WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Wi-Fi® – WiMAX® Interworking

WMF-T37-010-R016v01

WiMAX Forum® Approved

(2010-11-30)

WiMAX Forum Proprietary

TABLE OF CONTENTS

List of Figures

List of Tables

1. Introduction and Document Scope

This document specifies the reference model and procedures for interworking and roaming between Wi-Fi® and WiMAX® networks. The purpose of this document is to identify the requirements and impacts to the Wi-Fi access network and the WiMAX network to support the interworking and roaming functionality.

2. Abbreviations and Definitions

2.1 Abbreviations

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

AN	Access Network
CUI	Chargeable User Identity
DM	Dual Mode
IWK	Interworking
VSA	Vendor Specific Attributes
Wi-Fi®	Wireless Fidelity
WIF	Wi-Fi Interworking Function
WiMAX® SFF	WiMAX® Signal Forwarding Function
Wi-Fi SFF	Wi-Fi Signal Forwarding Function
WBA	Wireless Broadband Alliance
WPA™	Wi-Fi Protected Access®
WRIX	Wireless Roaming Intermediary eXchange
WISPr	Wireless ISP roaming

2.2 Terms & Definitions

Single Radio Handover: A Dual Mode terminal where *only a single radio is* transmitting 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.

Wi-Fi -WiMAX® Roaming: The ability for a Wi-Fi or WiMAX® subscriber to access services in a visited Wi-FiWi-Fi or WiMAX network different from the home network.

3. References

[1] WMF-T32-001-R016, WiMAX Forum® Network Architecture - Architecture Tenets, Reference Model and Reference Points – Base Specification

[2] WiMAX Forum® Mobile System Profile

[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 v1.05

[6] Wireless Broadband Alliance WRIX Standard Service Specification, Interconnect Definition v1.05

[7] Wireless Broadband Alliance WISPr 2.0, version 1.0

[8] IETF RFC 5176 [2008], Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

[9] IEEE Std 802.21-2009, Media Independent Handover Services

[10] WMF-T37-011-R016, WiMAX Forum® Network Architecture, Architecture, detailed Protocols and Procedures, Single Radio Interworking between Non-WiMAX and WiMAX Access Networks

[11] WMF-T33-001-R016, WiMAX Forum® Network Architecture “Detailed Protocols and Procedures, Base Specification"

[12] “Standard Connectivity Management Objects EAP Paramets, Version 1.0”. Open Mobile Alliance. OMA-DDS-DM_ConnMO_EAP-V1_0-20071017-D.doc. URL:http://www.openmobilealliance.org

4. General Requirements and Principles

This section defines the architectural principles and requirements for interworking and roaming between Wi-Fi and WiMAX® networks.

4.1 Requirements

4.1.1 Requirements for interworking between Wi-Fi and WiMAX®

- Common Billing for accessing Wi-Fi and WiMAX networks shall be supported. Wi-Fi 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 Wi-Fi systems shall be supported.
- Both single radio and dual radio handovers shall be supported.

4.1.2 Requirements for roaming between Wi-Fi and WiMAX®

- Separate Credentials

  Roaming between Wi-Fi and WiMAX networks shall be supported using separate credentials. The Wi-Fi and WiMAX subscribers use separate credentials in this case when accessing the visited network. This applies to both WISPr 1.0 and WISPr 2.0 based Wi-Fi networks.

  - The home WiMAX service provider may assign both WiMAX and Wi-Fi credentials. Separate Wi-Fi credentials are assigned to WiMAX subscribers for roaming to visited Wi-Fi networks.
  - The home Wi-Fi service provider assigns Wi-Fi credentials. The Wi-Fi subscribers use separate credentials assigned by visited WiMAX service provider for roaming to visited WiMAX networks.

  WISPr 1.0 based Wi-Fi networks do not support secure transport of credentials and hence it is better to have separate credentials for WISPr 1.0 based Wi-Fi networks. It is more appropriate for these Wi-Fi networks to be supported through use of separate Wi-Fi credentials issued by the WiMAX service provider. WISPr The subscriber is always authenticated in the home network and uses common credentials for accessing the visited network as well as the home network.

- Common Credentials

  Roaming between Wi-Fi and WiMAX networks may be supported using common credentials. Wi-Fi networks must support EAP based authentication for this to work. Non WPA™ based Wi-Fi networks may support EAP based authentication using WISPr 2.0. The subscriber is always authenticated in the home network and uses common credentials for accessing the visited network as when accessing the home network.

  - Wi-Fi subscriber roams to a visited WiMAX network and is authenticated by home Wi-Fi AAA based on Wi-Fi credentials.
  - WiMAX subscriber roams to a visited Wi-Fi network and is authenticated by home WiMAX AAA based on common credentials assigned by WiMAX network.

- Common Billing for accessing Wi-Fi and WiMAX networks shall be supported. Wi-Fi and WiMAX may use different credentials but the user may be provided with a consolidated bill.

5. Architecture Reference Model

5.1 Interworking Reference Model

Figure 6-1 represents the Wi-Fi-WiMAX® Interworking Network Reference Model (NRM). The Interworking NRM describes the case wherein either the same service provider deploys both Wi-Fi and WiMAX access networks, or these two networks are deployed by different service providers. In the latter case where Wi-Fi and WiMAX networks are deployed by different service providers, the two service providers are required to have a contractual agreement between them to enable co-coordinated network access.

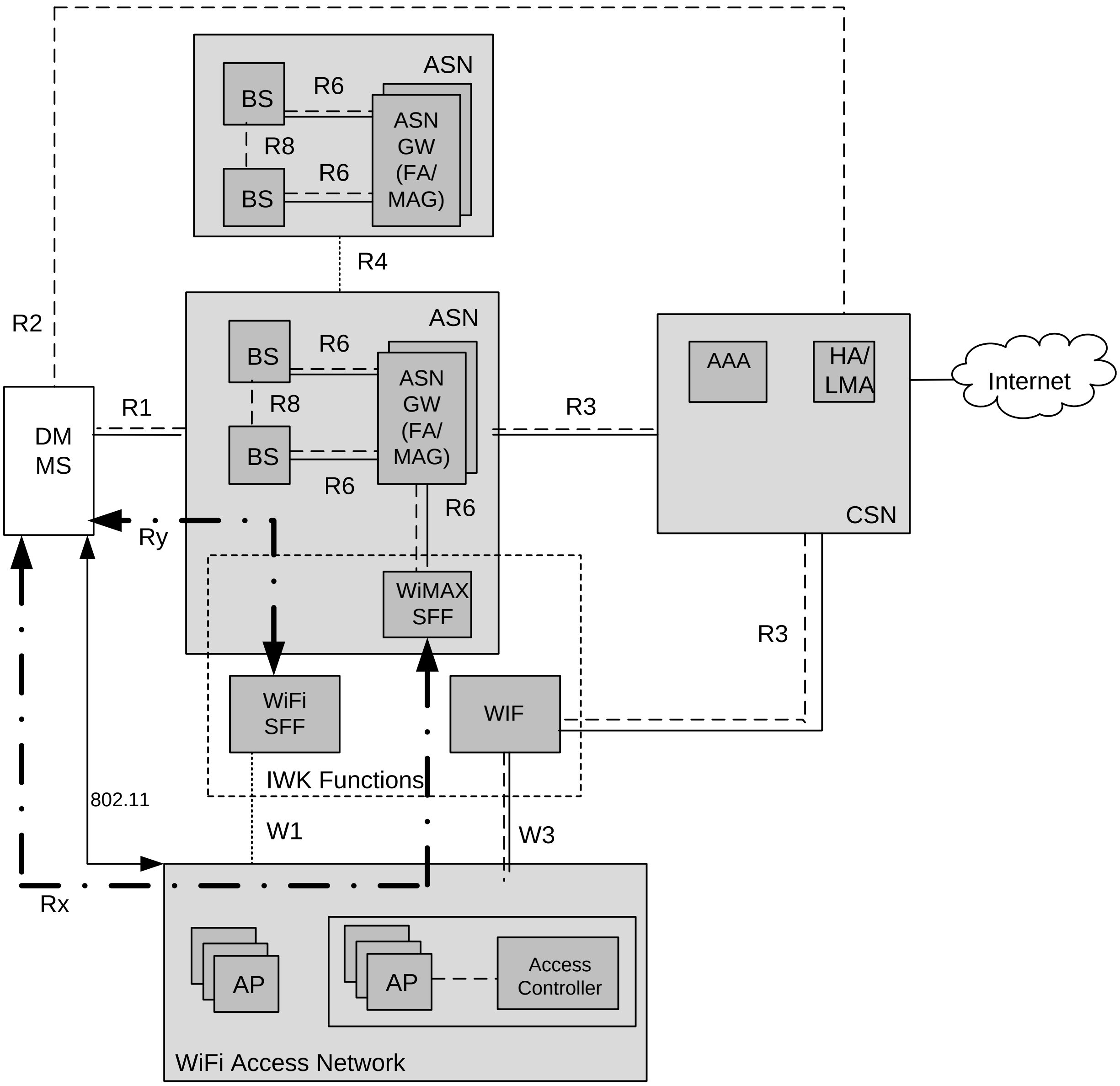


Figure 6-1 – Wi-Fi-WiMAX® Interworking Network Reference Model

The reference model introduces new logical entities called WiMAX SFF, Wi-Fi SFF and WIF, collectively labeled "Interworking Functions". The functional decomposition of the IWK Functions is shown in Figure 6-1 – Wi-Fi-WiMAX Interworking Network Reference ModelFigure 6-1. The IWK Functions consist of the following independent logical entities:

1. Wi-Fi Interworking Function (WIF).
2. WiMAX Signal Forwarding Function (SFF) used to support single radio handovers from Wi-Fi to WiMAX.
3. Wi-Fi Signal Forwarding Function (SFF) used to support single radio handovers from WiMAX to Wi-Fi.

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.

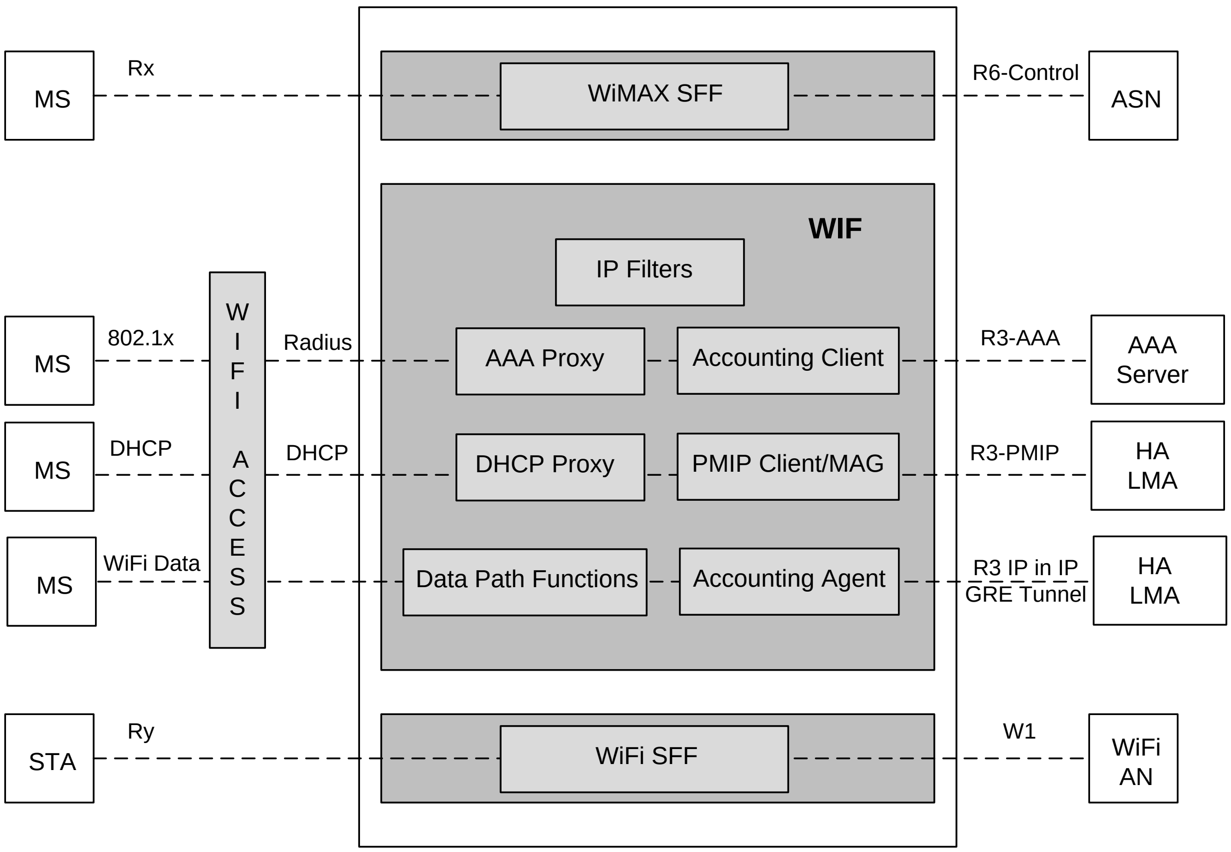


Figure 6-2 – Interworking Functions Decomposition

5.1.1 Wi-Fi Interworking Function (WIF)

The Wi-Fi Interworking Function enables the mobile device connected to the Wi-Fi 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 Wi-Fi traffic traversing the CSN
- Data Path Functions to create IP in IP or GRE tunnel
- IP Filters for filtering out IP packets from unauthorized Wi-Fi STAs

5.1.2 WiMAX® SFF

The WiMAX Signal Forwarding Function enables single radio handovers from Wi-Fi 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 handover, the WiMAX SFF may or may not be be collocated in the new serving ASN.

5.1.3 Wi-Fi SFF

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

5.2 Interworking Reference Points

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

5.2.1 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.

5.2.2 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 Wi-Fi to WiMAX. These messages are transferred over the Wi-Fi access network and maybe routed through the WiMAX CSN.

5.2.3 Reference Point Ry

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

5.2.4 Reference Point W1

Reference Point W1 is between the Wi-Fi SFF and the Wi-Fi access network. Wi-Fi SFF forwards messages to the Wi-Fi access network through this reference point.

5.2.5 Reference Point W3

Reference Point W3 consists of control plane protocols between Wi-Fi access network and Wi-Fi 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 Wi-Fi access network and WIF.

5.3 Roaming Scenarios

The following scenarios are covered for Wi-Fi-WiMAX® roaming.

5.3.1 Visited Wi-Fi Access Network

5.3.1.1 Visited Wi-Fi Access Network (802.1X enabled) to Home WiMAX CSN

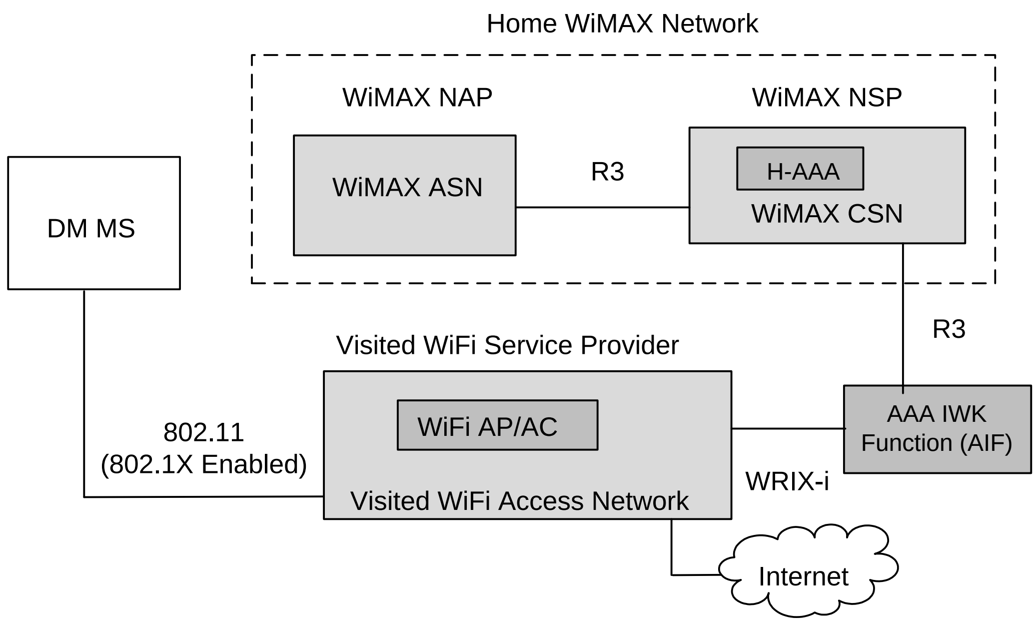


Figure 6-3 – Roaming from Visited Wi-Fi Access Network (802.1X enabled) to Home WiMAX® CSN

In this case, the WiMAX subscriber gains access to the internet using WiMAX subscription via an 802.1X enabled Wi-Fi access network. The MS needs to use the same EAP methods that are supported by the WiMAX home network. The WiMAX network detects that the MS is roaming through visited Wi-Fi that is 802.1X enabled and suggests the appropriate EAP method (EAP-TTLS). The visited Wi-Fi service provider has a roaming agreement with the home WiMAX Network Service Provider. The WiMAX H-AAA authenticates the user. The AAA IWK Function (AIF) provides the interworking functionality between H-AAA and the Wi-Fi network and converts the WRIX-i RADIUS protocol to WiMAX R3 protocol.

The WiMAX subscriber uses common credentials in this case, i.e. the same set of credentials for accessing the visited Wi-Fi network as when accessing the home WiMAX network. The WiMAX subscriber uses MSCHAPv2 (the user credentials i.eusername and password) for inner method of EAP-TTLS.

The subscriber may not be able to access the WiMAX private device certificate and use the WiMAX MAC address when roaming through visited Wi-Fi access network. This is applicable when the subscriber is using separate Wi-Fi and WiMAX modems as they would have different MAC addresses in this case. This limits the use of EAP TLS. It may be possible to overcome these limitations when the subscriber uses a combo Wi-Fi and WiMAX modem with common MAC address. In such cases EAP TLS may be used suitably.

