence of WiFi SFF) from the network.

7.5 Network Discovery and Selection during Handovers

The following are certain aspects to be considered in network discovery and selection during handovers.

7.5.1 Handovers from WiMAX to WiFi

The MS may discover suitable WiFi network through query-response procedure with Information Server or periodic scanning. The MS may decide to handover to WiFi based on a number of factors such as available QoS, power, cost etc. The MS may perform a single or dual radio handover procedure based on its capabilities of mobile device. If the mobile device supports single radio handovers the mobile needs to discover the presence of WiFi SFF. If this discovery is successful the mobile initiates single radio handover procedures. Alternatively based on the mobile capabilities and other criteria it may initiate dual radio handover procedures. The network does not need any special indication for single or dual radio handover as it would know about the type of handover procedure initiated based on the use of WiFi SFF. After handover to WiFi the mobile device may choose to configure the WiMAX radio in idle mode (for both dual radio and single radio devices). This permits the mobile device to switch back to WiMAX quickly in case the WiFi coverage degrades abruptly.

Figure 7-3 below shows how the Information services can facilitate a SR/DR WiMAX to WiFi handover.

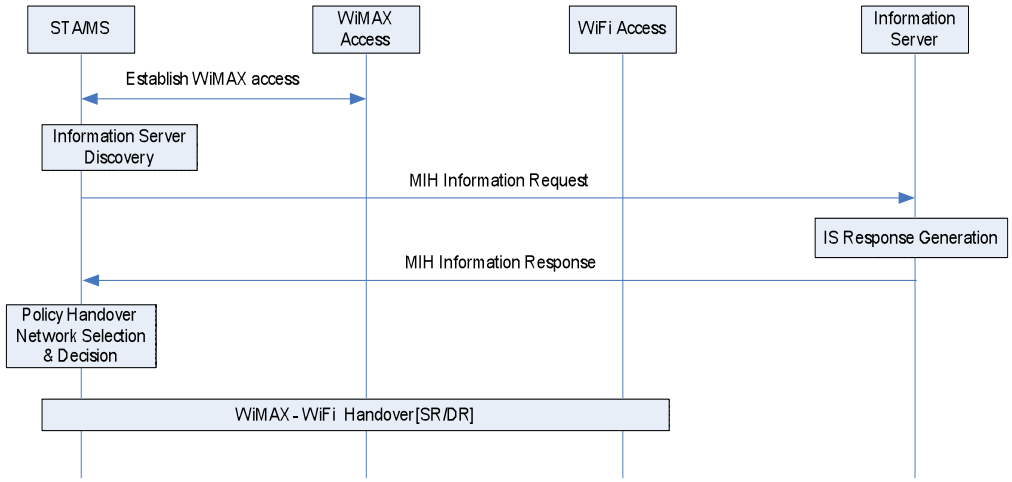

Figure 7-3 WiMAX to WiFi HO facilitated by IS

1. MS/STA discovers Information Server via DHCP or DNS. Alternatively, Information Server address may also be pre-provisioned in the MS/STA.
2. MS/STA MAY need to do authentication with the Information Server.
3. MS/STA does query-response with the Information Server to get information about access networks in the vicinity and other relevant information needed for handover.
4. MS selects a target network (WiFi network in this case) for handover based on the operator policies.

7.5.2 Handovers from WiFi to WiMAX

The mobile device needs to connect to the WiFi access which enables WiMAX interworking functionality. This can be accomplished by use of appropriate SSIDs or specific IEs in 802.11 beacons. Once connected to WiFi, the STA

can discover the presence of WiMAX network either through Information Server or through periodic scanning. The mobile may decide to handover to WiMAX when going out of WiFi coverage or based on variety of other factors. If the mobile decides to perform single radio handovers, it may need to discover WiMAX SFF and Operator Policy for single radio handover through WiMAX SFF. The network does not need any special indication for single or dual radio handover as it would know about the type of handover procedure initiated based on the use of WiMAX SFF.

Figure 7-4 shows how the MIH services can facilitate a SR/DR handover from WiFi to WiMAX.

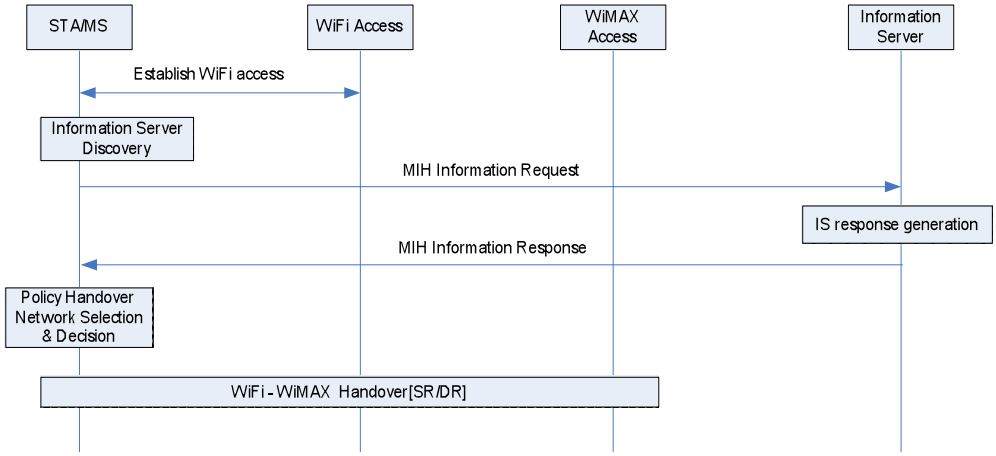

Figure 7-4 WiFi to WiMAX HO facilitated by IS

1. MS/STA discovers Information Server by DHCP or DNS. Alternatively, Information Server address may also be pre-provisioned in the MS/STA.
2. MS/STA MAY need to do authentication with the Information Server.
3. MS selects a target network (WiMAX network in this case) for handover based on the operator policies.

7.6 Information Elements

The information server provides a list of information elements (IE). The Information Elements shall be of the TLV type and are transmitted in the request/response messages between MS/STA and the Information Server.

The information server may provide following types of information:

1. Information for assistance with Access Network Discovery. This includes

- Access networks in vicinity of MS
- Information to assist with scanning and Access network discovery
- Information to assist in access network selection

This information is sent to the MS by IS as a list of IEs with information such as:

- Signal Forwarding Function (SFF)
- Link types of access network
- Operator and service provider identifier for the access network
- QoS characteristics/parameters

- Supported frequency bands
- Address configuration method (e.g. DHCP or autoconfigure)
- Data rate supported by the link layer of the access network

2. Inter System Mobility Policy related information

On request from MS/STA or from the network. Information server may provide a list of IEs with information related to:

- Roaming Policies
- Roaming partners
- Cost of services or network uses

3. Vendor/Operator specific information. This includes

- Operator identifier
- Services provided

Editor's Note: These IEs are subject to availability of appropriate stage-3 text.

8. Subscription and Provisioning

8.1 Deployment scenarios

As the dual mode device accessing the network for services, several use case scenarios can be considered.

8.1.1 Single Subscription

In this scenario the dual mode device maintains a single subscription with either WiMAX or WiFi network operator. If subscription is maintained with the WiMAX network, the dual mode device can access the WiMAX services either directly, by connecting through WiMAX access, or indirectly via the WiFi network.

If subscription is maintained with the WiFi network, the dual mode device can access the WiFi services either directly, by connecting through the WiFi access network, or indirectly, by connecting through the WiMAX access to the services offered by the WiMAX network with the subsriber authentication and authorization of the WiFi network that maintains the subscription.

The case in scope of this document is an indirect access, when the WiMAX network provides access and IP Mobility (HA), as well as the authentication and authorization path to the WiFi AAA, which maintains the single WiFi subscription of the device.

In order to establish the access and mobility security within the WiMAX network, the WiMAX AAA uses the EAP-TTLS protocol to establish the outer tunnel for WiFi subscription authentication. While establishing this tunnel, the WiMAX AAA presents its Certificate to the device in order to prove that it is a legitimate WiMAX network, that is also authorized to provide the WiMAX services to the WiFi subscriber with WiMAX capabilities. As defined in [1], all required security associations for WiMAX operation are derived from the outer EAP-TTLS protocol.

Note: The dual mode device that maintains a single WiFi subscription may not be required to have a provisioned WiMAX Device Certificate. How the WiMAX AAA may handle absence of the Device Certificate in the EAP-TTLS signalling – is FFS.

Once the tunnel is established, the WiFi AAA can be accessed in order to validate the user subscription. The inner method in EAP-TTLS is used for this. Any inner method that provides mutual authentication also allows assurance to the device that services offered by the WiMAX serving network are authorized by the WiFi AAA.

As the result of successful subsctiption authentication the WiFi AAA authorized the WiMAX services.

8.1.2 Dual Subscription

The dual radio MS/STA may maintain two independent subscriptions and therefore two independent sets of credentials: one set with the WiFi network and its AAA and another with the WiMAX AAA for access to the WiMAX network. In such case, each accessed network conducts its own access authentication and authorization.

When dual set of access credentials are used, independent MS subscriptions are retained at the WiMAX AAA and the WiFi AAA , i.e. the WiMAX AAA contains the WiMAX subscription record associated with MS NAI, and the WiFi AAA may contain records associated with just user name and password. In this case, an interface between the WiMAX AAA and the WiFi AAA is not required.

8.2 IP Services

8.2.1 Single Subscription Case:

In this scenario IP services (Simple IP or Mobile IP) are provided only by the WiMAX network regardless whether the device maintains a WiMAX or WiFi subscription.

8.2.2 Dual Subscription Case:

Simple IP services can be provided by the WiFi or the WiMAX networks. Mobile IP services can only be provided by the WiMAX CSN since placement of HA in the WiFi network is out of scope. When device transitions from one technology to another, the respective target technology conducts Initial Network Entry using credentials specific to the target access technology.

9. Authentication and Security

While in an active mode and connected to either WiMAX or WiFi access network, the Dual Mode WiMAX/WiFi device can pre-register and pre-authenticate on the alternate access technology (i.e. WiFi or WiMAX). This applies to both Dual Radio and Single Radio configuration. In order to preserve the security context on the active serving network, the AAA generates a secod security context for the same device, one that is associated with the disparate access technology where pre-registartion and pre-autentication is performed.