5.3.1.2 Visited Wi-Fi Access Network (non-802.1X enabled) to Home WiMAX CSN

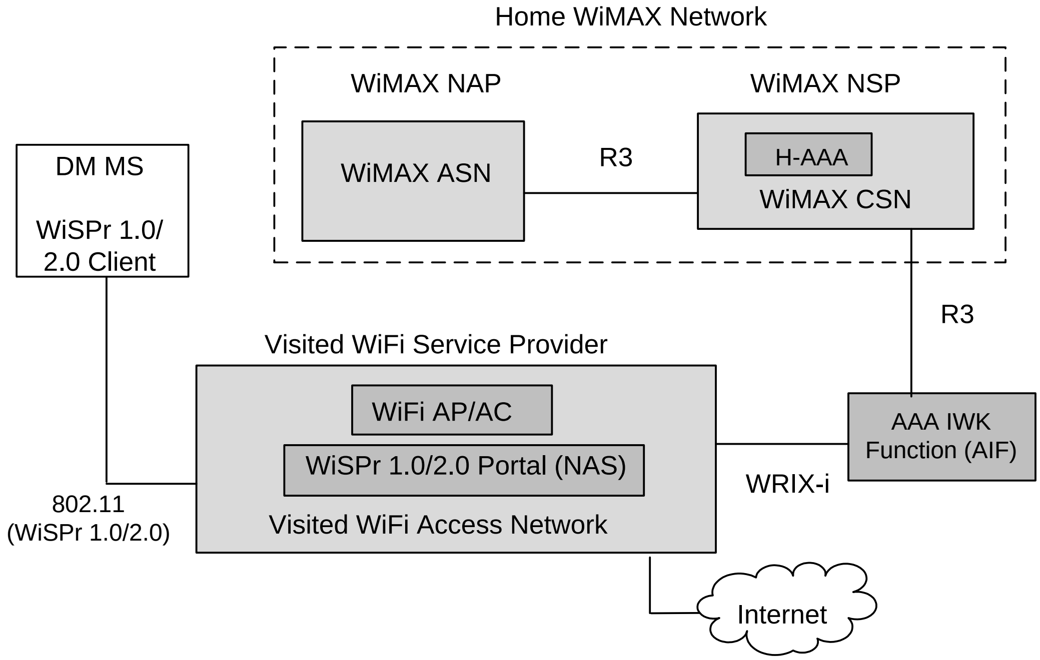


Figure 6-4 – Roaming from Visited Wi-Fi Access Network (WISPr enabled) to Home WiMAX® CSN

In this case, a WiMAX subscriber gains access to the internet using WiMAX subscription via a WISPr 1.0 or WISPr 2.0 enabled Wi-Fi access network. The visited Wi-Fi service provider has a roaming agreement with the home WiMAX Network Service Provider. The WiMAX H-AAA authenticates the user. The AAA IWK Function (AIF) provides the interworking functionality between H-AAA and the Wi-Fi network which uses the WRIX-i RADIUS protocol. The AAA IWK unction (AIF) converts the WRIX-i RADIUS protocol to WiMAX R3 protocol.

The Username-Password is transported to the Wi-Fi network using WISPr 1.0 or WISPr 2.0. The Wi-Fi access network then initiates EAP-TTLS which is not mutually authenticated (since the Wi-Fi network doesn't have WiMAX device credential) and contains the Username Password in phase 2 of the EAP-TTLS. The credentials are used as follows in case of WISPr 1.0 or WISPr 2.0 based networks.

- WISPr 1.0 based Wi-Fi Networks: In this case the WiMAX subscriber uses separate credentials assigned by the WiMAX service provider to access the visited Wi-Fi access network. The separate set of credentials would need to be provisioned into the mobile device by the WiMAX service provider.
- WISPr 2.0 based Wi-Fi Networks: In this case the WiMAX subscriber may use separate or common credentials. The separate set of credentials would be assigned by the WiMAX service provider and may be provisioned into the mobile device by the WiMAX service provider. When using common credentials, the WiMAX subscriber uses the user credentials (Username/Password) assigned by the WiMAX service provider.

The subscriber may not be able to access the WiMAX private device certificate and use the WiMAX MAC address when roaming through visited Wi-Fi access network. This is applicable when he subscriber is using separate Wi-Fi and WiMAX modems as they would have different MAC addresses in this case. This limits the use of EAP TLS. It may be possible to overcome these limitations when the subscriber uses a combo Wi-Fi and WiMAX modem with common MAC address. In such cases EAP TLS may be used suitably.

5.3.2 Visited WiMAX® Access Network to Home Wi-Fi

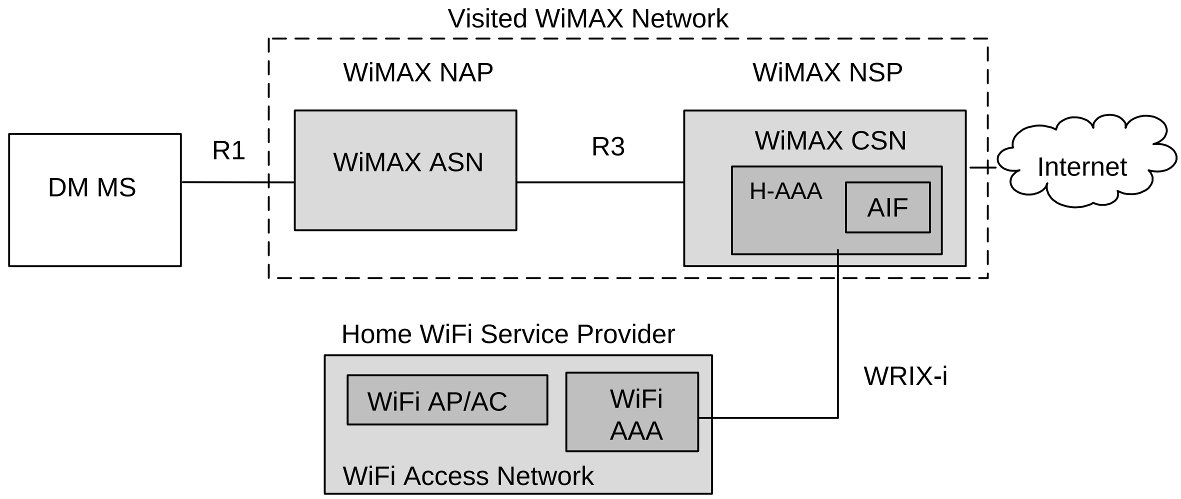


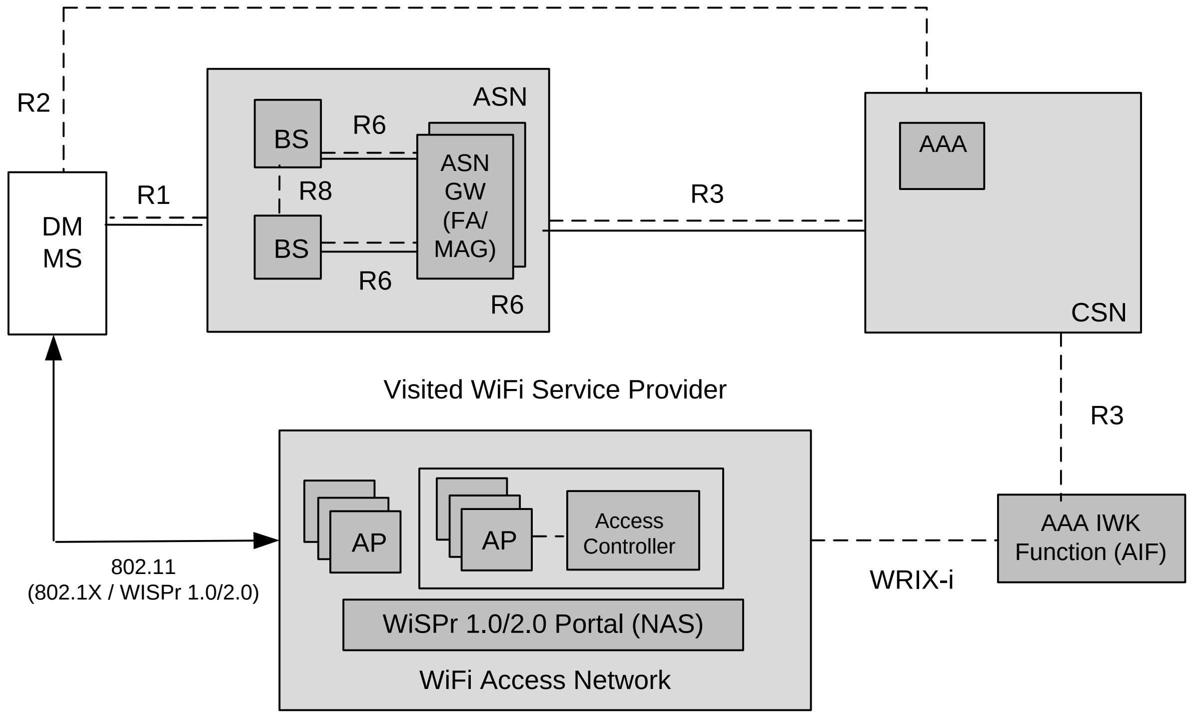
Figure 6-5 – Roaming from Visited WiMAX® Access Network to Home Wi-Fi Network

In this case, a Wi-Fi subscriber gains access to the internet using his Wi-Fi subscription via a WiMAX access network. The WiMAX Network Service Provider has a roaming agreement with the home Wi-Fi service provider. The Wi-Fi AAA authenticates the user. The AAA IWK unction (AIF) provides the interworking functionality between WiMAX H-AAA and the Wi-Fi AAA using the WRIX-i RADIUS protocol. The AIF is in the WiMAX CSN and acts as H-AAA since it terminates the TTLS tunnel and manages the security keys.

The Wi-Fi subscriber uses credentials assigned by the WiMAX service provider and uses EAP TTLS with PAP. This is because the home Wi-Fi network can only support PAP. In this case EAP-TTLS is used as follows:

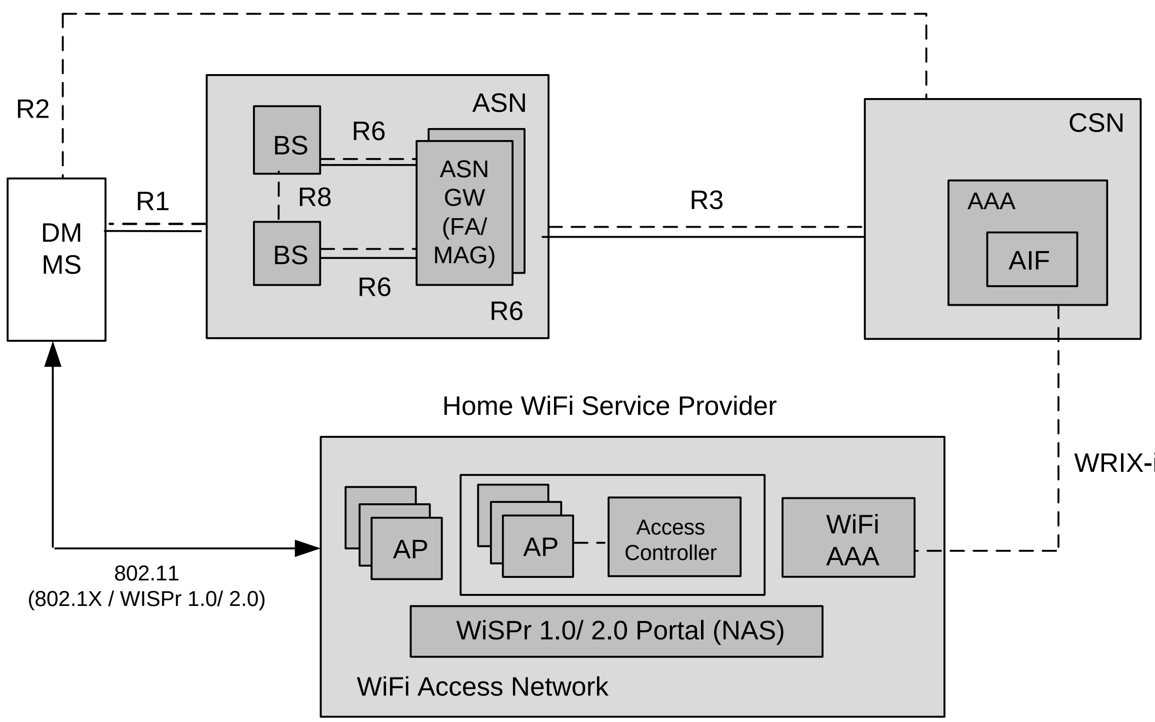
- Outer method contains the WIMAX Device credential.
- Inner method is passed to the Wi-Fi Home operator using WRIX-i. The inner method could contain any Wi-Fi specific method of authentication including username password or even an 802.1x method such as EAP-PEAP.

5.4 Roaming Reference Model



1

2 **Figure 6-6 – Wi-Fi-WiMAX® Roaming Network Reference Model for Visited Wi-Fi**



3

4 **Figure 6-7 – Wi-Fi-WiMAX® Roaming Network Reference Model for Visited WiMAX®**

Figure 6-6 represents the Wi-Fi-WiMAX Roaming Network Reference Model (NRM) for visited Wi-Fi case. Figure 6-7 represents the Wi-Fi-WiMAX Roaming Network Reference Model (NRM) for visited WiMAX case. The NRM describes the case wherein the Wi-Fi and WiMAX networks are deployed by different service providers and the two service providers have roaming agreement between them. The Wi-Fi access network supports EAP based authentication and is 802.1X or WISPr 1.0/2.0 enabled. The reference model introduces a new logical entity called AAA Interworking Function (AIF).

5.4.1 AAA Interworking Function (AIF)

The AAA IWK unction (AIF) is a logical entity and provides the interworking functionality between the WiMAX AAA and the Wi-Fi AAA. The Wi-Fi AAA uses the WRIX-i (RADIUS) protocol.

5.4.2 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) Wi-Fi networks to perform EAP based authentication. The dual mode mobile device needs a WISPr2.0 client implementation and the Wi-Fi 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. However the Wi-Fi AP operates in open mode in this case and user traffic is not encrypted.
Further details about WISPr can be found in [3]. WISPr 2.0 has no impact on WiMAX networks.

5.4.3 Wireless Roaming Intermediary Exchange (WRIX)

For accessing open Wi-Fi networks the WBA has specified a common settlement and roaming specifications called WRIX. WRIX provides an independent functional module to provide centralized aggregation adaptation between Wi-Fi roaming partners. WRIX provides several interfaces. The WRIX-i interface is used for RADIUS interconnection.

5.5 Interworking and Roaming Reference Model

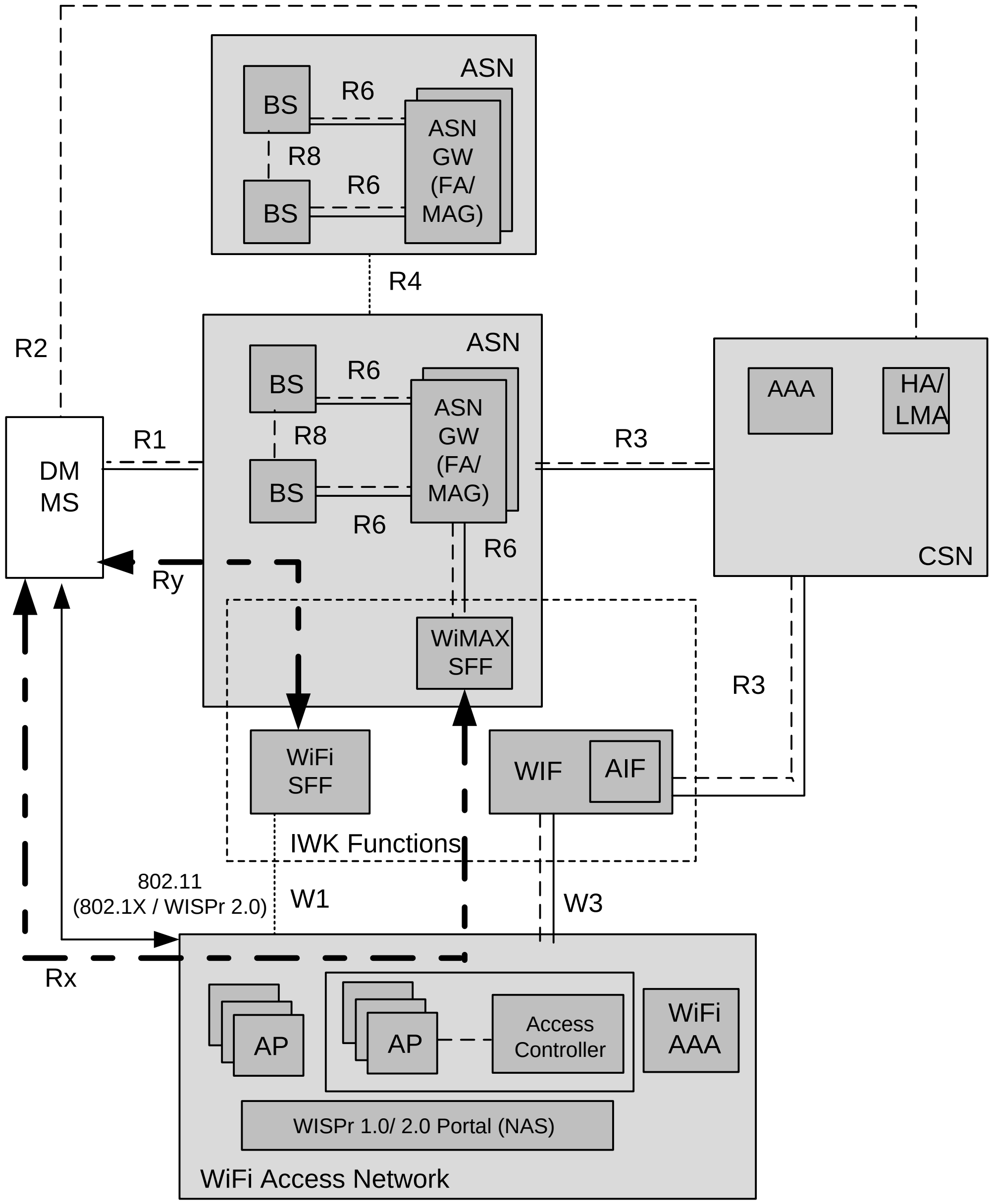


Figure 6-8 – Wi-Fi-WiMAX® Interworking and Roaming Network Reference Model for Visited Wi-Fi

Figure 6-8 represents the combined Wi-Fi-WiMAX Interworking and Roaming Network Reference Model (NRM). The NRM describes the case wherein the Wi-Fi 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 coordinated access between them. The Roaming functionality by itself only provides nomadic access (no IP session continuity) whereas the IWK Function provides IP Session continuity during handovers. Irrespective of whether WiMAX is the home or visited network the key distribution to the HA/LMA has to be provided by the WiMAX AAA.

6. Access Network Discovery and Selection

6.1 Access Network Discovery and Selection Principles

The following principles apply for network discovery and selection when the dual mode Wi-Fi-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 access networks in the 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.

6.2 Architecture for Access Network Discovery and Selection

The Access Network Discovery and Selection is based on the Media Independent Information Service (MIIS) defined in [9]. Below Figure 7-1 shows the architecture for Access Network Discovery and Selection.

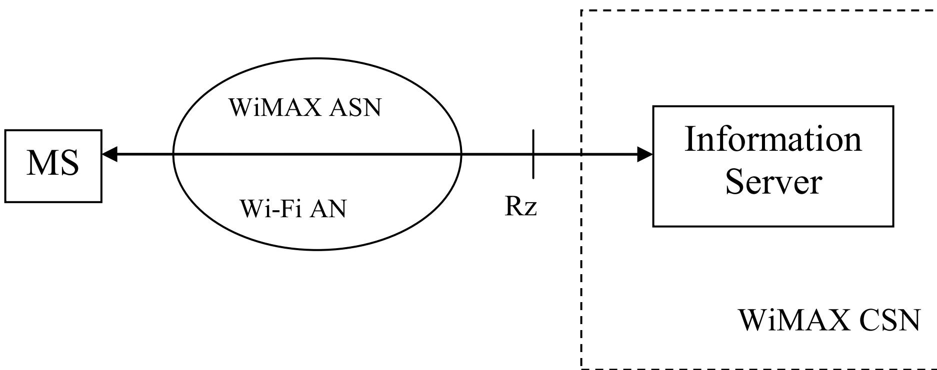


Figure 7-1 – Architecture for Access Network Discovery and Selection

6.2.1 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 and the SFF information. This is as per operator policies. The Information 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.

6.2.2 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 Server may use UDP transport protocol for information exchange.

6.3 Access Network Discovery and Selection procedure

The Network Discovery and Selection procedure is based on MIH protocol defined in [9]. 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:

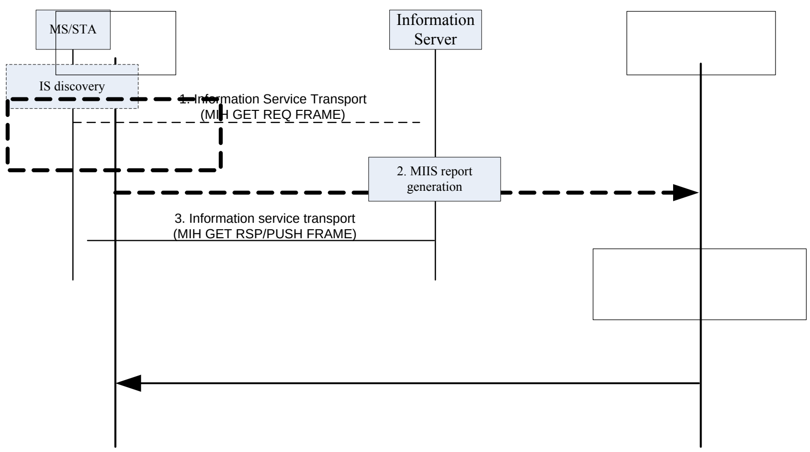


Figure 7-2 – Call flow of network discovery and selection

As indicated in Figure 7-1 the Information Server (IS) is located in the WiMAX® CSN. The MS/STA can access the IS either from the WiMAX network or from the visited Wi-Fi 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: The MS/STA may send a MIH_Get_Information request to the IS to query the information of available access networks. This message may include the MS/STA's location information, a list of link types or identities of access networks.

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

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

6.4 Interworking Function Discovery

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

The Wi-Fi access network may provide multiple connectivity options. One of the options may be to use WiMAX® interworking while there may be other options to connect to Wi-Fi network in conventional ways. The Wi-Fi access network can provide this distinction by the use of suitable SSIDs. The Wi-Fi network may deploy virtual APs with multiple SSIDs. If the Wi-Fi 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 Wi-Fi access. If the Wi-Fi access provides WiMAX interworking by default (as the only option to connect) then there is no need for virtual APs or multiple SSIDs.

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

6.5 Network Discovery and Selection during Handovers

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

6.5.1 Handovers from WiMAX® to Wi-Fi

The MS may discover suitable Wi-Fi network through query-response procedure with Information Server or periodic scanning. The MS may decide to handover to Wi-Fi 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 Wi-Fi 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 Wi-Fi SFF. After handover to Wi-Fi 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 Wi-Fi coverage degrades abruptly.

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

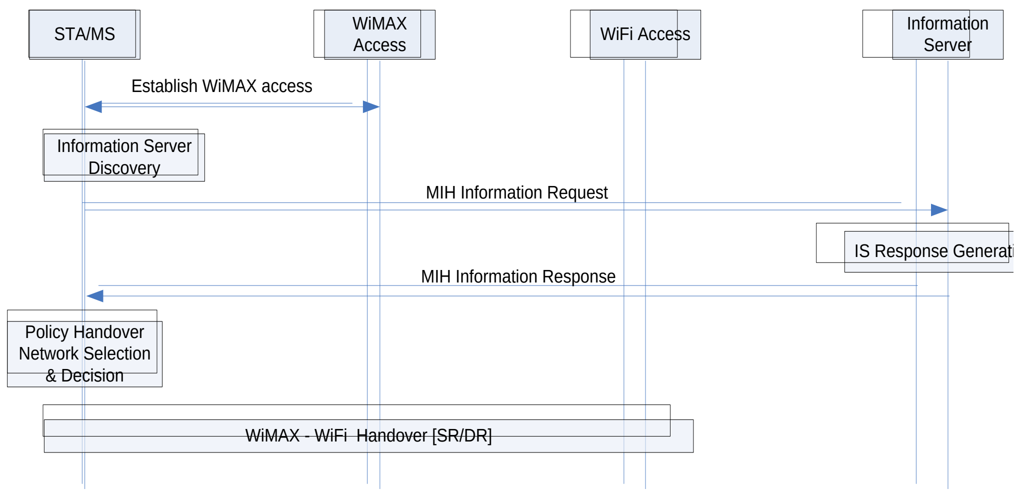


Figure 7-3 – WiMAX® to Wi-Fi HO facilitated by IS

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 (Wi-Fi network in this case) for handover based on the operator policies.

6.5.2 Handovers from Wi-Fi to WiMAX®

The mobile device needs to connect to the Wi-Fi 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 Wi-Fi, 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 Wi-Fi 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 Wi-Fi to WiMAX.

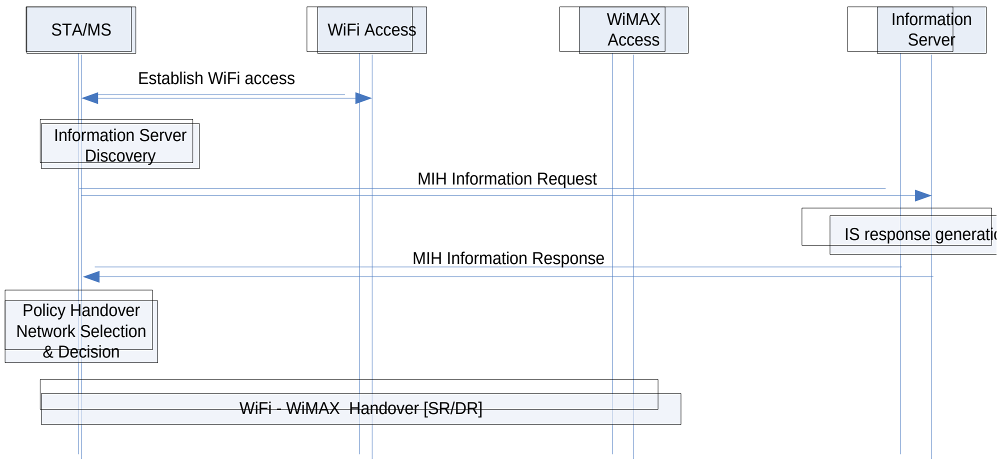


Figure 7-4 – Wi-Fi to WiMAX® HO facilitated by IS

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.

6.6 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.

For reference to 802.21 IE(s) please refer to [9].

Additional IEs may be added like

- Signal Forwarding Function (SFF)
- Data rate supported by the link layer of the access network
- Roaming Policies
- Roaming partners

7. Subscription and Provisioning

7.1 Deployment scenarios

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

7.1.1 Single Subscription

In this scenario the dual mode device maintains a single subscription with either WiMAX® or Wi-Fi 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 Wi-Fi network.

If subscription is maintained with the Wi-Fi network, the dual mode device can access the Wi-Fi services either directly, by connecting through the Wi-Fi access network, or indirectly, by connecting through the WiMAX access to the services offered by the WiMAX network with the subscriber authentication and authorization of the Wi-Fi 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 Wi-Fi AAA, which maintains the single Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi AAA.

As a result of successful subscription authentication the Wi-Fi AAA authorizes the WiMAX services.

7.1.2 Dual Subscription

The dual radio MS/STA may maintain two independent subscriptions and therefore two independent sets of credentials: one set with the Wi-Fi 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 Wi-Fi AAA , i.e. the WiMAX AAA contains the WiMAX subscription record associated with MS NAI, and the Wi-Fi AAA may contain records associated with just user name and password. In this case, an interface between the WiMAX AAA and the Wi-Fi AAA is not required.

7.2 IP Services

7.2.1 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 Wi-Fi subscription.

7.2.2 Dual Subscription Case:

Simple IP services can be provided by the Wi-Fi or the WiMAX networks. Mobile IP services can only be provided by the WiMAX CSN since placement of HA in the Wi-Fi 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.

7.3 Provisioning Wi-Fi Credentials for Dual mode Module

7.3.1 Introduction

The WiMAX® Supplementary object is used to provision Wi-Fi credentials for dual mode module. The operator may provision Wi-Fi subscription information as part as the WiMAX subscription. The Wi-Fi credentials are transferred to a WISPr client that resides on a Wi-Fi device to be used. The Wi-Fi networks are detected based on SSIDs and are presented to the user as valid or invalid scenarios. The mapping between the Wi-Fi aggregator and the supported Wi-Fi networks is the responsibility of the WISPr client. The WISPr Client identifies the Wi-Fi operator based on the REALM and automatically maps the user credentials to the correct list of SSIDs. For further details on WiMAX Supplementary MO please refer to (OTA-OMA-DM A10 - http://members.wimaxforum.org/apps/org/workgroup/nwg/download.php/49072/latest)

Provisioning Wi-Fi credentials for single mode modules is out of scope.

7.3.2 Graphical Representation

Figure 8-1 provides the updated structure of WiMAX Supplementary MO. A new leaf called as Wi-Fi Subscription is added.

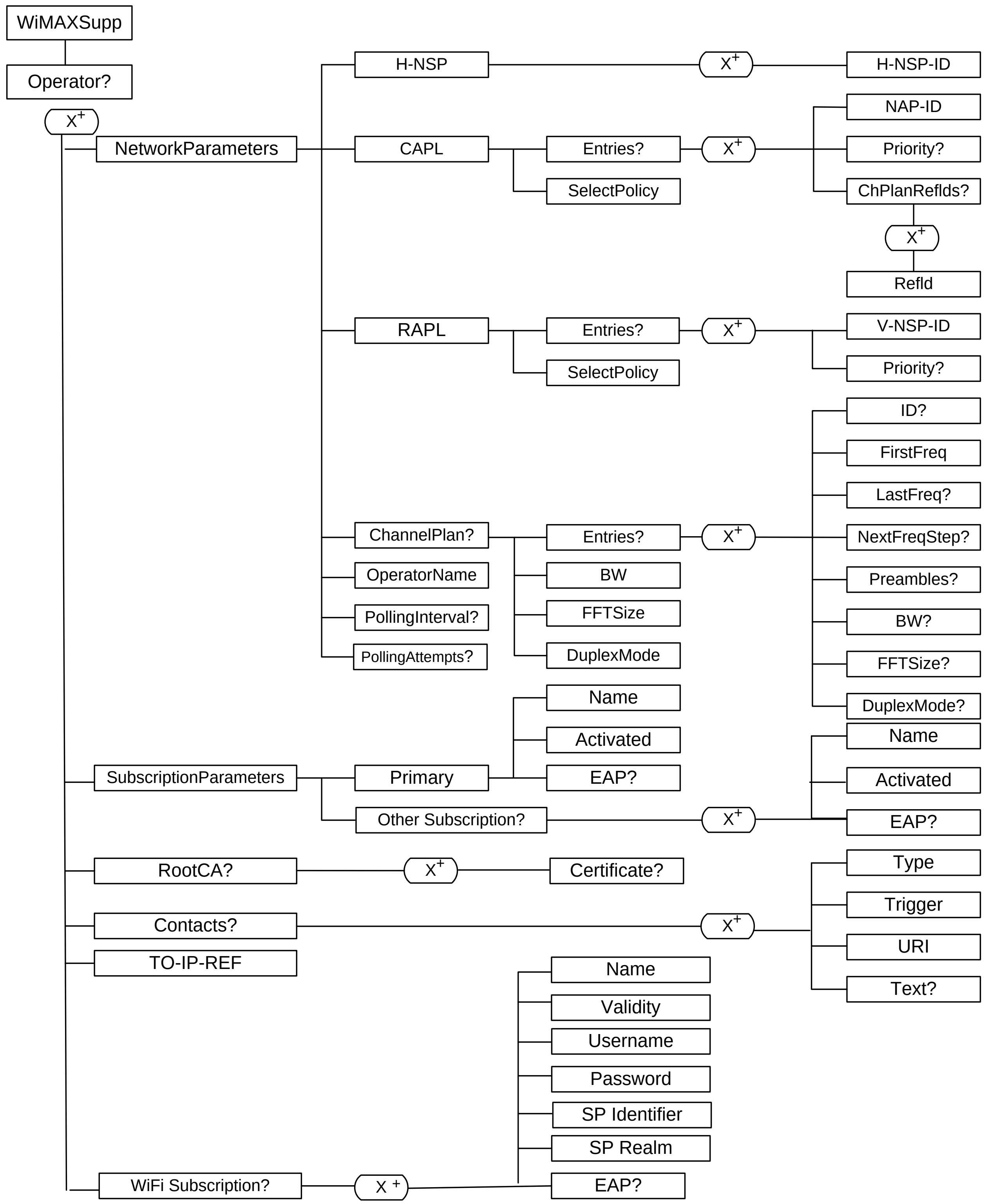


Figure 8-1 – WiMAX® Supplementary Management Object

7.3.2.1 Wi-Fi Subscription Node

The Wi-Fi Subscription interior node contains information associated with Wi-Fi subscription. A user is allowed to have more than one Wi-Fi subscription with an operator. This node enables a user and the operators to manage authentication parameters that are associated with user's subscriptions. The decision of which subscription parameters are used during network entry authentication is out of the scope of this specification.

7.3.2.1.1 WiMAXSupp/Operator/<X>/Wi-FiSubscription/

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the subscription parameters. See Section 8.3.2.1.2.1 for further details.

7.3.2.1.2 Wi-Fi Subscription parameters

This interior node contains the Wi-Fi subscriber parameters.

7.3.2.1.2.1 WiMAXSupp/Operator/<X>/Wi-FiSubscription/Name

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies the human readable name of the subscriber. The operator SHALL assure the human readable name of the subscriber is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

The MIME type of the node SHALL be 'text/plain; charset=utf-8'. The maximum length SHALL be 255 bytes. In UTF-8 format, each character MAY take one to four bytes.

7.3.2.1.2.2 WiMAXSupp/Operator/<X>/Wi-FiSubscription/Primary/Validity

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get, Replace

This leaf node indicates the provisioning status of the Subscriber. If the value of the node is FALSE, the device SHALL enter the network in the provisioning mode when using primary subscription, by providing a <*WiMAXdecoratedNAI*> during the EAP negotiation that indicates the provisioning service mode. Upon completion of the provisioning phase, the OMA DM server SHALL set the value to TRUE to indicate that the device SHALL use regular network entry using the provisioned parameters. As long as this leaf node value is true, all provisioned parameters should be considered by the device as the most updated parameters hence the device should first use the provisioned operator name and subscription parameters for its normal operation and only afterwards can use other alternative sources for the same parameters, if needed, such as 802.16 MAC messages. This node SHALL be included into the last OMA DM Package message from the Device Management Server to the device. When this node is sent to the device, it is able to know that all configurations are uploaded to the device.

The point of time when the OMA-Session, in which this node was set, was completed is considered as the completion point of provisioning phase by the device. (If the device needs to trigger something at the end of activation, it will use this point as the trigger).

7.3.2.1.2.3 WiMAXSupp/Operator/<X>/Wi-FiSubscription/Username

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies the username of the subscriber for authentication. The operator SHALL ensure that the username of the subscriber is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

7.3.2.1.2.4 WiMAXSupp/Operator/<X>/Wi-FiSubscription/Password

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies the password of the subscriber.