In order to generate a unique security context for each access technology using the same NAI, the respective NAS reports its type in the AAA Request message to the authenticating network. When the AAA receives the AAA Request message, it checks the reported “FFS-NAS”and determines, based on the NAI, whether the request is for an initial network access or a pre-registration requiring additional security context for the device.

For initial network access, the AAA conducts the EAP Authentication procedure and stores the resulting security context and its associated Security Parameter Indices (SPI) as the active one for the device. Likewise the MS associates the computed security context with the initial network access.

During the pre-registration on the disparate access technology, the supplicant in the dual mode device creates a second security context associated with the disparate access technology (this could also be handled by a second supplicant). Likewise, the AAA creates the second security context for the same session associated with the access technology on which the device has pre-registered.

If during active session the AAA receives the AAA Request from the same access technology associated with already exisiting security context i.e. same NAI and same access technlogy (indicated through"FFS- NAS", the AAA conducts a Re-Authentication and replaces the security context with the newly generated one.

If the AAA already has the security context for the device, but the AAA Request comes from the disparate access technlology, the AAA checks the subscription record of the device to verify that it is authorized for access from the target access technology, in which case the AAA conducts the EAP access pre-authentication. Upon successful completion of the EAP authentication, the AAA generates a second security context with its associated SPI(s) and stores it alongside the active security context. If the mobile is not authorized to access the disparate access technology, the AAA rejects the AAA Request.

For a Multi-Mode device, when specific security context expires due to its lifetime expiration or de-registration on one of the access technologies, the AAA and the MS delete the expired context while retaining other valid contexts. For a Multi-Mode device, when the session is terminated, all the related security contexts are deleted at the AAA, NASs and MS.

10. Initial Network Entry

The network entry procedure for WiFi and WiMAX networks are described below.

10.1 WiFi Network Entry Procedure

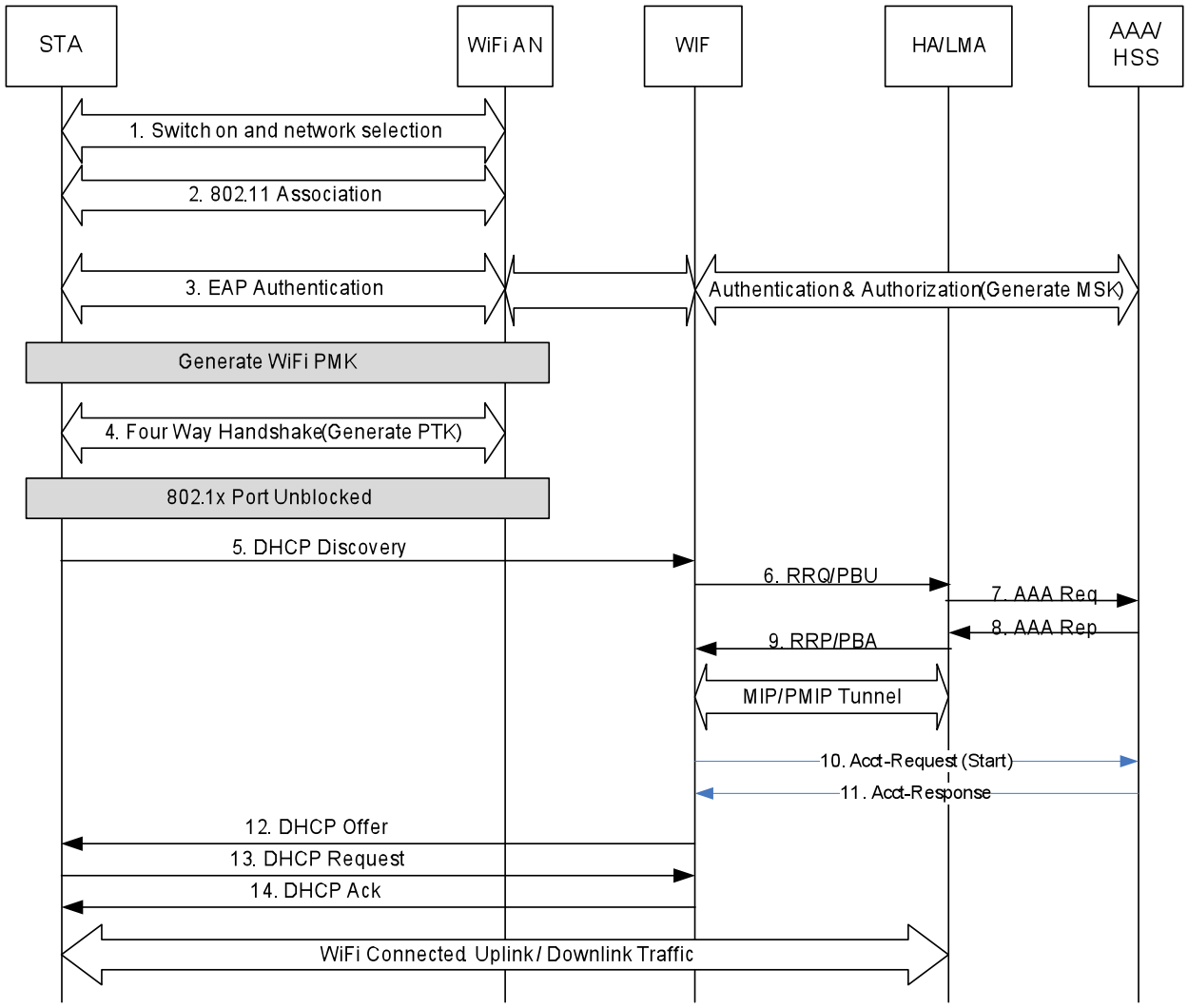

Figure 10-2 WiFi Initial Network Entry Procedure

1. The WiFi STA is switched on, and captures WiFi signaling and then performs network discovery and selection.
2. The STA establishes Association with the WiFi AN
3. The STA authenticates with the WiMAX CSN using 802.1X/EAPOL and various EAP methods such as EAP-TLS and EAP-AKA. The WiFi Access Network may select a WIF based on the realm of STA's NAI, and forwards the EAP messages to the AAA Proxy in the WIF which then facilitates authenticaton on behalf of the WiFi STA. The AAA request from the WIF contains the "FFS-NAS" identifying the access technology. During the authentication, the MSK generated in the AAA Server is transferred to the WiFi AN, and then at the end of the successful authentication, a PMK is derived from the MSK at the WiFi AN.

Editor's Note: "FFS-NAS" will be defined by the Security subteam based on the procedures defined in the IETF (presently ambiguous) to allocate NAS Port type.

The WiMAX-Session-ID and the CUI are delivered to the Accounting Client at WIF.

4. The STA then conducts the four-way handshake with the authenticator in the WiFi AN. During the four-way handshake procedure, a fresh pairwise transient key (PTK) is derived from the PMK. Upon successful completion of the 4-Way Handshake, the 802.1X port is unblocked.
5. The STA sends a DHCPDISCOVER message in order to discover a DHCP server for host IP configuration. WiFi access network forwards the DHCPDISCOVER message to the WIF which is selected during STA authentication.
6. The FA/MAG in the WIF is triggered to initiate PMIP registration procedure. The same NAI used during the EAP authentication procedure is used in the RRQ/Binding Update message. Unless the optional simultaneous binding is supported and invoked, in the RRQ message, the 'S' bit is set to “0”. For the PBU message, the Handoff Indicator option may be set to the value "1" (attachment over a new interface) and the Access Technology Type option may be set to the value "4" (indicatinge IEEE 802.11a/b/g) as specified in RFC 5213. The rest of he fields are initialized as per [4].
7. If the MN-HA key identified by the SPI is not available, the HA requests the MN-HA key from the AAA.
8. The MN-HA key associated wit the MN-HA SPI is returned to the HA for MN-HA AE validation.
9. The HA/LMA responds with the RRP/PMIP PBU message. Once the MN-A AE is validated, the HA/LMA assigns an IP to the MS. If the assigned HoA value in the MIP RRQ/PBU is 0.0.0.0, the HA assigns the HoA, otherwise the HoA in the PMIP Registration request/PBU is used. If this is the initial entry for the MS, the HA/LMA creates a binding cache for the MS.At this point the PMIP tunnel is established between WIF and the HA/LMA.
10. The Accounting Client at WIF sends an Acct-Request (start) message to the AAA
11. Upon receiving the accounting request message, the AAA sends an Acct-Response message to the Accounting Client at WIF
12. The DHCP Proxy in the WIF sends a DHCPOFFER message to the STA.
13. The STA responds to the first DHCPOFFER message received with a DHCPREQUEST message to the DHCP Proxy along with the address information received in DHCPOFFER.
14. The DHCP Proxy in the WIF acknowledges the use of this IP address and other configuration parameters.

10.2 WiMAX Network Entry Procedure

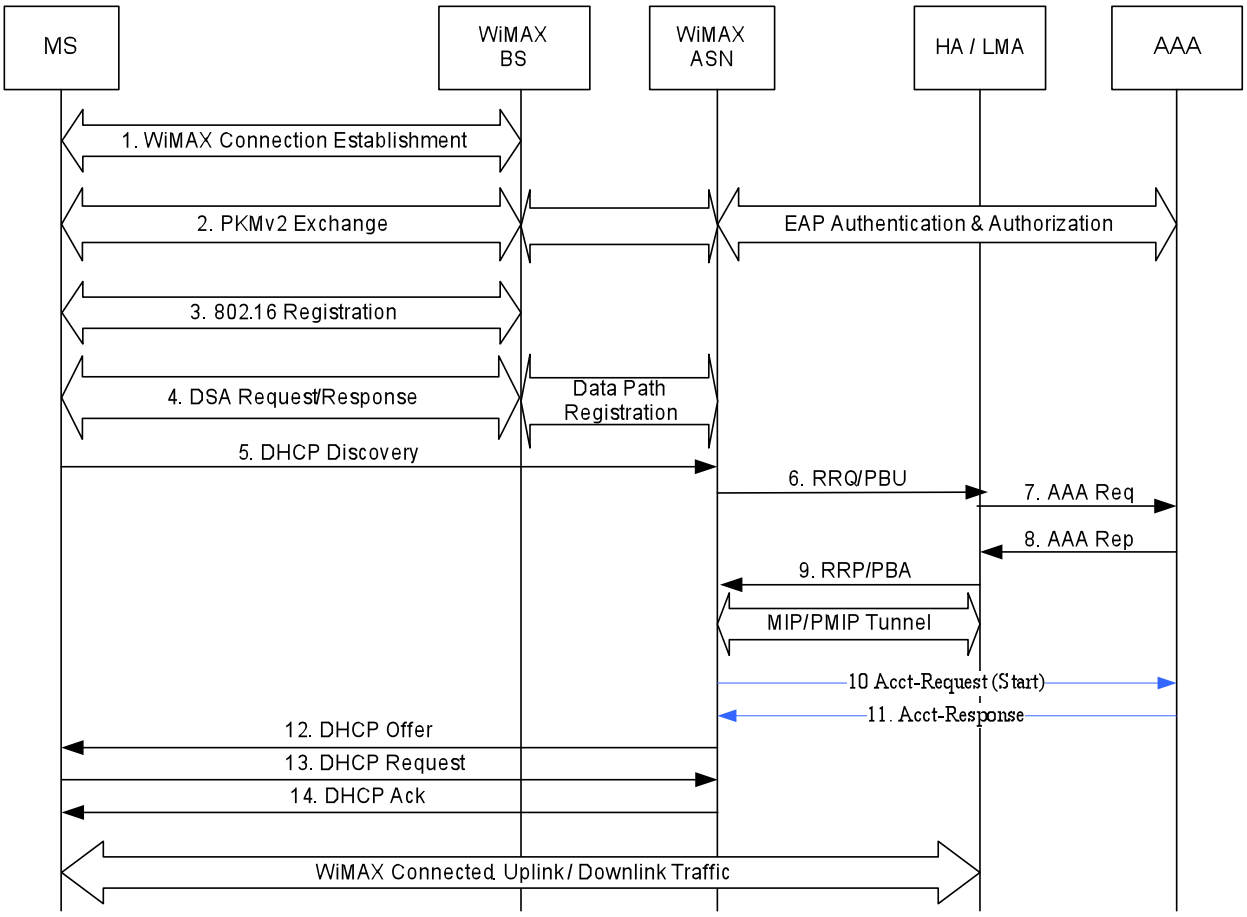

Figure 10-2 WiMAX Initial Network Entry Procedure

1. The MS connects to the WiMAX BS and establishes the WiMAX connection. For details of this procedure please refer to [1].

2. The MS authenticates with the WiMAX CSN using PKMv2 and EAP-TLS/TTLS/CHAPv2/AKA. The MS identifies itself with the NAI during access authentication. The WiMAX ASN includes “FFS-NAS” in the AAA Request to identify the access technology. At the end of this step, MSK is generated at the MS and delivered from the AAA to the WiMAX ASN (ASN-GW Authenticator).

Editor’s Note: “FFS-NAS” will be defined by the Security sbteam basd on the procedures defined in the IETF (presently ambiguous) to allocate NAS Port type.

3. The MS then registers with the 802.16 network

4. The MS then establishes the service flows using DSA Request/Response and also completes data path registration with the ASN.

5. The MS sends a DHCPDISCOVER message in order to discover a DHCP server for host IP configuration.

6. The PMIPv4 client of the MAG in the ASN is triggered to initiate registration procedure. The same NAI is used during the EAP authentication procedure is used in the MIP RRQ or Binding Update message. Unless the optional simultaneous binding is supported and invoked, in the RRQ message, the 'S' bit is set to “0”. For the PBU message, the Handoff Indicator option may be set to the value "1" (attachment over a new

interface) and the Access Technology Type option may be set to the value "5" (IEEE 802.16e) as specified in RFC 5213. The rest of the fields are initialized as per [4].

7. If the MN-HA key identified by the SPI is not available, the HA requests the MN-HA key from the AAA.
8. The MN-HA key associated wit the MN-HA SPI is returned to the HA for MN-HA AE validation.
9. The HA/LMA responds with the PMIP RRP or PMIP PBU message. Once the MN-A AE is validated, the HA/LMA assigns an IP to the MS. If the assigned HoA value in the MIP RRQ/PBU is 0.0.0.0, the HA assigns the HoA, otherwise the HoA in the PMIP Registration request/PBU is used. If this is the initial entry for the MS, the HA/LMA creates a binding cache for the MS. At this point PMIP tunnel us established between the ANS and the HA/LMA.
10. The Accounting Client sends an Acct-Request (start) message to the AAA
11. Upon receiving the accounting request message, the AAA sends an Acct-Response message to the Accounting Client
12. The DHCP proxy in the ASN sends a DHCPOFFER message to MS.
13. The MS responds to the first DHCPOFFER message received with a DHCPREQUEST message to the DHCP proxy along with the address information received in the DHCPOFFER.
14. The DHCP Proxy acknowledges the use of this IP address and other configuration parameters as defined in RFC 2131 by sending a DHCPACK message.

11. Handover

This section describes dual radio and single radio handover procedures.

11.1 Dual radio handover procedures

11.1.1 WiMAX to WiFi Dual Radio Handover

The dual radio MS is initially connected to the WiMAX network and the MS is assigned an IP address from the WiMAX CSN as part of WiMAX Network Entry procedure. The MS determines the presence of WiFi networks in the neighborhood and it also determines if the WiFi network can connect it to the WiMAX CSN and provides interworking services. The MS decides to perform a handover to WiFi. The MS performs the WiFi Network entry procedure as dscribed in section-9. For accessing the WiMAX CSN the dual radio mobile identifies itself with a unique NAI during authentication. Please refer to figure 11-1 below for further details.

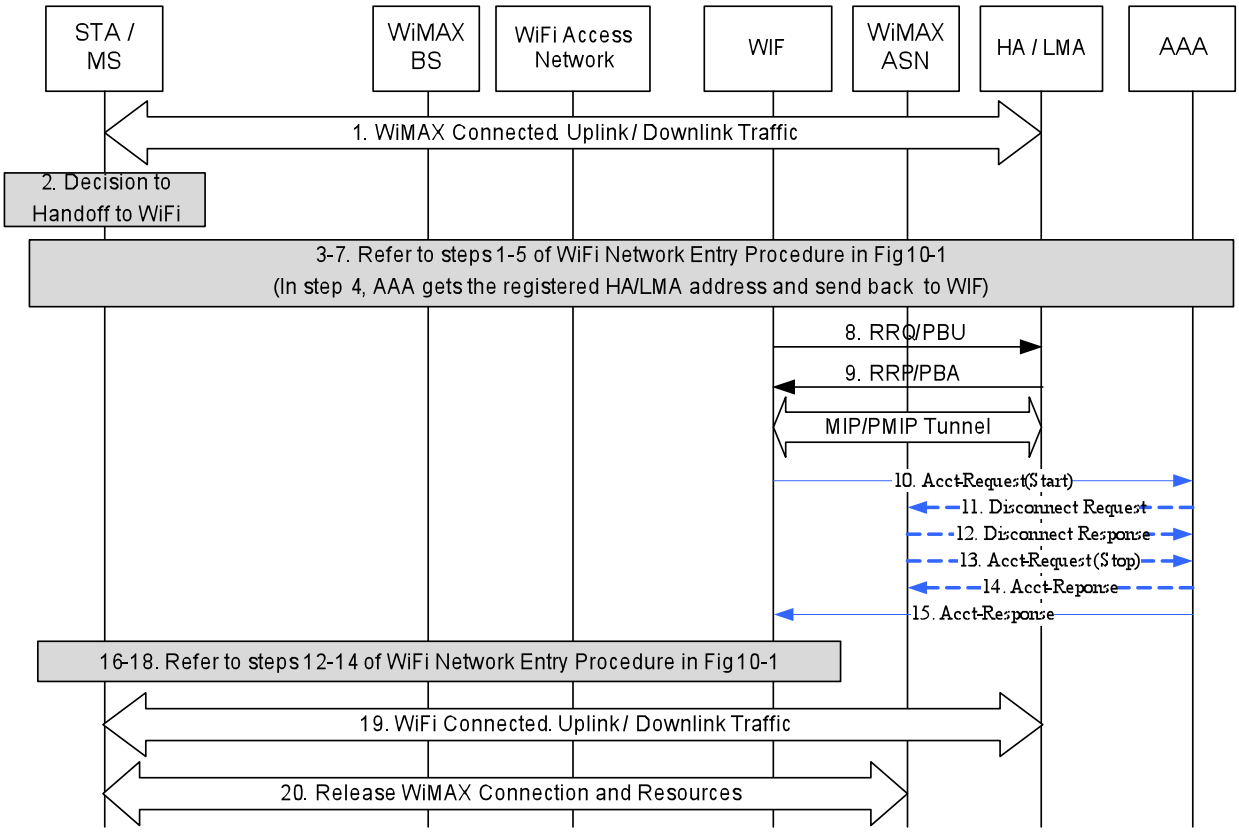

Figure 11-1 WiMAX to WiFi Dual Radio Handover Procedure

1. The mobile device is initially connected to WiMAX access network.
2. Decision is made to handover to WiFi access network.

3-7. Please refer to steps 1-5 in Fig 10-1 of section 10 on WiFi Network Entry procedure. The registered HA/LMA address will be returned from AAA to WIF in step 3.

8. The FA/MAG in the WIF is triggered to initiate PMIP registration procedure. The same NAI used during the EAP authentication procedure is used in the RRQ/Binding Update message.
9. Based on the NAI, the HA assigns the same IP address that has been assigned when connected using the WiMAX access network. The HA updates the binding cache for the MS and sends a PMIP RRQ or Proxy Binding Ack to the WIF along with IP address for mobile device. If the HA/LMA doesn't support simulatenous binding, it invokes the release procedure as described in x.x.x.
10. The Accounting Client at WIF sends an Acct-Request (start) message to the AAA
11. Optionally, the AAA may send a disconnect request message to the WiMAX network for various reasons such as it may not have enough quota for online accounting.
12. The WiMAX sends a disconnect response message to the AAA.
13. The Accounting Client at WiMAX sends an Acct-Request (STOP) message to the AAA
14. The AAA server returns an Acct-Response message to the Accounting Cient.
15. The AAA server returns an Acct-Response message to the Accounting Client at WIF to start the accounting at the WiFi side.