7.3.2.1.2.5 WiMAXSupp/Operator/<X>/Wi-FiSubscription/ServiceProviderIdentifier

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Replace

This leaf node specifies the human readable identifier of the Wi-Fi service provider (could be SSID as well).

7.3.2.1.2.6 WiMAXSupp/Operator/<X>/Wi-FiSubscription/ServiceProviderRealm

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Chr	Get, Replace

This leaf node specifies the realm of the Wi-Fi service provider. The Wi-Fi service provider can be identified by the REALM.

7.3.2.1.2.7 WiMAXSupp/Operator/<X>/Wi-FiSubscription/EAP

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

The EAP interior node contains parameters for EAP authentication methods. It contains EAP MO as specified in [12]. Only a single EAP method is allowed to be configured for the MS to use with a specific operator. In the case it is a tunneled method (such as TTLS): the definition shall include the outer and the inner method nodes. In case EAP node is not populated, authentication is not performed.

8. Roaming

This section describes roaming procedures between Wi-Fi and WiMAX®.

8.1 Authentication

8.1.1 Separate Credentials

In this case the subscriber has separate set of credentials for accessing the two networks.

The WiMAX® service provider assigns the user another set of credentials that can be used with Wi-Fi networks. In this case the user uses WiMAX credentials to access WiMAX networks and the separately issued Wi-Fi credentials for accessing Wi-Fi networks.

The Wi-Fi subscribers use separate credentials assigned by WiMAX service provider for accessing the visited WiMAX networks.

8.1.2 Common Credentials

In this case the user has single set of credentials. The Wi-Fi subscriber only has Wi-Fi credentials and the WiMAX subscriber only has WiMAX credentials.

The private key of the WiMAX device certificate is available only to the WiMAX module. The Wi-Fi module cannot access the WiMAX device certificate. The Wi-Fi and WiMAX modules may have different MAC addresses. As such the WiMAX device certificate cannot be used for Wi-Fi authentication. Hence WiMAX user credentials will be used for authentication in this case. The following EAP methods should be used.

- WiMAX subscriber roaming to Visited Wi-Fi network
  - EAP TTLS with MS CHAP v2.
- Wi-Fi subscriber roaming to Visited WiMAX network
  - EAP TTLS with PAP

The subscriber may not be able to access the WiMAX private device certificate and use the WiMAX MAC address when roaming through visited Wi-Fi. This is applicable when he subscriber is using separate Wi-Fi and WiMAX modems as they would have different MAC addresses in this case. This limits the use of EAP TLS. It may be possible to overcome these limitations when the subscriber uses a combo Wi-Fi and WiMAX modem with common MAC address. In such cases EAP TLS may be used suitably.

8.2 Roaming from Visited Wi-Fi to Home WiMAX®

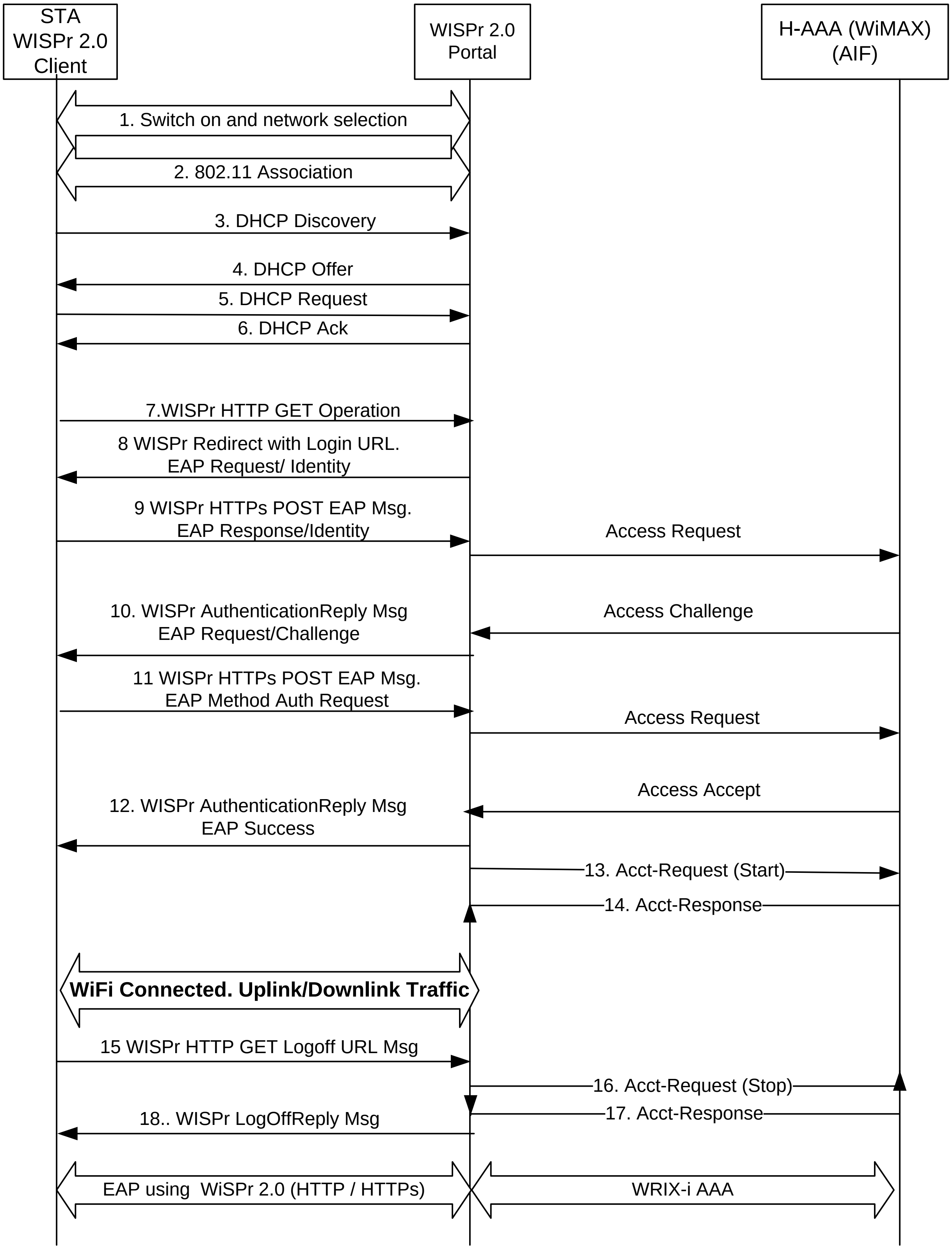
In this roaming scenario the WiMAX® subscriber uses the Wi-Fi access network to gain access to the IP services based on WiMAX subscription. The usage scenarios for this case are already described in 6.3.

8.2.1 Roaming from WISPr 1.0 enabled Visited Wi-Fi

In this case the WiMAX subscriber uses separate Wi-Fi specific credentials to roam to the visited Wi-Fi network (WISPr 1.0 based). Please refer to WISPr 1.0 document for more details.

8.2.2 Roaming from WISPr 2.0 enabled Visited Wi-Fi

In this case the WiMAX subscriber uses common credentials to roam to the visited Wi-Fi network (WISPr 2.0 based).



1

2 **Figure 9-1 – Roaming with Visited Wi-Fi (WISPr 2.0 based) and Home WiMAX®**

3

The WISPr 2.0 protocol is implemented using a mix of unsecure and secure HTTP transactions. WISPr 2.0 transactions are always initiated by the client. The client passes parameters to WISPr Portal in the access gateway using HTTP Request. The WISPr Portal responds to these requests and sends parameters back in HTTP response.

1. The Wi-Fi STA is switched on, and captures Wi-Fi signaling and then performs network discovery and selection.
2. The STA establishes Association with the Wi-Fi AN.
3. The STA uses DHCP to get an IP address in steps 3-6. The Wi-Fi AN is operating in open authentication mode.
7. The WISPr client uses unsecure HTTP GET to initiate the WISPr protocol. The URL used in the HTTP GET is referred to as the "Arbitrary URL". The Arbitrary URL may contain a hostname or IP Address, a port and query parameters and complies with RFC 2936 and RFC 2616. This is the only way to trigger the WISPr protocol.
8. The WISPr portal in the access gateway responds with a Redirect message. If the access gateway supports EAP over WISPr, the response contains the <EAPMsg> element which contains the encoded EAP Identity Request. The Redirect message also includes the <loginURL> parameter that the client may use subsequently for authentication.
9. The client sends a WISPr POST EAP message and requests authentication by including the encoded EAP Response Identity message. The Wi-Fi access network uses the WRIX-i specification to generate RADIUS Access request message. The Wi-Fi AAA sends the RADIUS Access Request message as per WRIX-i specification to the AAA IWK Function. The AAA IWK Function (AIF) converts the RADIUS message from WRIX-i specification to WiMAX-R3 RADIUS message and sends the WiMAX R3 RADIUS message to the Home-AAA in the WiMAX CSN. The AIF inserts appropriate attributes in the EAP Access Request message so that the WiMAX AAA can recognize that this is a WiMAX user roaming through a visited Wi-Fi network.
10. The WiMAX AAA sends a RADIUS Access Challenge message as per WiMAX-R3 to the AIF. The AIF converts this message to the RADIUS access Challenge as per the WRIX-i specification and sends it to the Wi-Fi access network. The WISPr portal receives this message and sends a WISPr Authentication Reply message which contains the <EAPMsg> parameter encoded as the RADIUS Access Challenge message.
11. The client sends a WISPr POST EAP message and initiates the EAP method to execute (EAP TTLS without device certificate or EAP AKA).
12. On successful authentication by the H-NSP, the WiMAX AAA sends a EAP Success message as per WiMAX R3 to the AIF which then converts this to WRIX-i RADIUS message. This is included in the WISPr Authentication Reply (EAP Success). The WISPr portal includes the <logoffURL> parameter as well which is subsequently used to terminate the session. The appropriate accounting mode is selected as per the WiMAX capability attribute as well.
13. Start Accounting Request
14. Start Accounting Response
15. The client sends an unsecure WISPr HTTP GET (Logoff URL) request to terminate the session.
16. Stop Accounting request
17. Stop Accounting Response
18. The WISPr portal responds with a WISPr Logoff Reply Message.

8.2.3 Roaming from 802.1x enabled Visited Wi-Fi

In this case the Wi-Fi access network is 802.1x enabled and supports EAP methods natively. EAP messages are carried over the 802.11 air interface and the procedure is the same as network entry for 802.1x based Wi-Fi network. The flow is very similar to that described in clause 9.3.2.

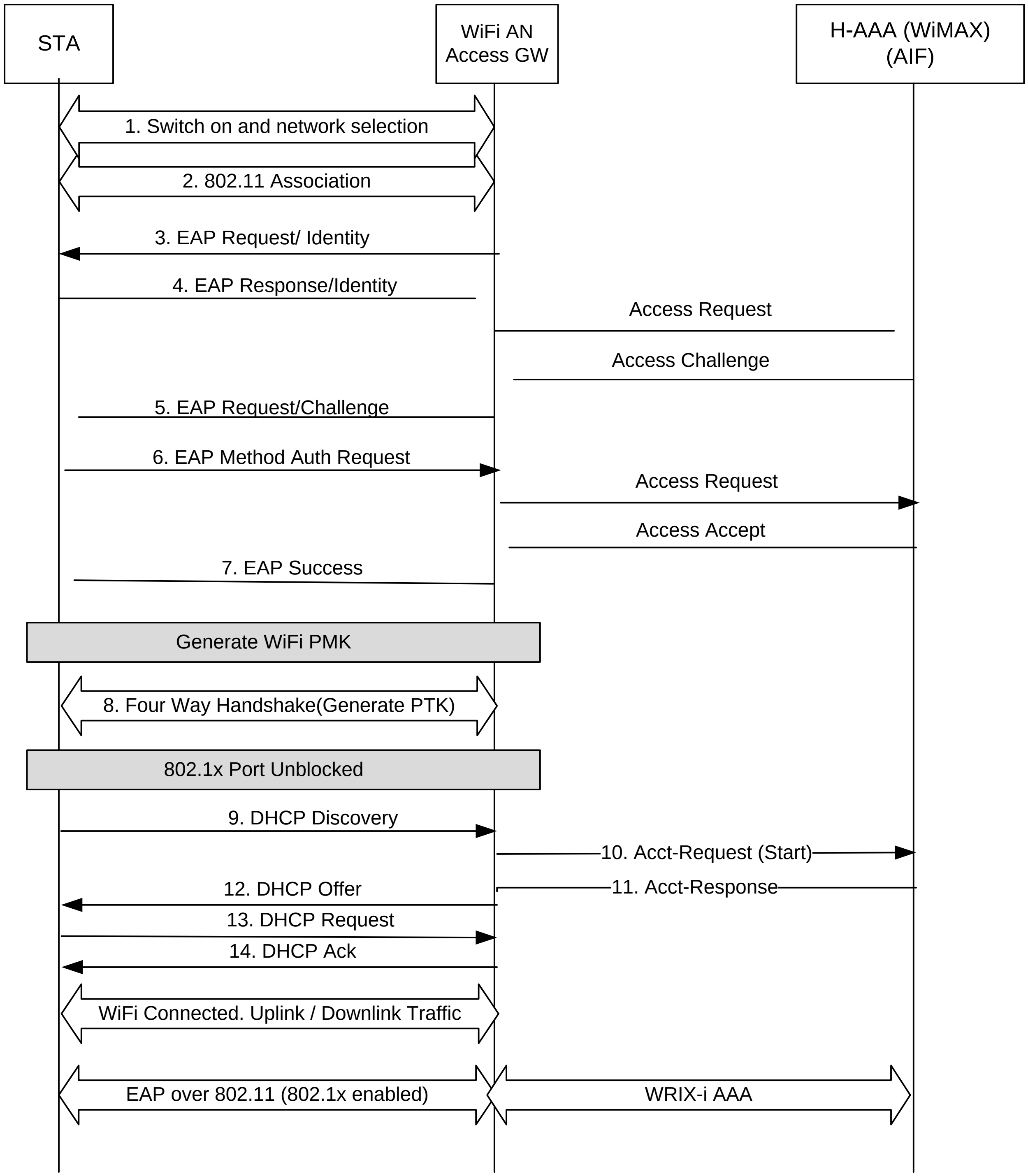


Figure 9-2 – Roaming with Visited Wi-Fi (802.1x based) and Home WiMAX®

8.3 Roaming from Visited WiMAX® to Home Wi-Fi

In this roaming scenario the Wi-Fi subscriber uses the WiMAX access network to gain access to services based on Wi-Fi subscription. The usage scenarios for this case are already described in 6.3. The EAP messages are carried over the 802.16 air interface and the AIF performs appropriate conversion (WiMAX to Wi-Fi) similar to the call flow as described in Figure 9-3

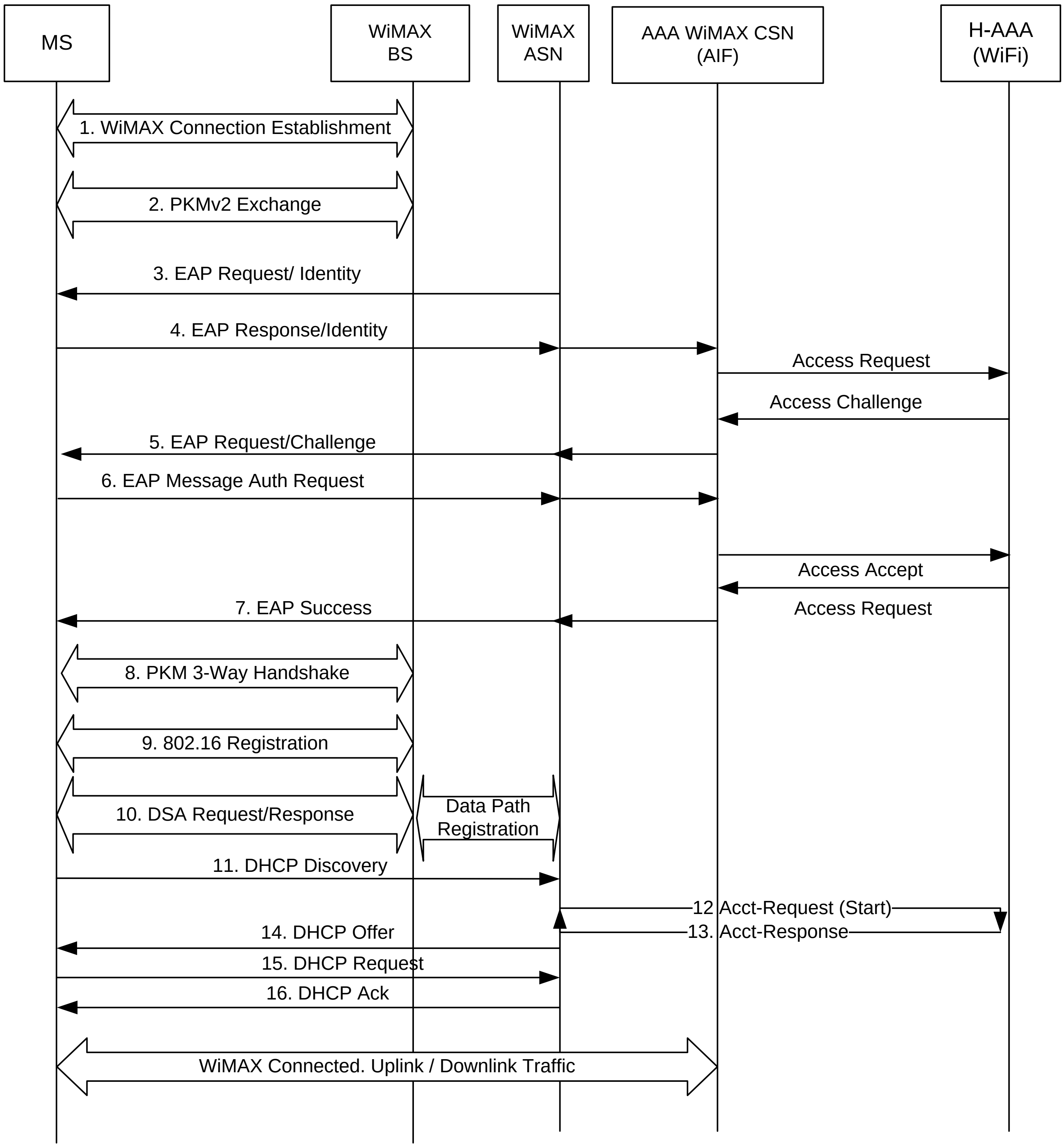


Figure 9-3 – Roaming with Visited WiMAX® and Home Wi-Fi

9. Authentication and Security

While in an active mode and connected to either WiMAX® or Wi-Fi access network, the Dual Mode WiMAX/Wi-Fi device can pre-register and pre-authenticate on the alternate access technology (i.e. Wi-Fi 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 second security context for the same device, one that is associated with the disparate access technology where pre-registration and pre-authentication is performed.