16-18. Please refer to steps 10-12 in Fig 10-1 of section 10 on WiFi Network Entry Procedure.

19. The data traffic is switched to the WiFi network.

20. The WiMAX connection is closed and WiMAX resources are released.

11.1.2 WiFi to WiMAX Dual Radio Handover

The dual radio MS is initially connected to the WiFi network and the MS is assigned an IP address from the WiMAX CSN as part of WiFi Network Entry procedure. The MS determines the presence of neighboring WiMAX networks and it also determines if the WiMAX network provides interworking services with the WiFi network. The MS decides to perform a handover to WiMAX. The MS performs the WiMAX Network entry procedure as dscribed in section-9. The Dual Mode mobile identifies itself with a unique NAI during authentication.

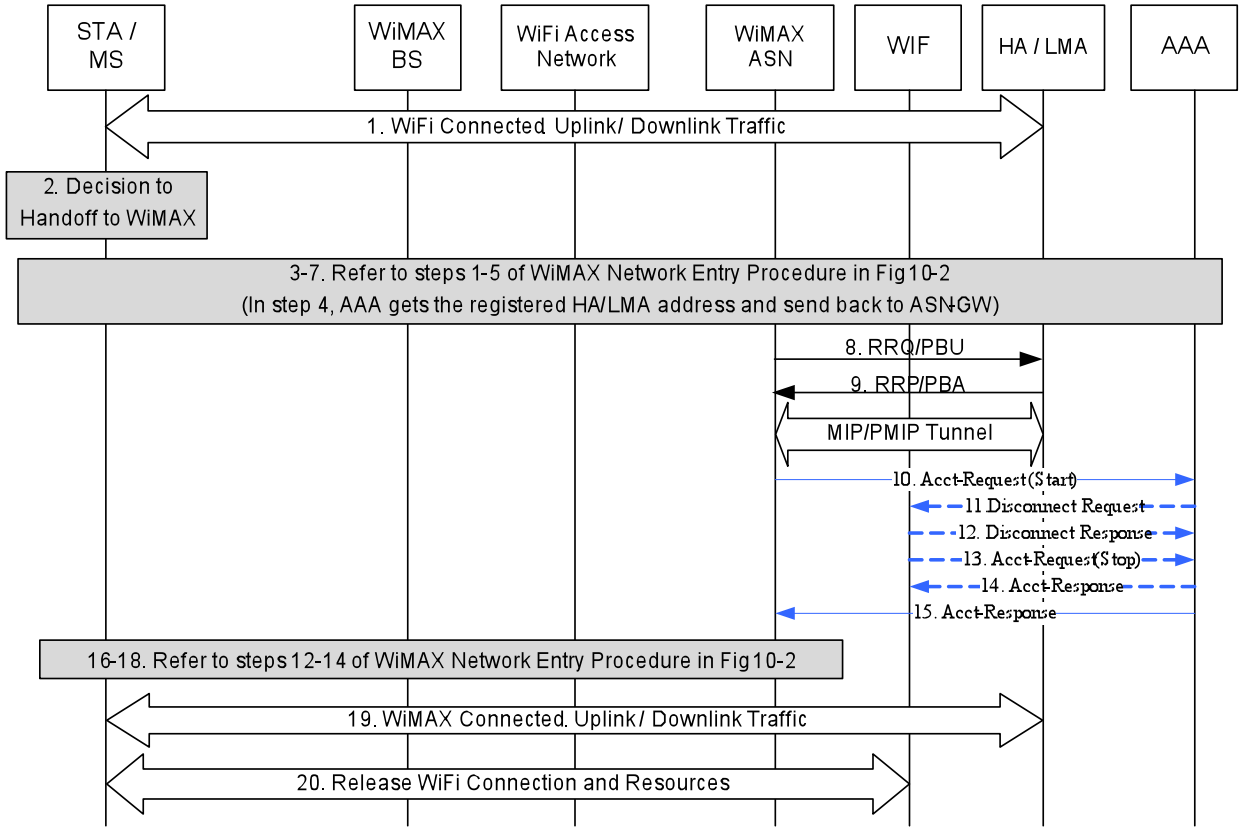

Figure 11-2 WiFi to WiMAX Dual Radio Handover Procedure

1. The mobile device is initially connected to WiFi access network.
2. Decision is made to handover to WiMAX access network.

3-7. Please refer to steps 1-5 in Fig 10-2 in section 10 on WiMAX Network Entry procedure

8. The FA/MAG in the ASN is triggered to initiate PMIP registration procedure. The same NAI used during the EAP authentication procedure is used in the RRQ/Proxy Binding Update message.
9. Once the MN-HA AE is validated, based on the NAI, the HA/LMA, (if the HoA is set to all zero in the MIP RRQ) the same IP address is assigned when connected using the WiFi access network. The HA/LMA updates the binding cache for the MS and sends a RRP/Proxy Binding Ack to the WiMAX ASN along with

IP address for mobile device. If the HA/LMA doesn't support simultaneous binding, it will invoke the release procedure as described in section xxx.

10. The Accounting Client sends an Acct-Request (start) message to the AAA
11. Optionally, the AAA may send a disconnect request message to the WIF for various reasons as it may not have enough quota for online accounting.
12. The WIF sends a disconnect response message to the AAA.
13. The Accounting Client at WIF sends an Acct-Request (STOP) message to the AAA.
14. The AAA server returns an Acct-Response message to the Accounting Cient.
15. Upon receiving the accounting request message, the AAA sends an Acct-Response message to the Accounting Client at WiMAX to start the accounting.

16-18. Please refer to steps 8-10 in Fig 10-2 of section 10 describing the WiMAX Network Entry Procedure.

19. The data traffic is switched to the WiMAX network.
20. The WiFi connection is closed and WiFi resources are released.

11.2 Single radio handover procedures

11.2.1 WiMAX to WiFi Single Radio Handover

In this scenario, initially MS is connected to the WiMAX network. It learns about availability of WiFi network and the interworking functionality. At this point based on one or more decision criteria, the MS decides to handover to the WiFi network. WiMAX to WiFi handover procedures is composed of the following phases, please see Fig 11-3 (for IEEE 802.11i based WiFi network) and see Fig 11-4 (for IEEE 802.11r, based WiFi network).

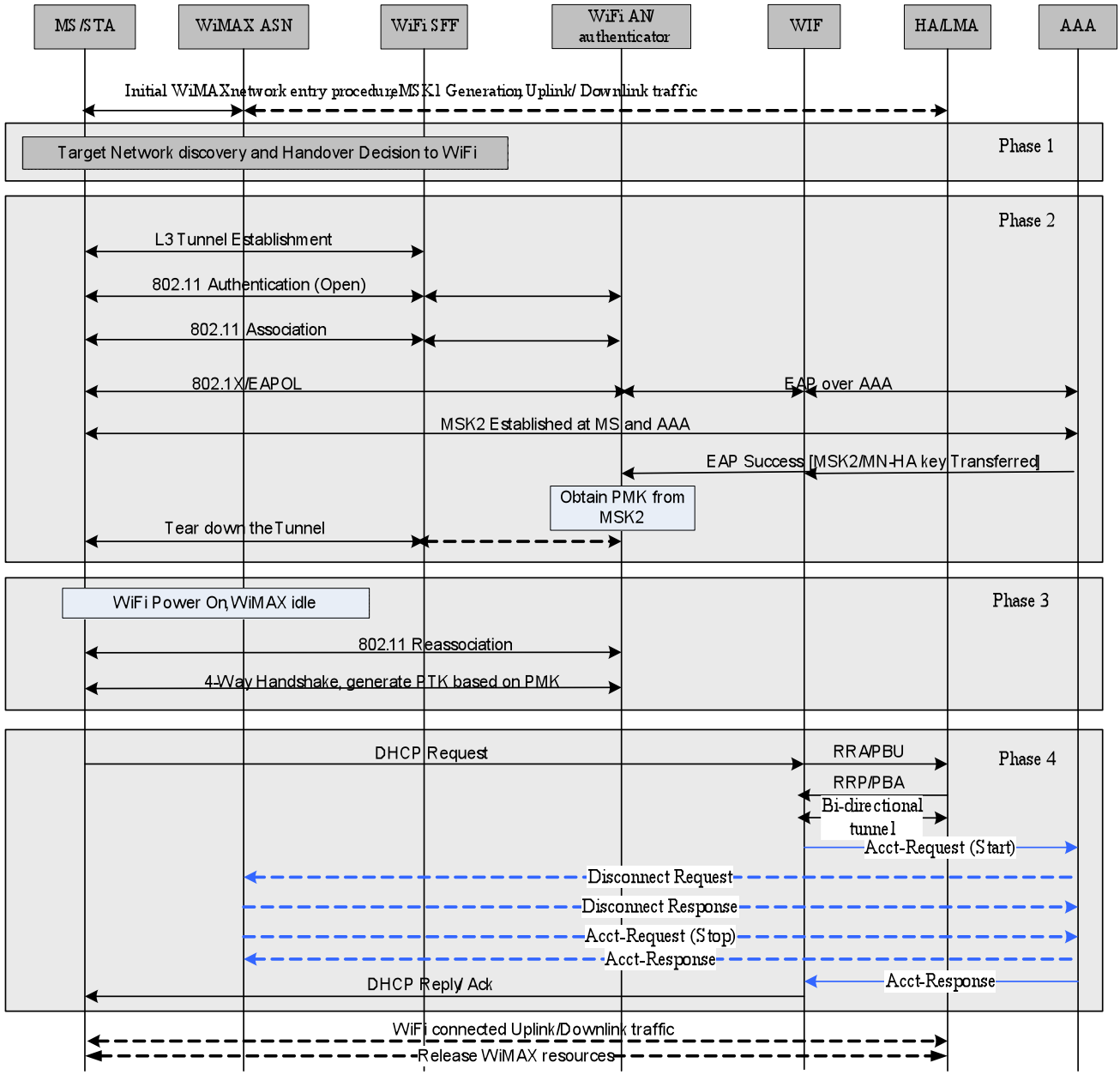

Fig 11-3 Single Radio Handover from WiMAX to 802.11i WiFi network

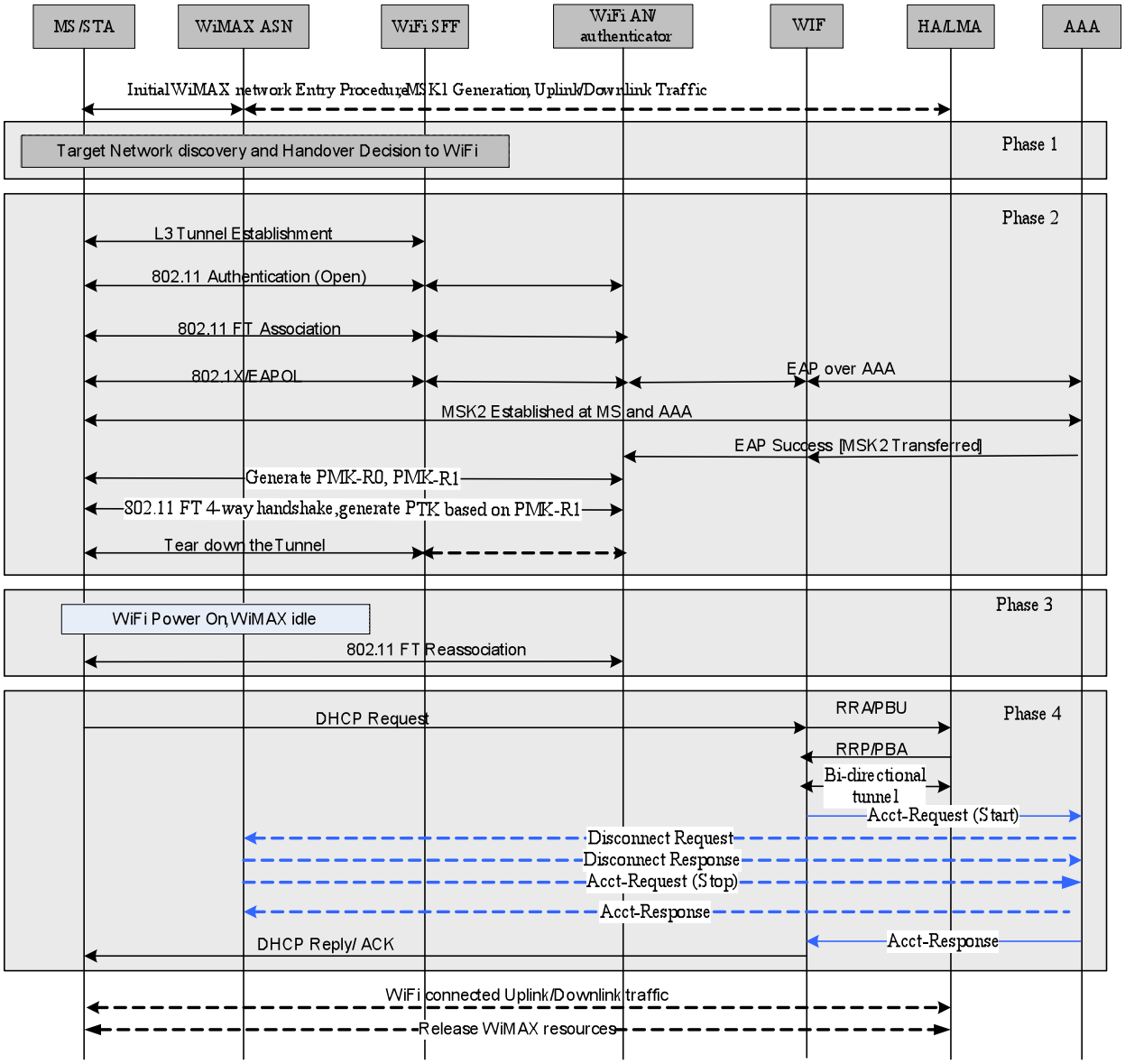

Fig 11-4 Single Radio Handover from WiMAX to WiFi network that supports IEEE 802.11r

In case the target WiFi network supports 802.11i the handover procedure shown in Fig 11-3 is as follows:

Phase Zero: Initial WiMAX Network Entry

The mobile device is initially connected to the WiMAX access network. Initial WiMAX network entry procedure is described in detail in the earlier section. During initial network entry and after a successful EAP procedure MSK and EMSK are generated. These are labeled as MSK1 and EMSK1.

Phase one: Target Network Detection and WiFi-SFF discovery

MS detects the WiFi network signal to determine a target AP and it discovers the address of the WiFi-SFF through DHCP or DNS procedure.

Phase two: Tunnel set-up and EAP-authentication.

1. After the MS discovers the address of WiFi-SFF, the MS establishes IP tunnel to the WiFi-SFF over Ry.
2. The EAP-authentication procedure over the tunnel is as per the IEEE 802.11i specification and is as described below:

- The MS sends Authentication Request frame with Open System algorithm to the target AP and receives Authentication Response frame from the target AP. The BSSID in the frame must be the BSSID of determined target AP. The WiFi-SFF discovers the target WiFi access network based on the BSSID in the Authentication Request frame and forwards the frame to the target network over w1. If the tunnel between the WiFi SFF and the target WiFi network has not been established, the WiFi SFF establishes it and then forwards the Authentication request frame to the WiFi access network.
- The MS associates to the target AP by sending Association Request frame to the AP and receiving Association Response frame from the AP.
- The STA sends the EAPOL-Start message to the target WiFi access network to initiate EAP-authentication over the IP-tunnel. The WiFi SFF forwards this message to the Autenticator located in the WiFi access network
- The MS and authentication server derives MSK and EMSK. These are labeled as MSK2 and EMSK2. The authentication server sends the MSK2 to the authenticator in the target WiFi network, and mobility keys derived from EMSK2 to the PMIP client at the WIF. The authenticator derives PMK from MSK2 according to 802.11i specification.

3. MS releases the IP tunnel created earlier with the WiFi SFF. The WiFi SFF may release the tunnel between the WiFi SFF and the target WiFi network.

Phase three: Handover to WiFi

1. MS decides to handover to the WiFi access network. The WiFi interface is powered on and WiMAX interface may go into idle mode.
2. The MS sends re-association message to the target WiFi AP and then executes 4-way hanfshake procedure in orer to geerate PTK based on the earlier derived PMK..

Phase four: IP session continuity

MS requests and receives IP address anchored at the HA. In this case request and reply messages are proxied by DHCP proxy & PMIP Client/MAG in the Interworking Function, WIF. The Accounting Client at WIF sends an Acct-Request (start) message to the AAA. Optionally, the AAA may send a disconnect request message to the WiMAX network for various reasons such as it may not have enough quota for online accounting. The WiMAX sends a disconnect response message to the AAA. The Accounting Client at WiMAX sends an Acct-Request (STOP) message to the AAA. The AAA server returns an Acct-Response message to the Accounting Cient. The AAA server returns an Acct-Response message to the Accounting Client at WIF to start the accounting at the WiFi side.

Phase five: Release network resources

After the WiFi network is connected the WiMAX network releases the resources.

In case the target WiFi network supports 802.11r network, the handover procedure shown in Fig 11-4 is as follows:

Phase zero: Initial WiMAx Network Entry

The mobile device is initially connected to the WiMAx access network. Initial WiMAX network entry procedure is described in detail in the earlier section. During initial network entry and after a successful EAP procedutre, MSK and EMSK are generated. These are labeled as MSK1 and EMSK1.

Phase one: Target Network Detection and WiFi SFF discovery

MS detects the WiFi network signal to determine a target AP and discovers the address of the WiFi SFF through DHCP and DNS procedure.

Phase two: Tunnel setup and Network Entry.

1. After the MS discovers the address of WiFi SFF, the MS establishes IP tunnel to the WFi SFF over Ry.
2. The WiFi Network Entry procedure over the tunnel is as per the IEEE 802.11r specification and is as described below:
    - The MS sends Fast Transition Authentication Request frame with Open System algorithm to the target AP and receives fast transition Authentication Response frame from the target AP. The BSSID in the frame must be the BSSID of determined target AP. The WiFi-SFF discovers the target WiFi access based on the BSSID in the Fast Transition Authentication Request frame and forwards the frame to the target network over w1. If the tunnel between the WiFi SFF and the target WiFi network has not been stablished the WiFi SFF establishes it and then forwards the first frame of the Fast transition Authentication Request as per the Network Entry procedure.
    - The MS associates to the target AP by sending Fast Transition Association Request frame to the AP and receiving Association Response frame from the AP.
    - The MS starts 802.1x authentication by sending a EAPoL_Start message.
    - The MS negotiates MSK and EMSK with authentication server. These are labeled as MSK2 and EMSK2.The authentication server sends MSK2 to the authenticator in target WiFi network and the mobility keys derived from EMSK2 to the PMIP client at WIF.
    - The MS negotiates PMK-R1 with the authenticator based on MSK2 according to 802.11r specification.
    - The MS negotiates PTK with the target AP based on PMK-R1 by a Fast Transition 4-Way handshake.
3. MS releases the IP tunnel created earlier with the WiFi SFF. The WiFi SFF may release the tunnel between the WiFi SFF and the target WiFi network. The WiFi-SFF may release the tunnel between the WiFi-SFF and the target WiFi network. During pre-authentication, all of the 802.11 MAC frames from the MS are sent to the WiFi-SFF through the tunnel between the MS and the WiFi-SFF. The WiFi-SFF then forwards the frames to the target WiFi network through the tunnel between the WiFi-SFF and the target WiFi network.