When the MS connects using any access network the combination of NAI, the client MAC address, and the access technology type are used by the MS to identify the network session. If any of these parameters change, it is considered a different network session. For example, the same NAI and MAC address can be used by both Wi-Fi and WiMAX access networks and it would still be considered a different session, since the access technology types are different. Or, one terminal can have two WiMAX interfaces using the same NAI but they can still have different WiMAX sessions based on different MAC addresses of each WiMAX module.

In order to generate a unique security context for each network session using the same NAI, the respective NAS reports its identifier and type, and the MS MAC address in the AAA Request message to the authenticating network. When the AAA receives the AAA Request message, it checks the reported attributes and determines 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 and same MS NAI and MAC address associated with already existing security context 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 technology (as indicated by the NAS type), 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 Wi-Fi and WiMAX® networks are described below.

10.1 Wi-Fi Network Entry Procedure

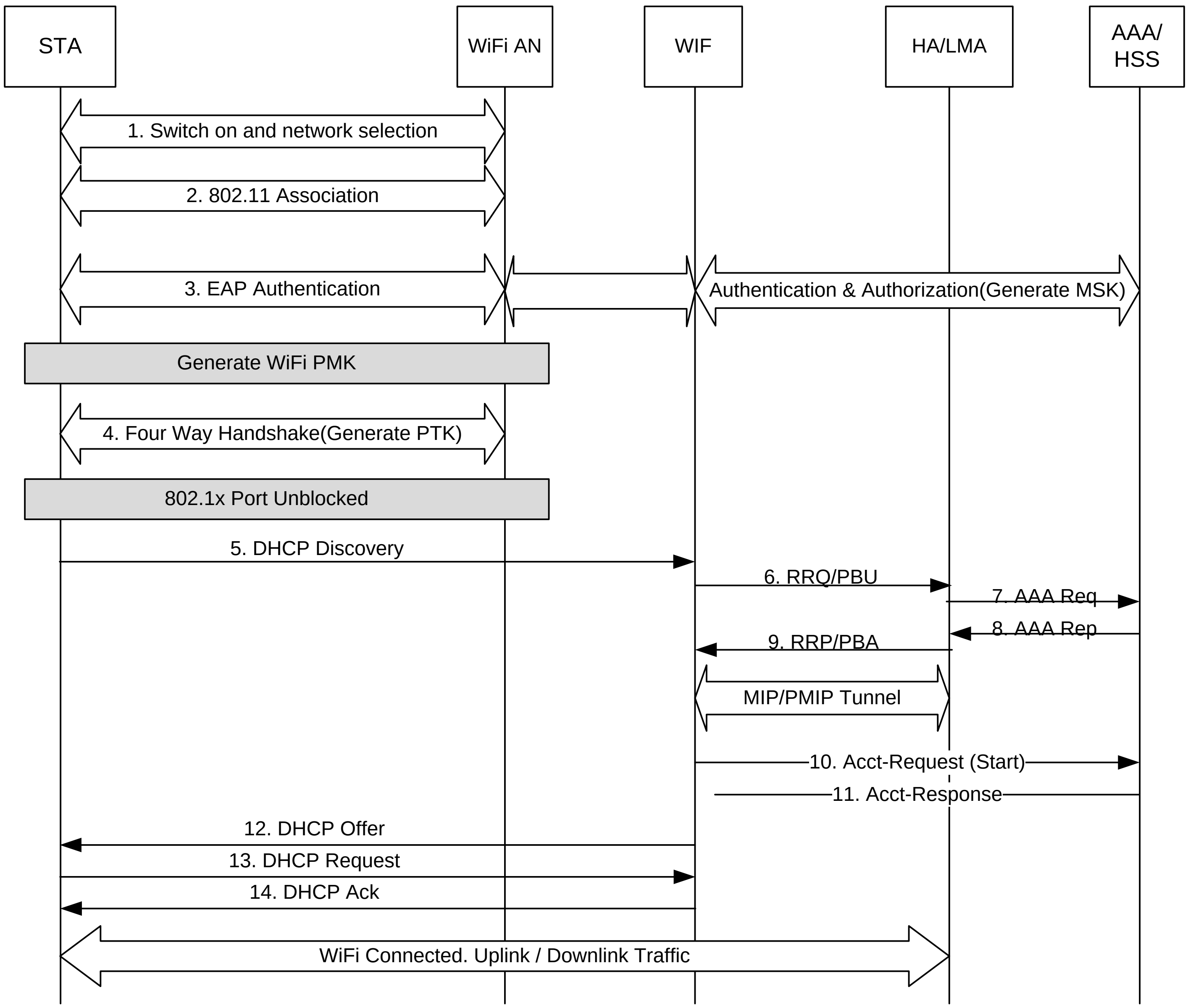


Figure 11-1 – Wi-Fi Initial Network Entry Procedure

1. The Wi-Fi STA is switched on, and captures Wi-Fi signaling and then performs network discovery and selection.

2. The STA establishes Association with the Wi-Fi 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 Wi-Fi 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 authentication on behalf of the Wi-Fi 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 Wi-Fi AN, and then at the end of the successful authentication, a PMK is derived from the MSK at the Wi-Fi 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 Wi-Fi AN. During the four-way handshake procedure, a fresh pair wise 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. Wi-Fi 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" (indicating IEEE 802.11a/b/g) 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 with 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

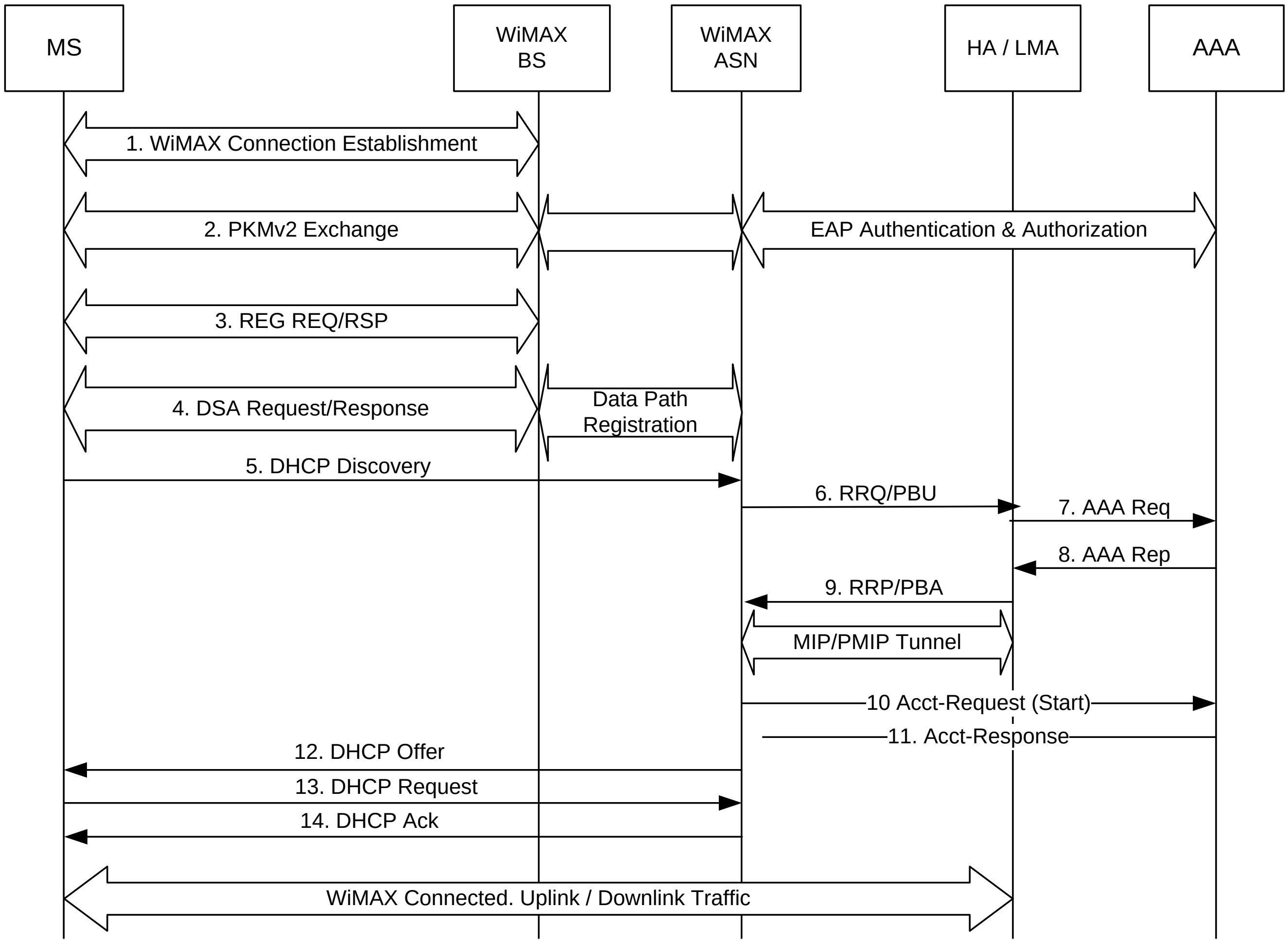


Figure 11-2 – WiMAX® Initial Network Entry Procedure

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 subteam based on the procedures defined in the IETF (presently ambiguous) to allocate NAS Port type.

3. The MS then registers with the 802.16 network using REG REQ/RSP.
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 with 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 PBA message. Once the MN-HA 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 Wi-Fi 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 Wi-Fi networks in the neighborhood and it also determines if the Wi-Fi network can connect it to the WiMAX CSN and provides interworking services. The MS decides to perform a handover to Wi-Fi. The MS performs the Wi-Fi Network entry procedure as described in section-9. For accessing the WiMAX CSN the dual radio mobile identifies itself with a unique NAI during authentication. Please refer to Figure 12-1 for further details.

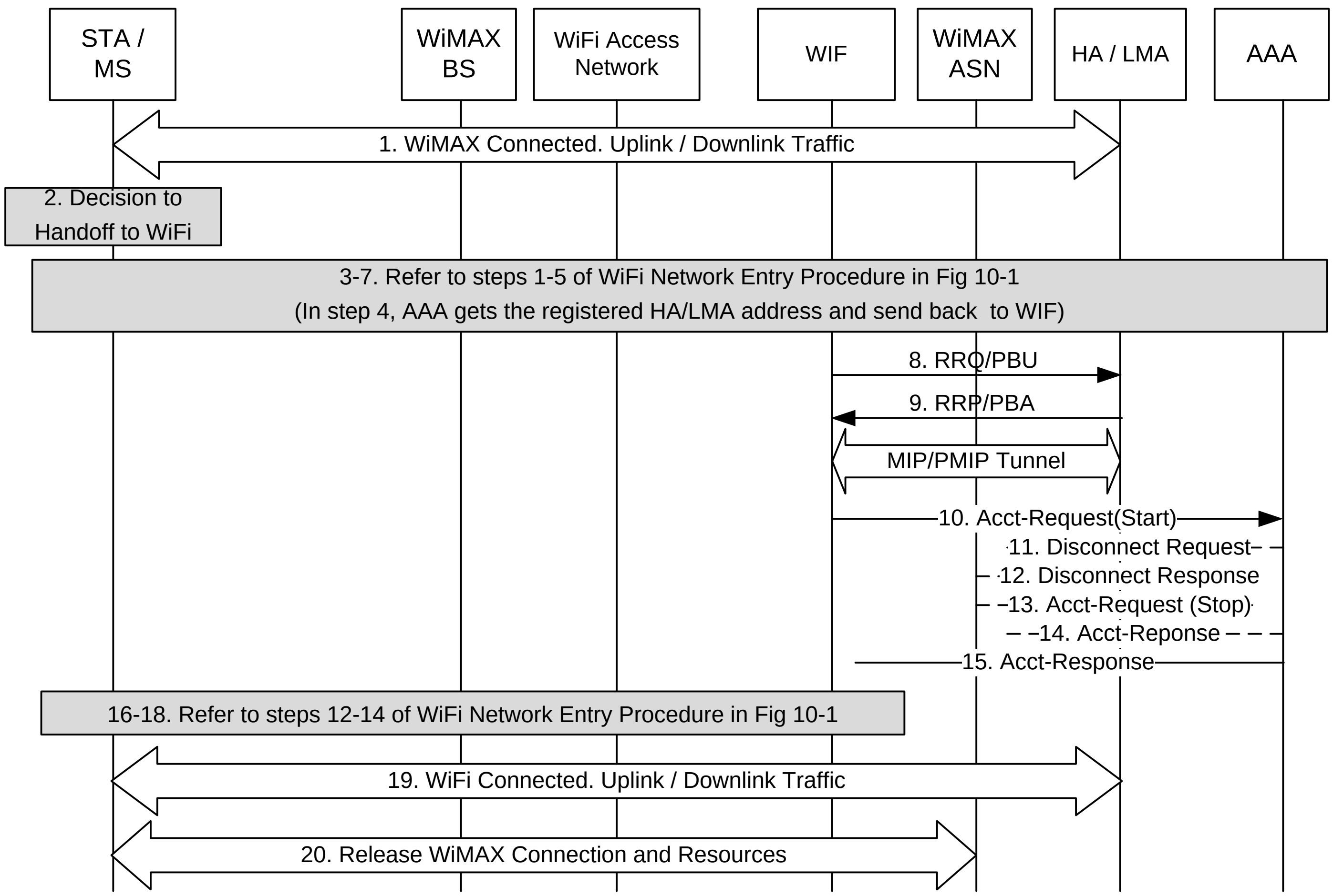


Figure 12-1 – WiMAX® to Wi-Fi Dual Radio Handover Procedure

1. The mobile device is initially connected to WiMAX access network.
2. MS decides to handover to Wi-Fi access network.

3-7. Please refer to steps 1-5 in Figure 11-1 of section 11 on Wi-Fi Network Entry procedure. The registered HA/LMA address will be returned from AAA to WIF in step 5.

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 was previously assigned when the device 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 simultaneous binding, it invokes the release procedure as described in4.5.2.1.2.5 in [1].
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 ASN sends a disconnect response message to the AAA.
13. The Accounting Client at WiMAX ASN sends an Acct-Request (STOP) message to the AAA
14. The AAA server returns an Acct-Response message to the Accounting Client.
15. The AAA server returns an Acct-Response message to the Accounting Client at WIF to start the accounting at the Wi-Fi side.

16-18. Please refer to steps 10-12 in Figure 11-1 of section 11 on Wi-Fi Network Entry Procedure.

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

11.1.2 Wi-Fi to WiMAX® Dual Radio Handover

The dual radio MS is initially connected to the Wi-Fi network and the MS is assigned an IP address from the WiMAX CSN as part of Wi-Fi 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 Wi-Fi network. The MS decides to perform a handover to WiMAX. The MS performs the WiMAX Network entry procedure as described in section-11. The Dual Mode mobile identifies itself with a unique NAI during authentication.

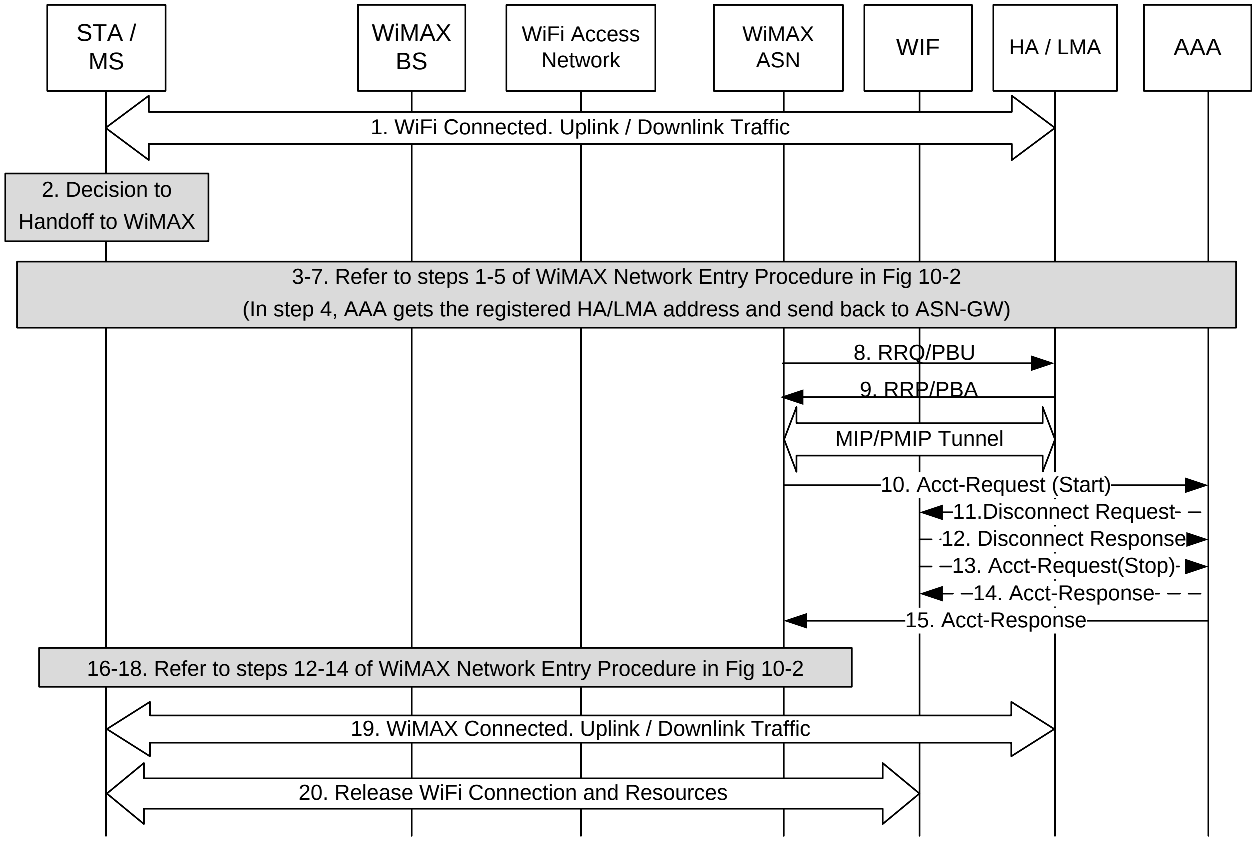


Figure 12-2 – Wi-Fi to WiMAX® Dual Radio Handover Procedure

1. The mobile device is initially connected to Wi-Fi access network.
2. The mobile device makes decision to handover to WiMAX access network.

3-7. Please refer to steps 1-5 in Figure 11-1 in section 11 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 Wi-Fi 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 14.2.2.
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 Client.
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 11 describing the WiMAX Network Entry Procedure.

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

20. The Wi-Fi connection is closed and Wi-Fi resources are released.

11.2 Single radio handover procedures

11.2.1 New Modes for Supporting Single Radio Handovers

The dual mode MS and the WiMAX® network are required to support three additional modes of service for supporting single radio handovers. The additional modes are Null Mode, Pseudo-Active Mode and Pseudo-Idle mode.

In Null mode the MS receives service from the Wi-Fi network, does not pre-register on the WiMAX network and the WiMAX-SFF context is said to be in Null mode. The Pseudo-Active mode is similar to the WiMAX active mode except that the MS maintains two sessions, a pre-registered inactive session in the WiMAX network and existing active session on the Wi-Fi network where it receives normal service. The Pseudo-Idle mode is similar to the WiMAX Idle mode except that the MS maintains two sessions, a pre-registered inactive idle session in the WiMAX network and existing active session in the Wi-Fi network where it receives normal service.

For definition of pre-registration, more detailed explanation of these modes and the transition between all modes, please refer to section 5.3 of [10].

11.2.2 WiMAX® to Wi-Fi Single Radio Handover

In this scenario, the MS is initially connected to the WiMAX network. It learns about the availability of a Wi-Fi network and the interworking functionality. At this point, based on one or more decision criteria, the MS decides to handover to the Wi-Fi network. The WiMAX to Wi-Fi single radio handover procedures is composed of multiple phases, please refer to Figure 12-3 for single radio handover from WiMAX to IEEE 802.11i based Wi-Fi network and to Figure 12-4 for single radio handover from WiMAX to IEEE 802.11r, based Wi-Fi network.

11.2.2.1 Single Radio Handover from WiMAX® to IEEE Std 802.11i based Wi-Fi network

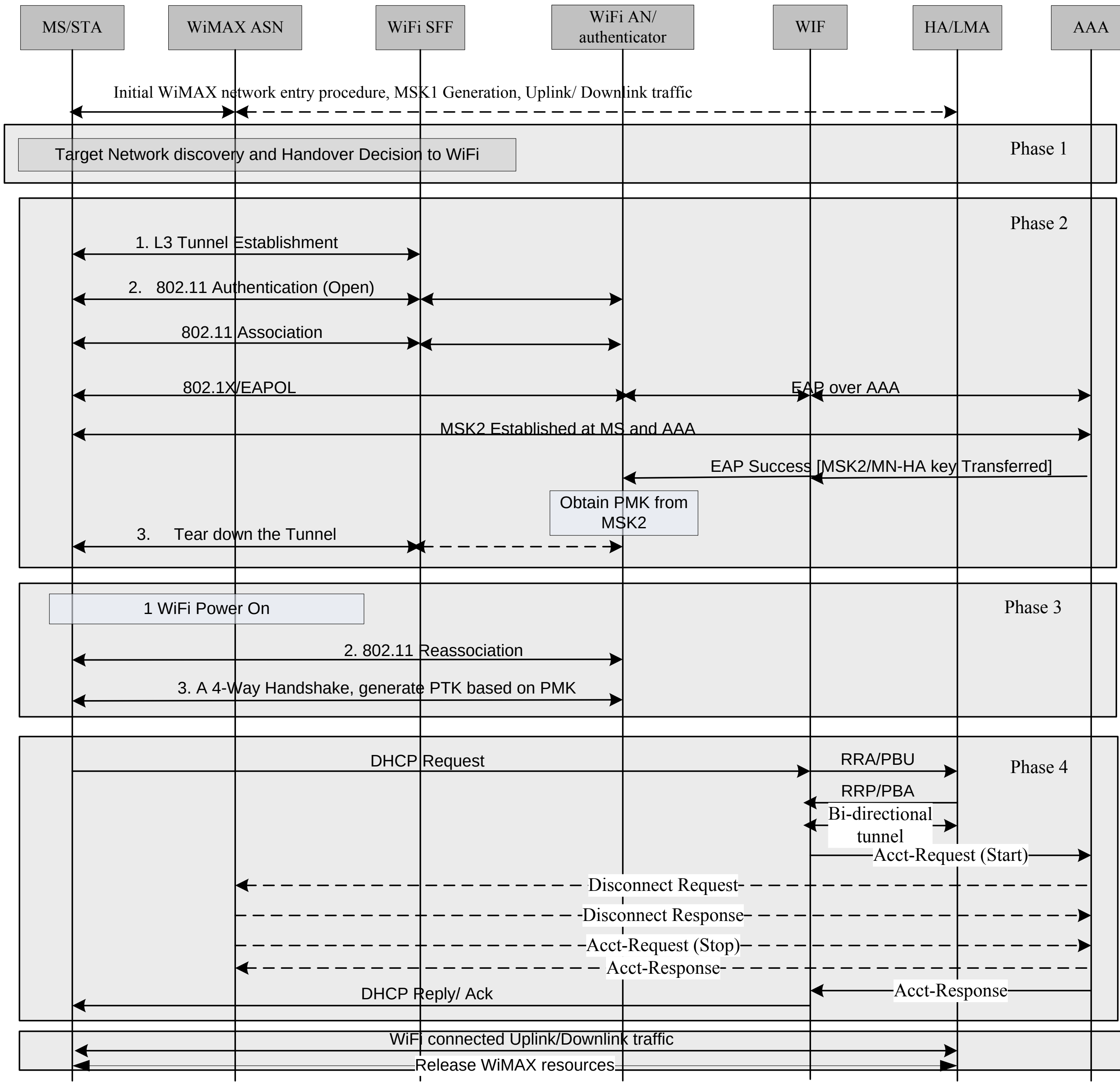


Figure 12-3 – Single Radio Handover from WiMAX® to IEEE Std 802.11i Wi-Fi network

In case the target Wi-Fi network supports 802.11i, the handover procedure follows Figure 12-3. The steps in the handover procedure are as follows:

<u>Phase Zero</u>: Initial WiMAX Network Entry

The mobile device is initially connected to the WiMAX access network. The initial WiMAX network entry procedure is described in section 11.2. During the initial WiMAX network entry, after a successful EAP procedure, the MSK and EMSK are generated. These are labeled as MSK1 and EMSK1 respectively.

<u>Phase one:</u> Target Network Detection and Wi-Fi-SFF discovery

The MS detects a Wi-Fi network signal, selects a target AP and discovers the address of the Wi-Fi-SFF through DHCP or DNS procedure.

<u>Phase two:</u> Tunnel set-up and target network preparation

1. After the MS discovers the address of the Wi-Fi-SFF, the MS establishes an IP tunnel to the Wi-Fi-SFF over Ry (the tunnel may be secured). Once established, all the 802.11 MAC messages from the MS/STA are sent to the Wi-Fi-SFF through the tunnel established between the MS and the Wi-Fi-SFF. The Wi-Fi-SFF then forwards the MAC messages to the target Wi-Fi network through a tunnel between itself and the Wi-Fi access network. If the tunnel between the Wi-Fi SFF and the target Wi-Fi network has not been established, the Wi-Fi SFF establishes it.
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 selected target AP. The Wi-Fi-SFF discovers the target Wi-Fi access network based on the BSSID in the Authentication Request frame and forwards the frame to the target network over w1.

Note: The open system algorithm, means the " Authentication algorithm number" IE has a value of " open system" as defined in 7.2.3.10 in IEEE 802.11-2009

- The MS associates with the target AP by sending an Association Request frame to the AP and receives an Association Response frame from the AP.
- The STA sends the EAPOL-Start message to the target Wi-Fi access network to initiate EAP-authentication over the IP-tunnel. The Wi-Fi SFF forwards this message to the Authenticator located in the Wi-Fi access network
- The MS and AAA server derive MSK and EMSK. These are labeled as MSK2 and EMSK2 respectively. The AAA server sends the MSK2 to the authenticator in the target Wi-Fi network and the mobility keys derived from EMSK2 to the PMIP client at the WIF. The authenticator derives PMK from MSK2 according to 802.11i specification.

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

<u>Phase three:</u> Single Radio Handover Action

1. The MS decides to handover to the Wi-Fi access network. The Wi-Fi interface is powered on.
2. The MS sends re-association message to the target Wi-Fi AP
3. The MS executes a 4-way handshake procedure in order to generate PTK based on the earlier derived PMK.

The MS requests and receives the IP address anchored at the HA. The request and reply messages are proxied by the DHCP proxy & PMIP Client/MAG in the Wi-Fi Interworking Function (WIF). The Accounting Client at the 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 (e.g. it may not have enough quota for online accounting). In case of a disconnect request, the WiMAX sends a disconnect response message to the AAA. The Accounting Client at the WiMAX network sends an Acct-Request (Stop) message to the AAA and the AAA server returns an Acct-Response message to the Accounting Client. The AAA server returns an Acct-Response message to the Accounting Client at the WIF in order to start an accounting session at the Wi-Fi network.

<u>Phase four:</u> Handle network resources in source network

After the Wi-Fi network is connected, based on the operator policy, the WiMAX network may immediately release the resources of the MS or retain them for a period of "Retain-Time". During this time period, the MS context is retained in the WiMAX ASN and the WiMAX network is not in the active mode.

<u>Optimized handover back to WiMAX:</u> During the "Retain Time", the MS may select a WiMAX SFF and triggers the context transfer from the serving WiMAX ASN (i.e. serving BS) to the newly selected WiMAX SFF. The MS

may subsequently handover to the WiMAX network. During this process the MS may enter the pseudo-active mode without the pre-registration phase. Please see [10] for more details.

11.2.2.2 Single Radio Handover from WiMAX to IEEE 802.11r based Wi-Fi network

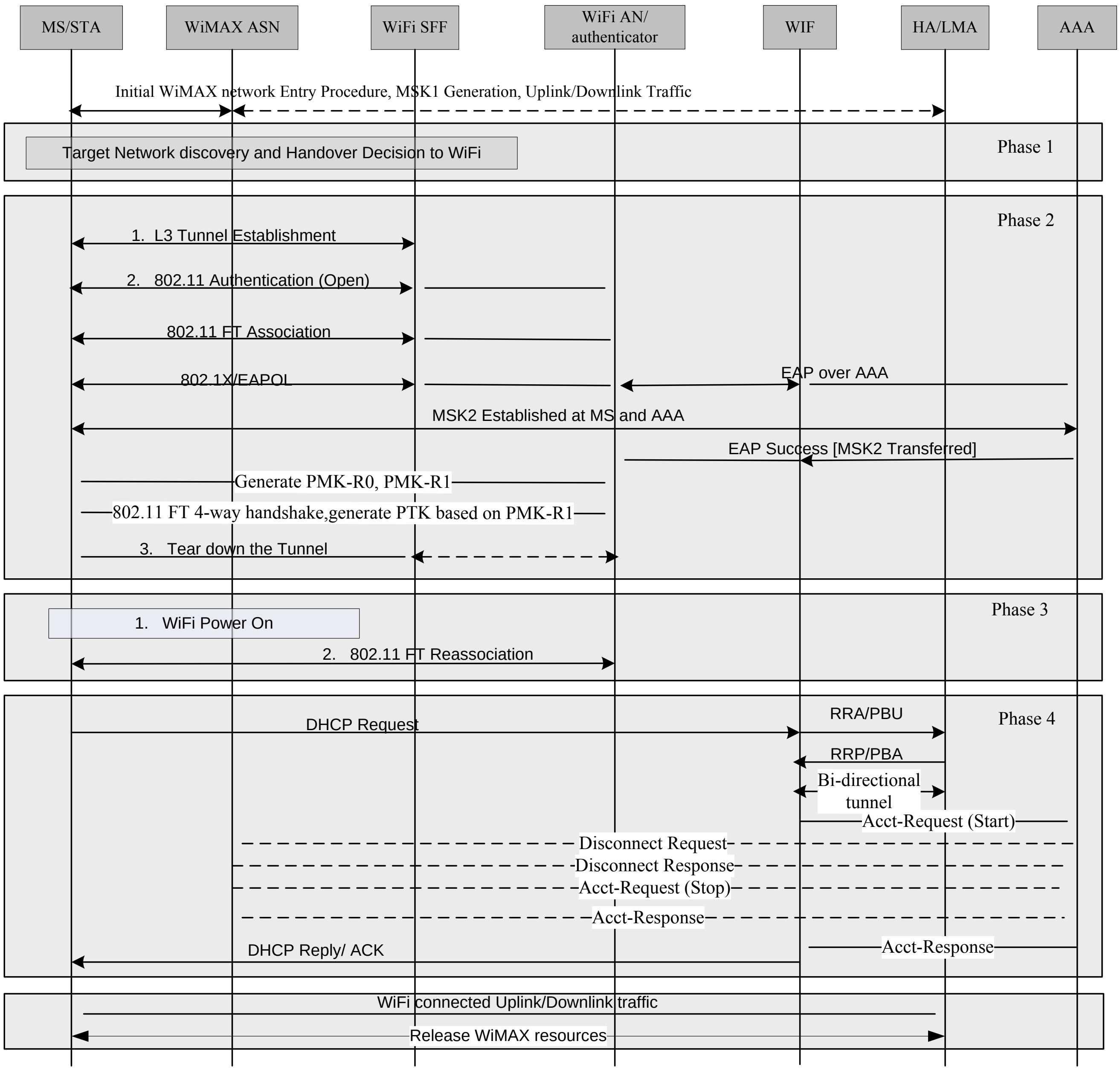


Figure 12-4 – Single Radio Handover from WiMAX® to Wi-Fi network that supports IEEE Std 802.11r

In case the target Wi-Fi network supports 802.11r based network, the handover procedure follows Figure 12-4. The steps in handover procedure are as follows:

<u>Phase zero:</u> Initial WiMAX Network Entry

The mobile device is initially connected to the WiMAX access network. The initial WiMAX network entry procedure is described in section 11.2. During initial WiMAX network entry and after a successful EAP procedure, the MSK and EMSK are generated. These are labeled as MSK1 and EMSK1 respectively.

Phase one: Target Network Detection and Wi-Fi SFF discovery

The MS detects the Wi-Fi network signal and selects a target AP. and the MS discovers the address of the Wi-Fi SFF through a DHCP or DNS procedure.

Phase two: Tunnel setup and target network preparation

1. After the MS discovers the address of the Wi-Fi SFF, the MS establishes an IP tunnel to the Wi-Fi SFF over Ry (the tunnel may be secured). Once established, all the 802.11 MAC messages from the MS/STA are sent to the Wi-Fi-SFF through the tunnel established between the MS and the Wi-Fi-SFF. The Wi-Fi-SFF then forwards the MAC messages to the target Wi-Fi network through a tunnel between itself and the target Wi-Fi network. If the tunnel between the Wi-Fi SFF and the target Wi-Fi network has not been established, the Wi-Fi SFF establishes it.
2. The Wi-Fi 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 selected target AP. The Wi-Fi-SFF discovers the target Wi-Fi access based on the BSSID in the Fast Transition Authentication Request frame and forwards the frame to the target network over w1.
    - The MS associates with the target AP by sending Fast Transition Association Request frame to the AP and receives Association Response frame from the AP.
    - The MS starts 802.1x authentication procedure by sending an EAPoL_Start message.
    - The MS negotiates MSK and EMSK with AAA server. These are labeled as MSK2 and EMSK2 respectively. The AAA server sends MSK2 to the authenticator in target Wi-Fi 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 based on Fast Transition 4-Way handshake.
3. The MS releases the IP tunnel that was created earlier with the Wi-Fi SFF. The Wi-Fi SFF may release the tunnel between the Wi-Fi SFF and the target Wi-Fi network.

Phase three: Single Radio Handover Action

1. The MS decides to handover to the Wi-Fi access network. Wi-Fi interface is powered on.
2. MS sends Fast Transition Reassociation Request to associate with the target AP and no 4-Way handshake is needed in this case.

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

Phase five: Handle network resources in source network

After the Wi-Fi network is connected, based on the operator policy, the WiMAX network may immediately release the resources of the MS, or retain it for a period of “Retain-Time”.

<u>**Optimized handover back to WiMAX:**</u> During the "Retain Time", the MS may select a WiMAX SFF and triggers the context transfer from the serving WiMAX ASN (i.e. serving BS) to the newly selected WiMAX SFF. The MS may subsequently handover to the WiMAX network. During this process the MS may enter the pseudo-active mode without the pre-registration phase. Please see [10] for more details.

11.2.3 Wi-Fi to WiMAX® Single Radio Handover

The steps in the handover procedure are as follows. Figure 12-6 provides the call flow for the Wi-Fi to WiMAX handover process.