Phase three: Handover to WiFi

1. MS decides to handover to the WiFi access network. WiFi interface is powered on and WiMAX interface may be put into idle mode.
2. MS sends Fast Transition Reassociation Request to associate to the target AP and no 4-Way handshake is needed in this case.

Phase four: IP session contiuity

MS requests and receives IP address anchored at the HA. In this case request and reply messages are proxied by DHCP proxy & PMIP Client/MAG in the Interworking Function, WIF. The Accounting Client at WIF sends an Acct-Request (start) message to the AAA. Optionally, the AAA may send a disconnect request message to the WiMAX network for various reasons such as it may not have enough quota for online accounting. The WiMAX sends a disconnect response message to the AAA. The Accounting Client at WiMAX sends an Acct-Request (STOP) message to the AAA. The AAA server returns an Acct-Response message to the Accounting Cient. The AAA server returns an Acct-Response message to the Accounting Client at WIF to start the accounting at the WiFi side.

Phase five: Release network resources.

After the WiFi network is connected, The WiMAX network releases the resources.

11.2.2 WiFi to WiMAX Single Radio Handover

Phase zero: Initial WiFi Network Entry

Initially the MS is connected to the WiFi network. Initial WiFi network entry procedure is described in detail in earlier section. During initial network entry and after a successful EAP procedure MSK is generated. We call this as MSK1. Later, the MS detects availabuility of WiMAX network and learns interworking support. At this point, based on one or more decision criteria, MS decides to handover to the WiMAX network. Overall procedure for WiFi to WiMAX single radio handover is composed of four phases.

Note: the steps and call flows in this document are similar to and is aligned with the 3G-WiMAX handover procedures/call flows.

Phase one: Target network detetion and WiMAX-SFF discovery

MS detects the WIMAX network signal directly and it discovers the address of the WiMAX SFF and Operator Policy on Idle/Active modes supported by the WiMAX SFF during SR handover through the Information Server (see section 7.5 also)..

Phase two: Tunnel set-up and pre-initial network entry (pre-registration phase)

After the MS discovers the address of WiMAX-SFF, it establishes tunnel to the WiMAX-SFF in the WiMAX network. It then performs initial WiMAX network entry procedure over the tunnel between the MS and the WiMAX-SFF. After successful EAP procedure, MSK is generated and sent by the AAA to the authentication. We call this as MSK2.

Phase three: Single Radio Handover action (Active or Idle-to-active)

MS performs handover procedure to the BS present in the ASN. When MS decides to handover to the BS in ASN, it performs “SR Handover Action” procedure toward WiMAX. The procedure can invoke Active or Idle mode described in following subclauses based on the Operator Policy. In this case WiMAX ASN-GW (preregistered ASN-GW) will trigger the Proxy Binding Update (PBU) anytime after successful data path registeration. The Accounting Client sends an Acct-Request (start) message to the AAA. Optionally, the AAA may send a disconnect request message to the WIF for various reasons as it may not have enough quota for online accounting. The WIF sends a disconnect response message to the AAA. The Accounting Client at WIF sends an Acct-Request (STOP) message to the AAA. The AAA server returns an Acct-Response message to the Accounting Cient. Upon receiving the accounting request message, the AAA sends an Acct-Response message to the Accounting Client at WiMAX to start the accounting.

Phase four: Release network resources.

After the MS gets IP address from the HA, in the above phase, the previous network releases the network resources.

Below figure provides the call flows involved in the entire handover process:

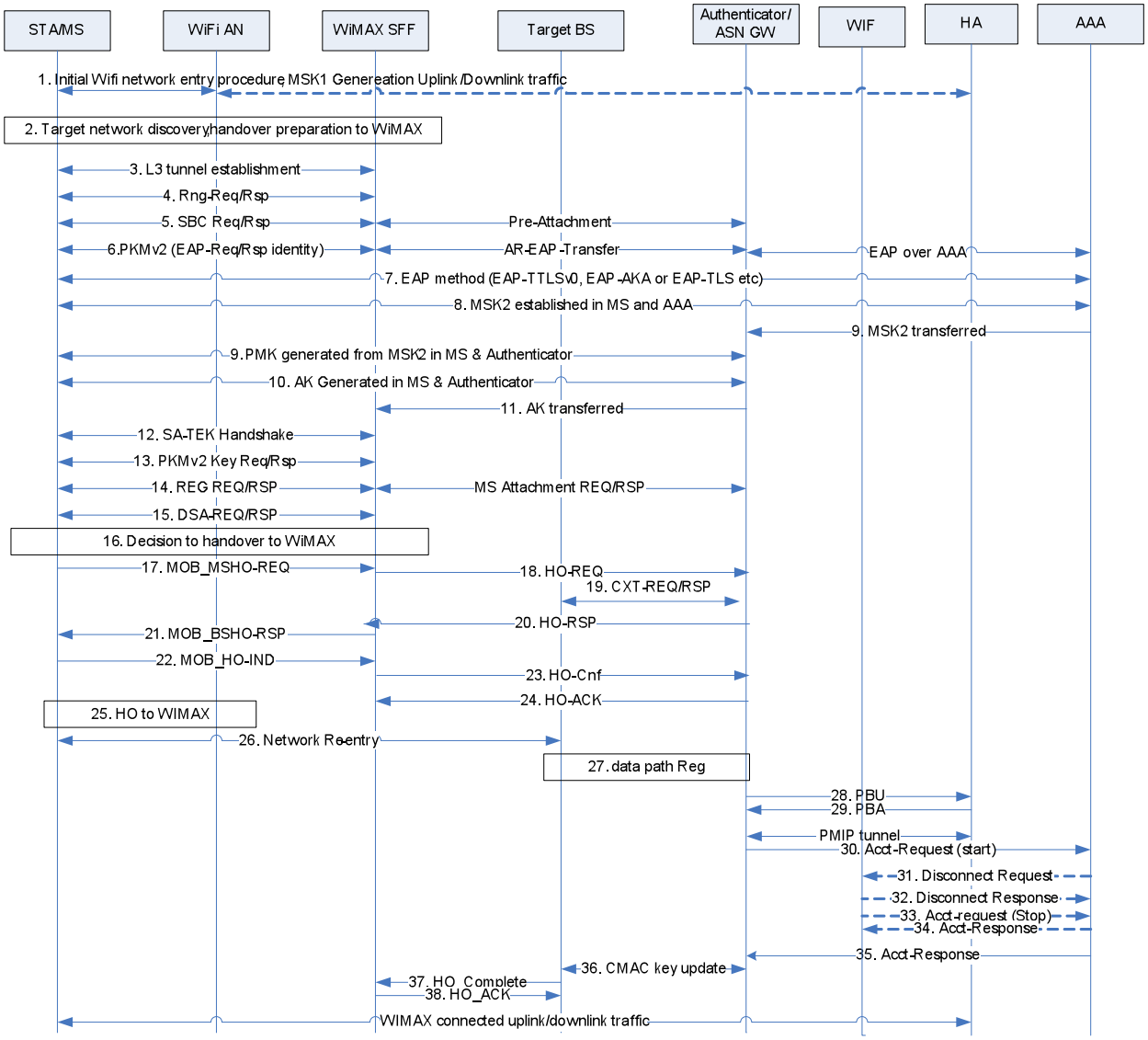

Fig 11-5 WiFi to WiMAX Single Radio Handover Procedures

11.2.1 Active Mode Handover Preparation Procedure

In cases where MS is configured to perform Single Radio handover using active mode, MS performs handover preparation procedures consisting of steps 17 to 24 in the above figure 1.

Details of steps 17 to 21 are decribed in section 4.7.2.1.2 of [NWG STG3].

Details of steps 22 to 24 are decribed in section 4.7.2.2.2 of [NWG STG3].

11.2.2 Single Radio Handover Action Procedure (Using Active Mode)

When the MS decides to handover to the WiMAX network, it performs procedures from step 26 to 32 as detailed in figure 11-5 above.

Steps 26 to 32 in the Fig 11-5 above are similar to handover action scenario 1 described in section 4.7.2.2.2 of [NWG STG3]. In Fig 11-5 above, preregistered ASN-GW triggers the Proxy Binding Update after successful data path registeration.

11.2.3 Idle Mode Entry Procedure

In cases where MS is configured to perform single radio handover action using Idle Entry, MS performs idle mode entry procedure as below. These steps are decribed in section 4.10.5.1 of the WiMAX NWG Stage-3 specification.

11.2.4 WiFi to WiMAX user plane protocol stack

The user plane protocol stack for the scenario where initially MS is connected to the WiFi network and later decides to handover to the WiMAX network is as shown below in the figure 11-6.

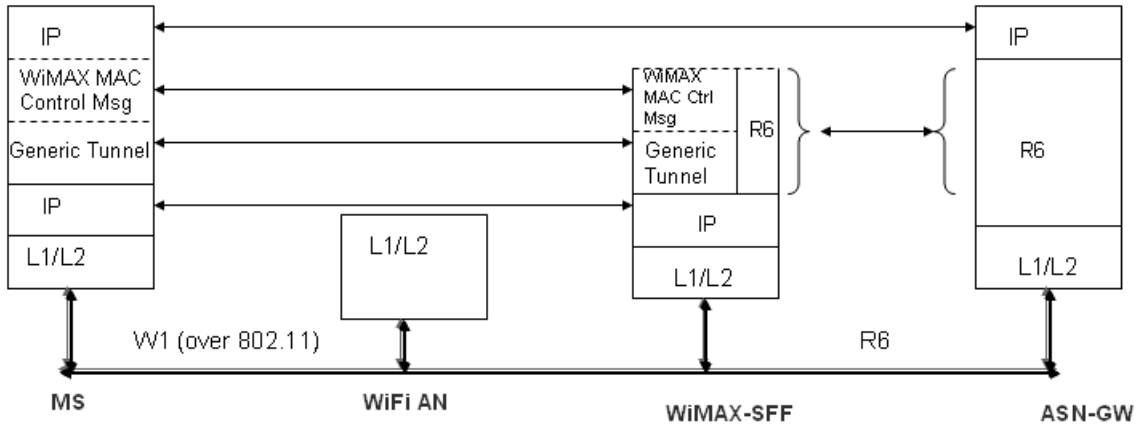

Figure 11-6 User plane Protocol Stack for WiFi to WiMAX Handover

12. Accounting

Accounting records for a session that involves WiMAX and WiFi networks SHALL be independently generated by the WiMAX NAS and CSN and by the WiFi Network. Since a subscriber can access both networks with different subscriptions simultaneously, subscriber or subscription based accounting can only be done after accounting records are consolidated and correlated at the back office. Hence the specification of subscriber or subscription based accounting is out of scope of this document.