Phase zero: Initial Wi-Fi Network Entry

The mobile device is initially connected to the Wi-Fi network. The initial Wi-Fi network entry procedure is described in 11.1. During the initial Wi-Fi network entry, after a successful EAP procedure, the MSK is generated. This key is labeled MSK1. Subsequently, the MS detects the availability of a WiMAX network and the presence of interworking support. At this point, based on one or more decision criteria, the MS decides to handover to the WiMAX network.

Note: The steps and call flows in this document are similar to and aligned with the 3G-WiMAX handover procedures/call flows [10].

Phase one: Target network detection and WiMAX-SFF discovery

The MS detects a WIMAX network signal and discovers the address of the WiMAX SFF through DHCP or DNS procedure. The MS may alternately discover the address of the WiMAX SFF and the operator policy through access to the Information Server (see section 7.5). In case a tunnel to the WiMAX SFF already exists this phase can be skipped.

Phase two: Tunnel set-up and target network preparation

If the SR MS is not registered with the WiMAX network and the WiMAX network has no context information about this SR MS, the MS establishes a tunnel between the MS and the WiMAX-SFF in the WiMAX network over R9 interface (the tunnel may be secured). Once established, all the IEEE 802.16 MAC messages from the MS/STA are sent to the WiMAX-SFF through the tunnel established between the MS and the WiMAX-SFF. The WiMAX-SFF then acts as a BS and can perform inter-RAT HO with the target WiMAX ASN using the R6 interface.

The MS must obtain the BSID of the WiMAX SFF in order to calculate the AK during authentication procedure. In case the MS discovers the IP address of the WiMAX SFF from an Information Server, the MS may get the BSID of the WiMAX SFF from the IS-. The WiMAX SFF may send a DCD message which includes the BSID of the WiMAX SFF only to the MS once the tunnel is established. Or, the MS may discover the BSID of the WiMAX SFF by setting B bit to '1' and including the BSID of the target BS in the R9 header when sending a RNG_REQ message to the WiMAX SFF through R9 tunnel. In case it receives such a R9 message, the WiMAX SFF shall include its BSID in the R9 header and set B bit to '1' when it responds a RNG_RSP message to the MS. Please see section 12.3.1 for details of R9 protocol. The SR MS then performs initial WiMAX network entry procedure through this tunnel. After successful EAP procedure in the WiMAX network, a MSK is generated and sent by the AAA server to the authenticator (step 9). This key is labeled MSK2.

When the SR MS context is maintained at the WiMAX network, the WiMAX network treats the MS in either pseudo active mode or pseudo idle mode. If the MS context is maintained in the WiMAX network, (within the Retain-Time period) this phase is skipped.

Phase three: Single Radio Handover Action

The MS performs Inter-RAT handover procedure to the target WIMAX BS at the target ASN. Depending on operator policy, this procedure can be invoked from WiMAX Pseudo Active or Pseudo Idle mode. For more details, please refer to [10]. As part of the HO procedure, the WiMAX ASN-GW that serves the WiMAX-SFF) triggers a Proxy Binding Update (PBU—step 29) anytime after successful data path registration. The Accounting Client sends an Acct-Request (Start) message (step 30) to the AAA server. Optionally, the AAA server may send a disconnect request message to the WIF for various reasons (e.g. it may not have enough quota for online accounting (step 31)) and the WIF sends a disconnect response message (step 32) back to the AAA server. The Accounting Client at WIF sends an Acct-Request (STOP) message (step 33) to the AAA server and the AAA server returns an Acct-Response message to the Accounting Client (step 34). Upon receiving the accounting request message, the AAA server sends an Acct-Response message to the Accounting Client at the WiMAX network to start the accounting session (step 35).

Phase four: Handle network resources in source network

After the MS gets an IP address (HoA) from the HA, in phase three, the Wi-Fi network releases the network resources.

The figure below provides the call flow for the Wi-Fi to WiMAX handover process where the WiMAX network has no MS context and the MS performs handover to the WiMAX network.

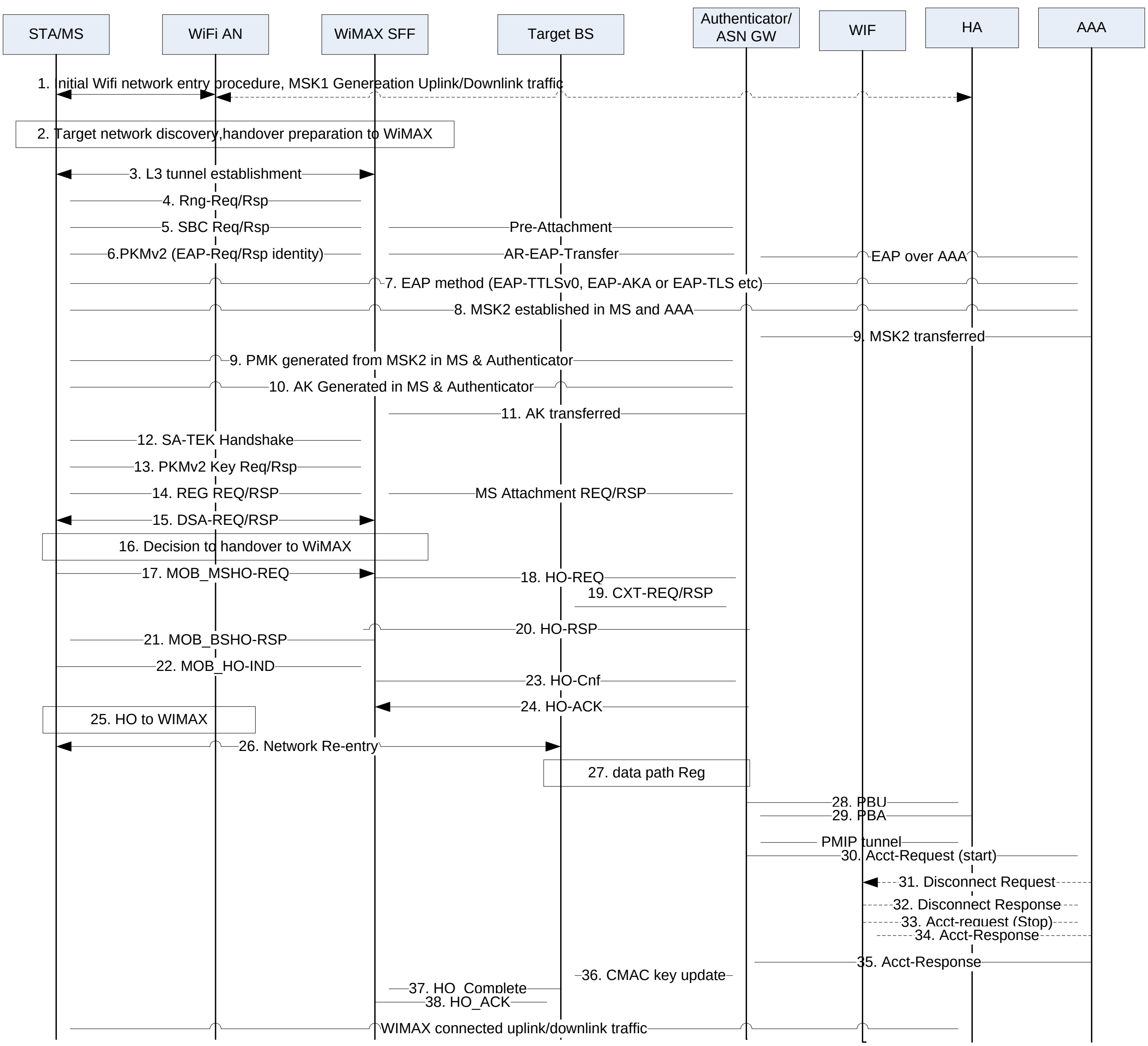


Figure 12-5 – Wi-Fi to WiMAX® Single Radio Handover Procedure

11.3 Interworking protocol stacks

11.3.1 Control plane protocol stack for SRHO from Wi-Fi to WiMAX®

Figure 12-6 shows the control plane protocol stack for the scenario where the MS is connected to the Wi-Fi network and later decides to handover to the WiMAX network.

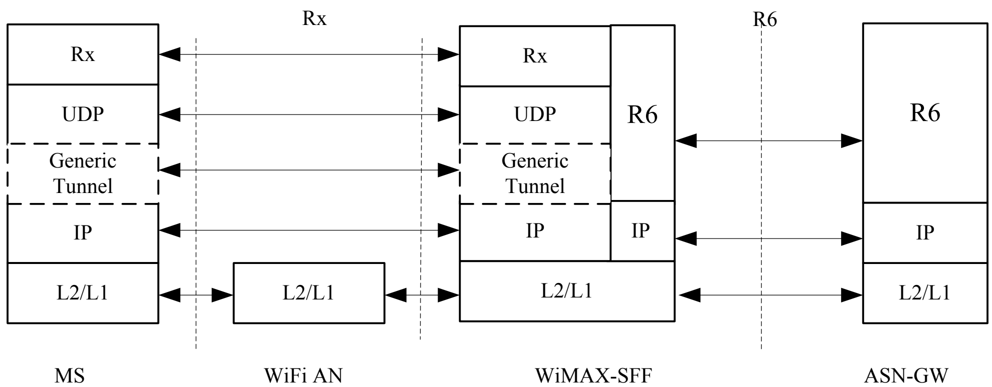


Figure 12-6 – Control plane Protocol Stack for SRHO from Wi-Fi to WiMAX®

If the Rx connection between MS and WiMAX SFF is secure, the generic tunnel deployment is optional.

The Rx protocol header is defined in Table 12-1.

Table 12-1 – Rx Protocol Header

Octets	Bits 8	7	6	5	4	3	2	1
1	Reserved						B	MTI
2-7	MSID							
8-13	BSID							
14-*n*	802.16e MAC PDU/Rx Control Message							

MTI (Message Type Indicator): This bit indicates the type of message.”0” indicates it is Rx Control Message, “1” indicates Encapsulated 802.16e MAC Message. MTI is defined in **Error! Reference source not found.**.

Note: The WiMAX Forum® Network Architecture interpretation of bit ordering of 802.16e MAC messages is different than that specified in IEEE Std 802.16-2009.

B: This bit indicates if the BSID field will be included in this message. “0” indicates that the BS ID is omitted in the message and “1” indicates BS ID is included.

Reserved: This field is reserved for future use. All bits should be set to “0”; receiver SHALL not validate these bits.

MSID: This is set to the 6-byte 802.16 MAC address of MS the message pertains to. For transactions not related to any specific MS, all bits shall be set to zero.

BSID: For MS to WiMAX SFF direction, BSID is set to the 6-byte Target WiMAX BS identity from MS to WiMAX SFF. For WiMAX SFF to MS direction, BSID is set to pseudo BSID of the WiMAX SFF. If the MS has the SFF BSID, the BSID field may be omitted by setting the B bit to “0”. If the BSID is not omitted, then it SHALL be set to the BSID received from the SFF.

802.16e MAC PDU: If MTI is “1”, Octet 8 – *n* contains Encapsulated 802.16e MAC PDU.

Rx Control Message: If MTI is “0”, Octet 8 - *n* contains Rx Control Message.

Table 12-2 – MTI (Message Type Indicator) Value

MTI (Binary)	Meaning
0	**Rx Control Message**
1	**Encapsulated 802.16e MAC PDU**

The Rx control message format is defined in Table 12-3.

Table 12-3 – Rx Control Message Format (MTI=0)

Octets	Bits 8 7 6 5 4 3 2 1
14	Message Type
15	Length
16-*n*	Message Body

The Rx Control message type is defined in Table 12-4.

Table 12-4 – Message Type (For MTI = 0)

Message Type (Binary)	Meaning
00000000	**Reserved**
00000001	**ERR_DLVRY**
00000010 to 11111111	**Reserved**

For Rx ERR_DLVRY Message type, the octet 16 in the message body of Rx indicates the error cause value defined in Table 12-9.

11.3.2 Control plane protocol stack for SRHO from WiMAX® to Wi-Fi

Figure 12-7 shows the control plane protocol stack for the scenario where the MS is connected to the WiMAX network and is preparing to handover to the Wi-Fi network through the Wi-Fi-SFF.

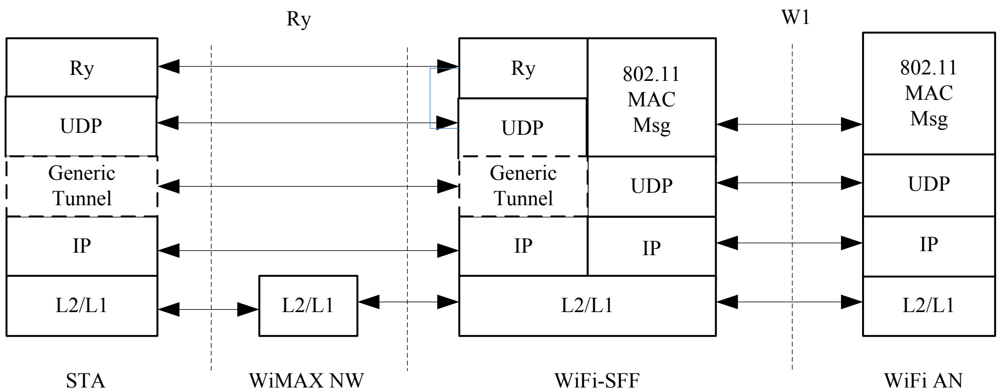


Figure 12-7 – Control plane Protocol Stack for SRHO from WiMAX® to Wi-Fi

If the connection between STA and Wi-Fi SFF is secure, the generic tunnel deployment is optional.

The Ry protocol header is defined in Table 12-5.

Table 12-5 – Ry Protocol Header

Octets	Bits 8	7	6	5	4	3	2	1
1	Reserved							MTI
2-*n*	802.11 MAC PDU/Ry Control Message							

MTI (Message Type Indicator): This bit indicates the type of message."0" indicates it is Ry Control Message, "1" indicates Encapsulated 802.11 MAC Message. MTI is defined in **Error! Reference source not found.**.

Reserved: This field is reserved for future use. All bits should be set to "0", receiver SHALL not validate these bits.

802.11 MAC PDU: If MTI is "1", Octet 2 – *n* contains Encapsulated 802.11 MAC PDU.

Ry Control Message: If MTI is "0", Octet 2 - *n* contains Ry Control Message.

Table 12-6 – MTI (Message Type Indicator) Value

MTI (Binary)	Meaning
0	**Ry Control Message**
1	**Encapsulated 802.11 MAC PDU**

The Ry control message format is defined in Table 12-7.

Table 12-7 – Ry Control Message Format (MTI=0)

Octets	Bits 8	7	6	5	4	3	2	1
2	Message Type							
3	Length							
4-*n*	Message Body							

The Ry control message type is defined in Table 12-8.

Table 12-8 – Message Type (For MTI = 0)

Message Type (Binary)	Meaning
00000000	**Reserved**
00000001	**ERR_DLVRY**
00000010 to 11111111	**Reserved**

For Ry ERR_DLVRY Message type, the octet 4 in the message body of Ry indicates the error cause value as defined in Table 12-9. Error delivery handling in the SFF is left to implementation.

Table 12-9 – Error Cause Values

Error cause value	Meaning	Notes
1	System failure	This value shall only be used in the Error Notification message sent by the SFF.
2	SFF rediscovery required	This value shall only be used in the Error Notification message sent by the SFF. When the MS/STA receives an Error Notification message including the error cause value for requiring the SFF rediscovery, the MS/STA shall rediscover the SFF.
All Others	Reserved	

11.3.3 Data plane protocol stack while connected to Wi-Fi

Figure 12-8 describes the data plane protocol stack while MS is connected to WiMAX network via Wi-Fi access network.

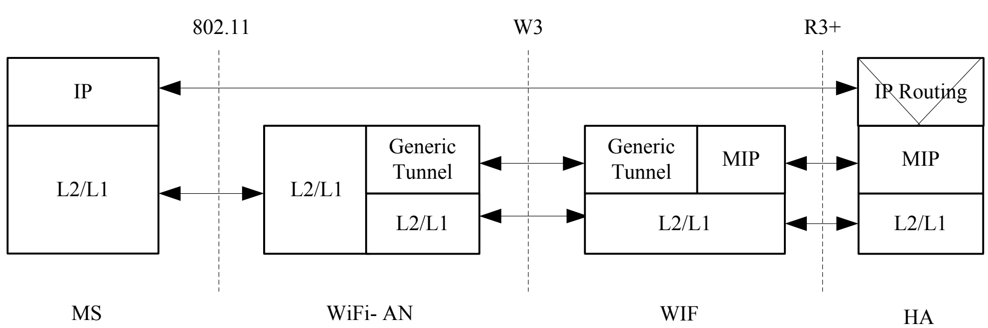


Figure 12-8 – Data plane protocol Stack while connected to Wi-Fi

12. Accounting

Accounting records for a session that involves WiMAX® and Wi-Fi networks SHALL be independently generated by the WiMAX NAS and CSN and by the Wi-Fi 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. Wi-Fi, 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi network SHALL NOT be forwarded to the AAA.

13. Network Exit

Network Exit procedure is a common scenario caused when MS exits from one or both networks or there is some failure or maintenance situation whereby the MS is forced to deregister from one or both networks and its context in the network(s) is deleted.

The following entities may initiate Network Exit procedure:

- MS, when it initiates a graceful shutdown from both networks;
- Wi-Fi AN, if the MS is connected to the Wi-Fi access network based on either graceful shutdown trigger or failure situation in the Wi-Fi network;
- Wi-Fi access network or STA after the MS/STA hands over to WiMAX® and, if set, the timer "Retain-Time" expires.
- WiMAX ASN, when the MS is connected to a WiMAX access network and if there is either a graceful shutdown trigger or failure situation in the network;
- WiMAX network or MS after the MS/STA hands over to Wi-Fi network and, if set, the timer "Retain-Time" expires or the exit condition is met based on the SR state diagram described in [10].
- WIF or HA/LMA, when the MS is connected to the Wi-Fi access network and the procedure is triggered based on failure or maintenance situation in the network such as the inability to build a MIP tunnel;
- Home AAA server located in the CSN.