For better correlation of the accounting records generated for the same session at each of the access networks, the WIF also generates Accounting Records and may include User Data Records (UDRs) information that comply with the WiMAX format and send the UDRs to the HAAA. If accounting information is not collected, the counter values SHALL be set to zero. The correlation of the potential numerous sets of accounting records for the same session (i.e. WiFi, WIF, WiMAX, HA) by the billing mediation system is out of scope of this document. Nevertheless, if the WiMAX-Session-ID and the Chargeable User Identity (CUI) attributes are supplied by the AAA and the WIF provides valid Accounting Records for the traversing WiFi traffic, it SHALL include the WiMAX-Session-ID (carried in the Acct-Multi-Session-Id) and CUI in all the accounting messages and the generated UDRs. The WiMAX-Session-ID, the CUI and accounting records time stamps can be used to correlate the accounting records

generated by the WiMAX system and the similar accounting records generated by the WIF for the interworking session.

12.1 Accounting Information Collection

The accounting client in the WIF MAY report counts of all data packets and octet counts sent and received through the FA/MAG to or from the mobile. Report of control and signaling data is optional. UDRs (User Data accounting Records) may be collected by the AAA client at the WIF and sent to the HAAA. The UDR records SHALL conform to the RADIUS packet structure as well as for the case of Diameter. Also note that per the WiMAX accounting architecture, the HA/LMA in the CSN may also generate all or a subset of the accounting records that are generated at the WIF.

12.2 WIF Accounting Requirements

The WIF SHALL generate IP-session based accounting records complying with the WiMAX accounting format and SHALL also support RFC 5176. If the WIF supports on-line accounting capabilities then it SHALL include the PPAC attribute in the RADIUS Access-Request packets.
The WIF SHALL include the WiMAX Capability attribute in the RADIUS Access-Request packet or WiMAX-Capability AVP in the Diameter WEDR message during the WiFi access network attachment in order to indicate its capabilities to the HAAA. The WIF SHALL also indicate support for IP session based accounting. If the WIF receives an Access-Accept/WEDA in which the HAAA did not select IP session accounting mode, the WIF SHALL not generate UDRs, nor provide any Accounting information to the AAA.

When full Accounting Information is generated by the WIF, any incoming accounting message from the WiFi network SHALL NOT be forwarded to the AAA.

13. Network Exit

MS De-registration is a common scenario caused by graceful shutdown or some failure or maintenance situation where MS is deregistered from network service and its context is deleted.

The following entities may initiate MS Deregistration process:

- MS, when it initiates graceful shutdown;
- WiFi AN, if MS is connected to WiFi access network based on either graceful shutdown trigger or failure situation in WiFi network;
- WiMAX ASN, when MS is connected to WiMAX access network and based on either graceful shutdown trigger or failure situation in network;
- WIF or HA/LMA, when MS is connected to WiFi access network and based on failure or maintenance situation in network such as unable to build MIP tunnel;
- Home AAA server located in CSN is also able to trigger MS Deregistration.

13.1 Network exit procedure from WiMAX side

The Network exit procedure from WiMAX side is the same as section 4.5.2 in [NWG stage 3].

13.2 Network exit procedure from WiFi side

This section describes the network exit procedure when MS/STA accesses to WiMAX CSN via WiFi AN, the WiFi network exit procedure can be initiated by MS/STA, WiFi access network, WIF, HA/LMA or AAA server. When the exit event happens at WiFi side, all the keys and related resources will be deleted for this access network.WiFi

13.2.1 Initiated by MS/STA or WiFi AN

MS/STA may start network exit procedure at WiFi side when initiates graceful shutdown. WiFi AN may initiate network exit procedure at WiFi side when some errors occurred, such as overload. Figure 13.1.1 represents STA/MS or WiFi AN initiated network exit procedure.

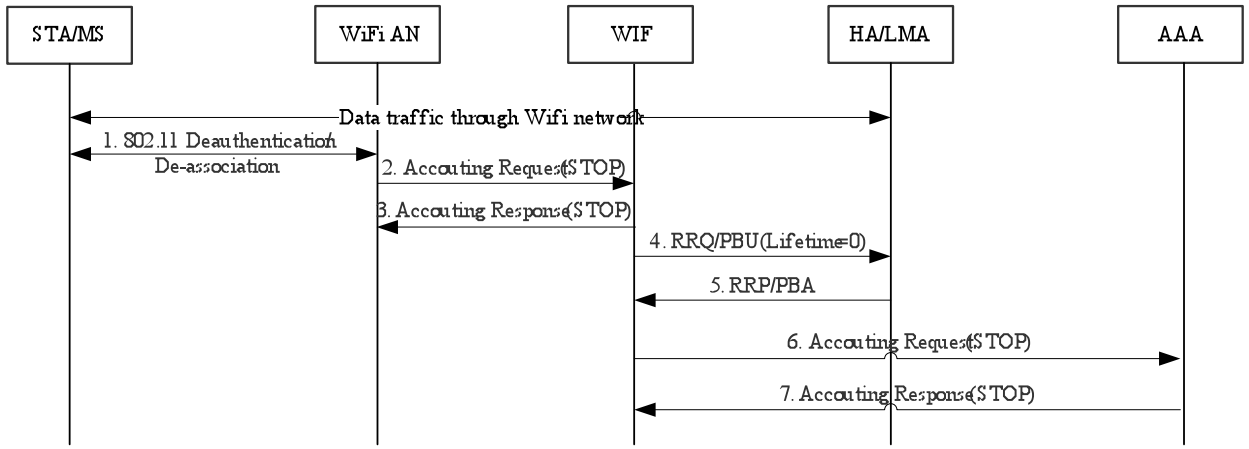

Figure 13.1.1: MS/STA or WiFi AN initiated network exit procedure

Step1: The MS/STA or WiFi AN may initiate network exit procedure using 802.11 Deauthentication or De-association procedure.

Step2: The WiFi AN may send an Accounting Request (STOP) message to the WIF. Otherwise, an ungraceful network exit procedure may be initiated because of the MS's context expired or PMIP session is expired based on configuration.

Step3: The WIF returns an Accounting Response (STOP) message to WiFi AN if it has received the Accounting Request (STOP) message.

Step4: The WIF sends a RRQ/PBU (lifetime=0) message to HA/LMA for MIP deregistration. This step can be performed before step 3.

Step5: HA/LMA responses to the WIF with a RRP/PBA message.

Step6: The Accounting Client function in WIF sends an Accounting Request (STOP) message to AAA server to indicate the network exit and stop collecting traffic information. This step can be performed after step 2 without waiting for step 5.

Step7: AAA server returns an Accounting Response (STOP) message to the WIF.

13.2.2 Network exit procedure initiated by WIF or HA/LMA

WIF may gracefully initiate network exit procedure at WiFi side by some failure situation or for maintenance for WIF element nodes. HA/LMA may decide to initiate WiFi side network exit procedure in case it detected expiry of the MS's MIP binding lifetime or another event eligible. Figure 13.2.1 represents WIF or HA/LMA initiated network exit procedure from WiFi AN.

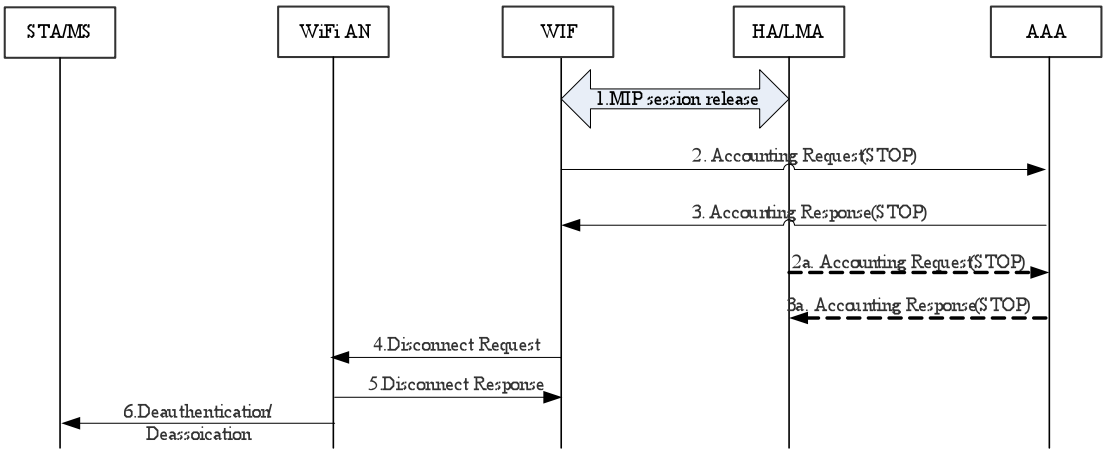

Figure 13.2.1 FA/MAG or HA/LMA initiated network exit procedure from WiFi AN

Step1: When WIF or HA/LMA determines to initiate the network exit, they shall perform the MIP session release by sending a RRQ/PBU (lifetime=0) message or Reg_Rev/BRI message.

Step2: The WIF sends an Accounting Request (STOP) message to AAA server. Optionally if there is an accounting client at HA, it may send Accounting Request (STOP) message to AAA as indicated in step 2a.

Step3: AAA server responses to the WIF with an Accounting Response (STOP) message. If it is received from HA, it sends a response message to HA as indicated in step 3a.

Step4: The WIF notifies WiFi AN of the network exit by Disconnect Request message. This step may happen prior to step 2.

Step5: WiFi AN responses to the WIF with Disconnect Response message.

Step6: WiFi AN invokes deauthentication/de-assoication with the STA/MS after it received the Disconnect Response message. This step may be performed prior to step 2.

13.2.3 Network exit procedure initiated by AAA

AAA server may initiate WiFi side network exit procedure because of changing service strategy including user's arrearage, report loss of mobile phone by user etc. Figure 13.3.1 represents AAA server initiated network exit procedure from WiFi AN.

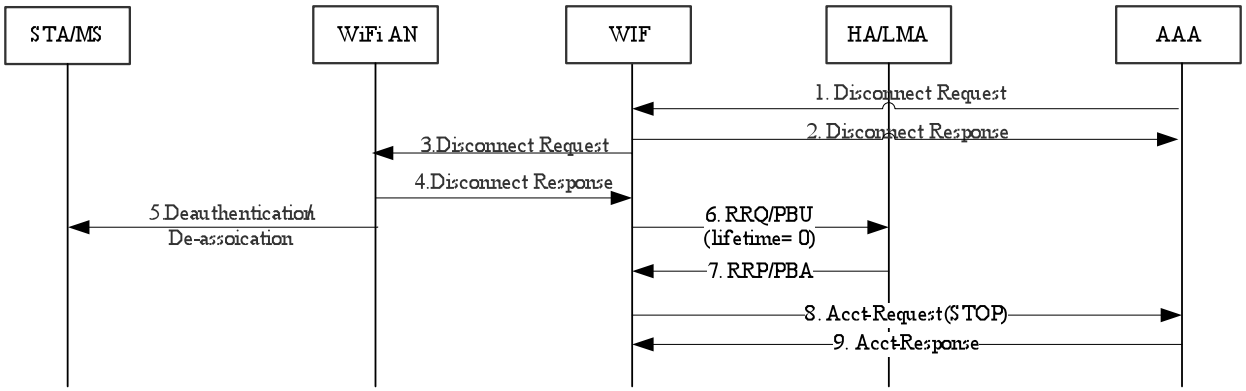

Figure 13.3.1: AAA initiated network exit procedure from WiFi AN

Step1: AAA server initiates the WiFi side network exit procedure by sending a Disconnect Request message to the WIF.

Step2: The WIF responses to AAA server with a Disconnect Response message.

Step3: The WIF sends a Disconnect Request message to WiFi AN.

Step4: WiFi AN responses to the WIF with a Disconnect Response message.

Step5: WiFi AN will invoke Deauthentication/Deassociation procedure with STA/MS.

Step6: The WIF sends a RRQ/PBU (lifetime=0) message to HA/LMA for MIP deregistration. This step can be performed before step 3.

Step7: HA/LMA responses to the WIF with a RRP/PBA message.

Step8: The Accounting Client function in WIF sends an Accounting Request (STOP) message to AAA server to indicate the network exit and stop collecting traffic information. This step can be performed after step 2 without waiting for step 4.

Step9: AAA server returns an Accounting Response (STOP) message to the WIF.

13.3 Network Exit for MS/STA in Idle and power Save mode

This section describes Network exit from the previous network while MS/STA has handed over to the current network.

13.3.1 MS/STA Handover to WiFi Network and WiMAx in Idle Mode

Due to various reasons such as ping-pong scenario or to avoid losing packets during handover, the MS/STA which initially was connected to the WiMAX network performs handovers to the WiFi AN but doesn't immediately exit the WiMAX network. Thus, in this case step(s) involving "Release WiMAX resources" in the call flows for single/dual radio handover to WiFi may not done based on operator policy.

Once the MS moves to the WiFi network, a MIP/PMIP tunnel is established between the LMA/HA and the WIF. The previous MIP/PMIP tunnel between the LMA/HA and the MAG/ASN is either removed or optionally maintained as a simultaneous binding for a programmable period of time. Hence, any future traffic is sent over the new MIP/PMIP tunnel to the MS/STA over WiFi or optionally on both.

After HO to the WiFi network, the MS/STA may enter WiMAX idle mode operation by creating the tunnel between MS and the WiMAX SFF. If the MS is not in the idle mode at WiMAX side, the MS will perform idle mode entry as per section 4.10 [NWG Stage 3]. Note, MS may enter idle mode in WiMAX before handover to Wifi based on operator policy. The MS will send WiMAX signaling message through the tunnel between MS and WiMAX SFF to maintain the idle mode as per section 4.10 [NWG Stage 3].Alternatively exit the WiMAX network after a programmable "retain time" value.

To exit the WiMAX while connected to the WiFi AN, the MS/STA sends network exit trigger message over l3 tunnel to the WiMAX-SFF/Interworking function. Subsequently, WiMAX-SFF/Interworking functional entities such as accounting client, PMIP Client/MAG, etc triggers and completes the WiMAX network exit procedure, including, stop accounting procedure and release mobility, security contexts, etc as per the section 4.5.2 [NWG stage 3].

After "retain time" value or due to some other reasons network MAY clean up the resources for the MS. The following network entities can initiate the Network Exit Procedure during idle mode to perform ungraceful Exit and is detailed in 4.5.2.2 [NWG Stage 3]:

- AAA Server/Authenticator

- Paging Controller
- HA/LMA
- DHCP Proxy/Relay

13.3.2 MS/STA Handover to WiMAX Network and WiFi in Power Save Mode

Due to various reasons such as ping-pong scenario or to avoid losing packets during handover, the MS/STA which initially was connected to the WiFi network performs handovers to the WiMAX network but doesn't immediately exit the WiFi network. Thus, in this case step(s) involving "Release WiFi resources" in the call flows for single/dual radio handover to WiMAX may not be done based on operator policy.

Once the MS moves to the WiMAX network, a MIP/PMIP tunnel is established between the LMA/HA and the MAG/ASN. The previous MIP/PMIP tunnel between the LMA/HA and WIF is either removed or optionally maintained as a simultaneous binding for a programmable period of time. Hence, any future traffic is sent over the new MIP/PMIP tunnel to the MS/STA over WiMAX or optionally on both.

After HO to the WiMAX network, the MS/STA may switch into the WiFi power save/Sleep mode operation as per its standard behavior. Alternatively, it may decide to exit the network after a programmable "retain time" value.

To exit WiFi while connected to the WiMAX, the MS/STA sends network exit trigger message, over l3 tunnel to the WiFi-SFF/ Interworking function. Subsequently, WiFi-SFF/Interworking functional entities such as accounting client, PMIP Client/MAG, etc triggers and completes the WiFi network exit procedure, including, stop accounting procedure and release mobility, security contexts, etc as per the above section 1.2.1.

After "retain time" value or due to some other reasons network MAY clean up the resources for the MS. The following network entities can initiate the Network Exit Procedure during Power save mode to perform Exit:

- AAA
- WIF or HA/LMA

These are as based on above sections 1.2.2 and 1.2.3

---

14. MS Implications

While in an active mode and connected to either WiMAX or WiFi access network, the Dual Mode WiMAX/WiFi device SHALL be able to pre-register and pre-authenticate on the alternate access technology (i.e. WiFi or WiMAX). This applies to both Dual Radio and Single Radio configuration.

For initial network access, the MS SHALL conduct the EAP Authentication procedure and SHALL store the resulting security context and its associated Security Parameter Indices (SPI) as the active one for the device.

During the pre-registration on the disparate access technology, the dual mode device SHALL generate a second security context associated with disparate access technology, and store it alongside the active security context.

For a Multi-Mode device, when specific security context expires due to its lifetime expiration or de-registration on one of the access technologies, the MS SHALL delete the expired context while retaining other valid contexts. For a Multi-Mode device, when the session is terminated, the MS SHALL delete all the related security contexts.

15. WiFi Access Network Requirements

<< This sections contains the implications on the WiFi Access Network >>

16. WIF Requirements

In order to assist AAA in generating a unique security context for each access technology using the same NAI, the WIF SHALL report its access type in the AAA Request message to the authenticating network.

For a Multi-Mode device, when the session is terminated, the related security context SHALL be deleted at the WIF

17. WiMAX ASN Requirements

In order to assist AAA in generating a unique security context for each access technology using the same NAI, the WiMAX ASN SHALL report its access type in the AAA Request message to the authenticating network.

For a Multi-Mode device, when the session is terminated, the related security context SHALL be deleted at the WiMAX ASN.

18. AAA Requirements and Implications

<<

In order to preserve the security context on the active serving network, the AAA SHALL generate a secod security context for the same device, one that is associated with the disparate access technology where pre-registartion and pre-autentication is performed based on the “FFS-NAS”reported by the NAS in the AAA Request. When the AAA receives the AAA Request message, it SHALL check the reported “FFS-NAS”and determine, based on the NAI, whether the request is for an initial network access or a pre-registration requiring additional security context for the device.

For initial network access, the AAA SHALL conduct the EAP Authentication procedure and SHALL store the resulting security context and its associated Security Parameter Indices (SPI) as the active one for the device.

During the pre-registration on the disparate access technology, the AAA SHALL create the second security context for the same session associated with the access technology on which the device has pre-registered.

If during active session the AAA receives the AAA Request from the same access technology associated with already exisiting security context i.e. same NAI and same access technology, the AAA SHALL conduct a Re-Authentication and SHALL replace the security context with the newly generated one.

If the AAA already has the security context for the device, but the AAA Request comes from the disparate access technlology, the AAA SHALL check the subscription record of the device to verify that the request is associated with the Multi-Mode device authorized for access from the target access technology, in which case the AAA SHALL conduct an EAP access pre-authentication. Upon successful completion of the EAP authentication, the AAA SHALL generate a second security context with its associated SPI(s) and SHALL store it alongside the active security context.

If the mobile is not authorized to access the disparate access technology, the AAA SHALL reject the AAA Request.

For a Multi-Mode device, when specific security context expires due to its lifetime expiration or de-registration on one of the access technologies, the AAA SHALL delete the expired context while retaining other valid contexts. For a Multi-Mode device, when the session is terminated, the AAA SHALL delete all related security contexts.

Editor Note: "FFS-NAS" will be identified by the Security subteam based on the procedures defined in the IETF (presently ambegious) to allocate NAS Port type

19. WiFi WiMAX Interworking Specific Messages and TLVs

<This section describes WiFi WiMAX IWK specific messages and TLVs>