13.1 Network exit procedure from the WiMAX® Network

The Network exit procedure from the WiMAX network is the same as described in section 4.5.2 in [11].

13.2 Network exit procedure from the Wi-Fi Network

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

13.2.1 Network Exit Procedure Initiated by MS/STA or Wi-Fi AN

The Wi-Fi access network or the MS/STA may initiate network exit procedure at the Wi-Fi network when some errors occur or during overload conditions. Figure 14-1 depicts STA/MS or Wi-Fi AN initiated network exit procedure.

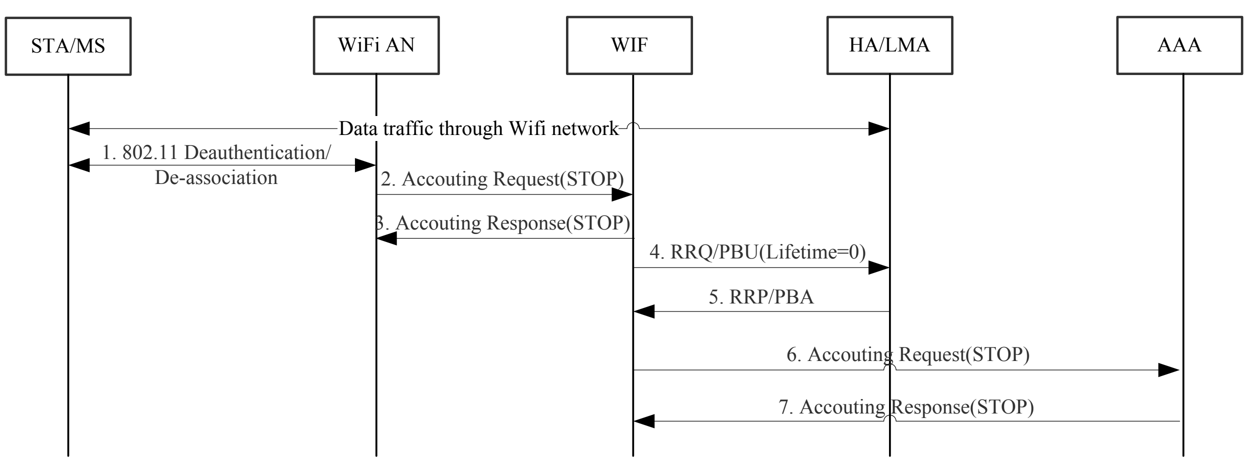


Figure 14-1 – MS/STA or Wi-Fi AN initiated network exit procedure

Step1: The MS/STA or Wi-Fi access network may initiate network exit procedure using 802.11 De-authentication or De-association procedure.

Step2: The Wi-Fi 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 the PMIP session is expired.

Step3: In response to Accounting Request (Stop) message, the WIF returns an Accounting Response (STOP) message to the Wi-Fi AN.

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

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

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

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

13.2.2 Network exit procedure initiated by the WIF or HA/LMA

The WIF may gracefully initiate network exit procedure at the Wi-Fi network during failure situation or for other maintenance reasons. Also, the HA/LMA may decide to initiate Wi-Fi network exit procedure in case it detects expiry of the MS's MIP binding or another terminating event. Figure 14-2 depicts a WIF or an HA/LMA initiated network exit procedure from the Wi-Fi AN.

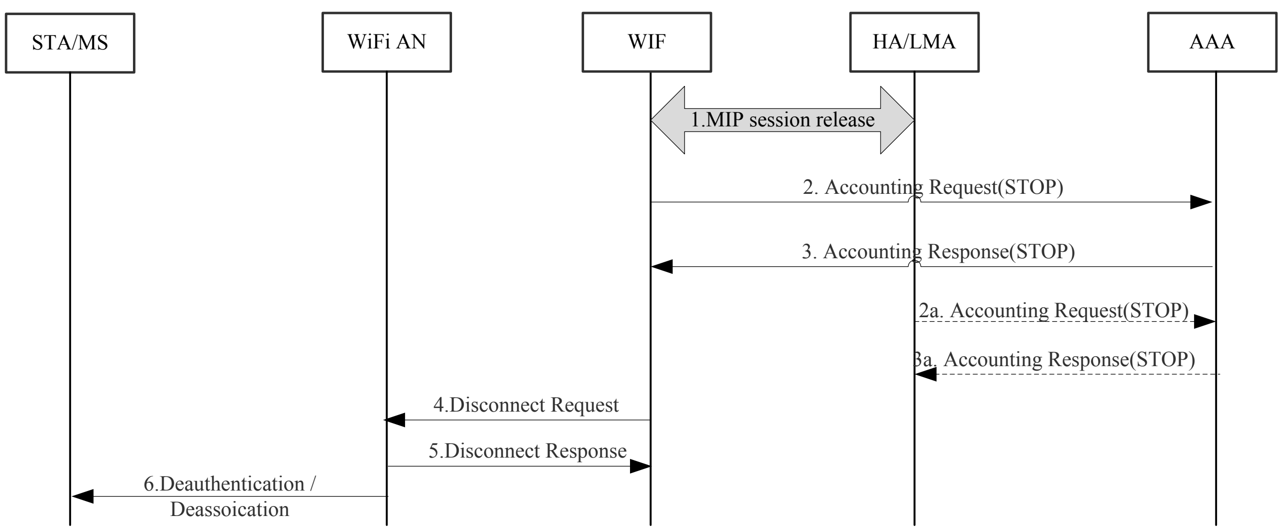


Figure 14-2 – FA/MAG or HA/LMA initiated network exit procedure from Wi-Fi AN

Step1: When the WIF or HA/LMA decides to initiate network exit procedure, they perform a 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 the AAA server. Optionally if there is an active accounting client in the HA, it may send Accounting Request (Stop) message to the AAA as indicated in step 2a.

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

Step4: The WIF notifies the Wi-Fi AN of a network exit by sending a Disconnect Request message. This step may happen prior to step 2.

Step5: The Wi-Fi access network responds to the WIF with a Disconnect Response message.

Step6: Upon receiving the Disconnect Response message, the Wi-Fi access network invokes de-authentication/de-association procedure with the STA/MS. This step may be performed prior to step 2.

13.2.3 Network exit procedure initiated by the AAA

The AAA server may initiate a Wi-Fi network exit procedure because of changing service strategy including user's arrearage, mobile phone loss report etc. Figure 14-3 depicts AAA server initiated network exit procedure from the Wi-Fi AN.

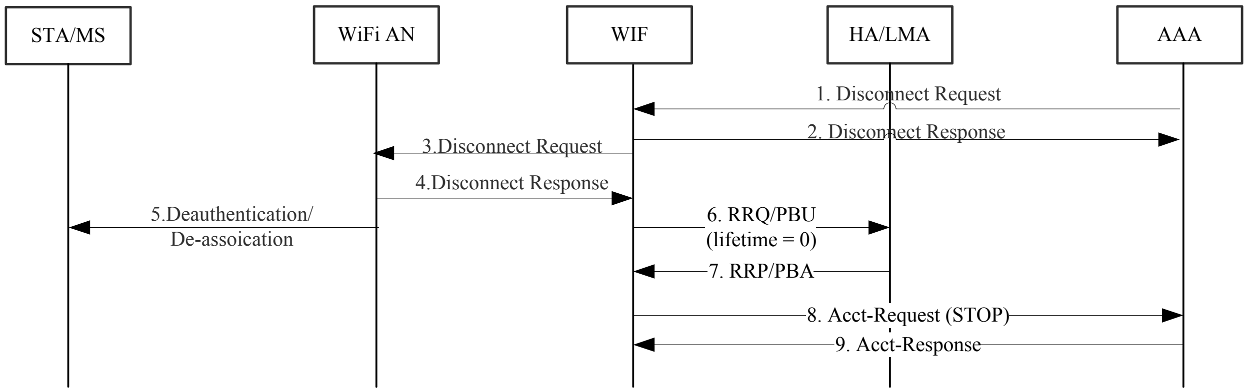


Figure 14-3 – AAA initiated network exit procedure from Wi-Fi AN

Step1: The AAA server initiates a Wi-Fi network exit procedure by sending a Disconnect Request message to the WIF.

Step2: The WIF responds to the AAA server by sending a Disconnect Response message.

Step3: The WIF sends a Disconnect Request message to the Wi-Fi AN.

Step4: The Wi-Fi access network responds to the WIF with a Disconnect Response message.

Step5: The Wi-Fi access network invokes De-authentication/De-association procedure with the STA/MS.

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

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

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

Step9: The 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 a serving network while the MS/STA has handed over to a target network.

13.3.1 MS/STA Handover to Wi-Fi Network and WiMAX® network Operation Modes

Due to various reasons, such as ping-pong scenario or in order to avoid loosing packets during handover, the MS/STA which initially was connected to the WiMAX® network performs a handover to the Wi-Fi access network but does not immediately release the MS context nor exits the WiMAX network. Thus in this case, step(s) involving "Release of WiMAX resources" in the call flows for a Single and Dual Radio handover to Wi-Fi network may not be executed immediately. This is governed by the "Retain-Time" period, as well as the transition states for a SR as described in [10], and also based on the operator policy.

Once the MS causes handover to the Wi-Fi 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 is optionally (only in the case of Dual Radio) 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 the Wi-Fi network. In case of Dual Radio mobile device, the traffic may be optionally sent on both networks.

After handover to the Wi-Fi network and in the case of Single Radio, after creating a tunnel between the MS and the WiMAX SFF, the MS/STA may enter the WiMAX Pseudo Active or Pseudo Idle modes. The MS transition to any of these modes is the same as described in [10]. While in Pseudo Idle mode, the MS may send WiMAX signaling message through the WiMAX-SFF tunnel in order to maintain the Pseudo idle mode as per section 4.10 [11]. Exit procedures in the WiMAX network may take place either when "Retain Time" period expires or as per network transition described in [10].

To exit the WiMAX network while still connected to the Wi-Fi access network through a Single Radio device, the MS/STA sends network exit trigger message to the WiMAX network through the Layer 3 tunnel to the WiMAX-SFF. Subsequently, the WiMAX network completes the network exit procedure as per section 4.5.2 of [11].

As mentioned above after the "Retain Time" period expires or due to some other reasons, the WiMAX network MAY release the MS resources. The following network entities can initiate a Network Exit Procedure as described in section 4.5.2.2 of [11]:

- AAA Server/Authenticator
- Paging Controller
- HA/LMA
- DHCP Proxy/Relay

13.3.2 MS/STA Handover to WiMAX® Network and Wi-Fi in Power-Save Mode

Due to various reasons such as ping-pong scenario or in order to avoid loosing packets during handover, the MS/STA which initially was connected to the Wi-Fi network, performs handover to the WiMAX network but does not immediately exit the Wi-Fi network. This is governed by the "Retain-Time" period set by the 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 in the case of dual radio mobile device, 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 the WiMAX network or optionally in the case of dual radio mobile device, on both networks.

After handover to the WiMAX network and during the "Retain-Time" period, the MS/STA may switch to the Wi-Fi Power Save/Sleep mode of operation. Alternatively, the MS/STA may decide to exit the network after a programmable "Retain Time" period.

To exit the Wi-Fi network while connected to the WiMAX, in the case of a Single Radio, the MS/STA sends network exit trigger message over the Layer 3 tunnel to the Wi-Fi-SFF and the Wi-Fi Interworking function. Subsequently, the Wi-Fi-SFF and the Interworking functional entities such as accounting client, PMIP Client/MAG, etc trigger and complete the Wi-Fi network exit procedure as per section 14.2.1 above.

After the "Retain Time" expires or due to some other reasons, the network MAY release the MS resources. The following network entities can initiate a Network Exit Procedure during the Wi-Fi Power save mode:

- AAA
- WIF or HA/LMA

These procedures are described in sections 14.2.2 and 14.2.3.

14. Dual Mode Device Implications

While in an active mode and connected to either WiMAX® or Wi-Fi access network, the device SHALL be able to pre-register and pre-authenticate on a potential target access technology (i.e. Wi-Fi or WiMAX). This applies to both dual radio handover and single radio handover.

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 security context establishment on a potential target access technology, the device SHALL generate a second security context associated with a potential target access technology, and store it alongside the active security context.

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. When the session is terminated, the MS SHALL delete all the related security contexts.

15. Wi-Fi Access Network Requirements

The Wi-Fi network SHALL support WISPr 1.0 and MAY support WISPr 2.0.

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.

For single radio handover from Wi-Fi to WiMAX, DHCP and MIP procedures may not be performed immediately after the target network preparation phase is complete. To allow this delay in IP allocation, the ASN-GW shall support R6_Attachment_Type TLV defined in [10]. When the MS attaches to the WiMAX network via a WiMAX SFF this TLV SHALL be included in the *MS_Preattachment_Req* message. This message is sent to the ASN-GW and informs it of a delay in IP allocation. If idle mode exit procedure is used for MS handover from Wi-Fi to WiMAX, this TLV shall also be included in *IM_Exit_State_Change_Rsp* message when MS exits the pseudo idle mode.

18. AAA Requirements and Implications

In order to preserve the security context on the active serving network, the AAA SHALL generate a second security context for the same device, one that is associated with the disparate access technology where pre-registration and pre-authentication is performed based on the “FFS-NAS” type reported by the NAS in the AAA Request. When the AAA receives the AAA Request message, it SHALL check the reported “FFS-NAS”type 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 existing security context i.e. same NAI and same MAC address, 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 (as identified by the NAI), but the AAA Request comes from the disparate access technology, 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.

19. Wi-Fi WiMAX® Interworking Specific Messages and TLVs

19.1 WRIX-i to WiMAX® R3 Mapping of AAA Attributes for Roaming

19.1.1 Attribute population required by H-AAA in case of a WiMAX® subscriber being served by a Wi-Fi network

The following tables list the mapping function performed by the AIF for different cases.

- (Table 20-1): Translates WRIX Access-Request to a WiMAX® R3 compliant Access-Request.
- (Table 20-2): Translates WiMAX R3 compliant Access-Accept to a WRIX Access-Accept.
- (Table 20-3): Translates WiMAX R3 compliant Access-Challenge to a WRIX Access-Challenge.

Translation of WiMAX R3 compliant Access-Reject to WRIX Access-Reject is not shown because it is relatively straight forward.

Note: Translation is performed strictly to R3 and not R3/R5. That is, the AIF may be deployed between the Wi-Fi access network and a VCSN or a CSN and thus the next RADIUS hop could either be a VAAA or a HAAA. Any RADIUS attribute not mentioned by the WRIX specification is assumed to be not support by the NAS located in the Wi-Fi access network domain.

Table 20-1 – Access-Request Mapping From WRIX to WiMAX® R3 Access-Request

Attribute	TYPE	Description	WRIX Access-Request	R3 Access-Request	AIF Processing Instruction	VAAA or HAAA Processing Instructions
User-Name	1	NAI obtained from the EAP-Response Identity (Outer-NAI).	1	1	The AIF may have to convert the routing declaration (if any) from the format used by the WRIX-i to the format used by WiMAX.	As per R3
User-Password	2	User's full password	1	0	The AIF MUST never receive an Access-Request with User-Password. In this case the AIF MUST silently discard the message.	If received, silently discard the attribute.
NAS-IP-Address	4	IP-Address of the originator of the Access-Request (NAS).	1	1	Forward.	As per R3
Service-Type	6	RFC2865	0	1	AIF SHALL add this attribute and set it to "2"= Framed	Note that WRIX does not use Service-Type and thus explicit re-authentication indication is not possible. HAAA therefore may

Attribute	TYPE	Description	WRIX Access-Request	R3 Access-Request	AIF Processing Instruction	VAAA or HAAA Processing Instructions
						treat each access request as a normal authentication unless it can use other means to detect that the session is being reauthenticated.
Framed-MTU	12	Usage as per RFC2865	0-1	0-1	If this attribute is present the AIF shall include this attribute without modification. If the Framed-MTU attribute is included within an Access-Request message containing an EAP-Message attribute then the attribute is indicating the appropriate MTU size to avoid exceeding the maximum payload size for messages containing EAP[46].	If the attribute is present, the Home AAA shall treat this as per [46].
Connect-Info	77	RFC2865	0-1	0-1	This attribute is not used by WiMAX. If the AIF receives this attribute it MAY forward the attribute over R3.	If the HAAA server receives this attribute it may silently ignore the attribute.
EAP-Message	79	The EAP exchanged transported over RADIUS.	1-n	1-n	If the AIF does not receive this attribute then it shall silently discard the packet.	As per R3.
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [46].	1	1	As per [46]	As per R3.
Chargeable-User-ID	89	RFC-4372	0-1	0-1	Proxy without modification.	As per R3.
Calling-Station-Id	31	Usage as per RFC-3580	0-1	1	If provided it SHALL be formatted as per R3 and forwarded. If not provided then the AIF SHALL populate calling Station Id with the MAC address set to	If the MAC address is set to 00-00-00-00-00-00 the HAAA must ignore this attribute.

Attribute	TYPE	Description	WRIX Access-Request	R3 Access-Request	AIF Processing Instruction	VAAA or HAAA Processing Instructions
					the following string: 00-00-00-00-00-00. (Note: The WiMAX H-AAA must ignore this value.)	
Acct-Session-Id	44	RFC2865	0-1	0-1	If this value is in the Access-Request then the AIF may include this attribute.	The HAAA may ignore this attribute if received in the Access-Request.
Event-Time-Stamp	55	RFC2869	1	0	The AIF SHALL not include this attribute in an Access-Request message.	The HAAA MUST ignore this attribute if received in the Access-Request
Location-Name	26/2 (vendor =14122)	WRIX specification	1	0-1	FFS, the AIF may be able to translate this attribute to the Operator-Name attribute.	If received, the HAAA MAY ignore this attribute.
Venue-Class	26/40 (vendor =3414)	WRIX specification	0-1	0-1	FFS, the AIF may be able to translate this attribute to the Operator-Name attribute.	If received, the HAAA MAY ignore this attribute.
WiMAX-Capability	26/1	Identifies the WiMAX Capabilities supported by the NAS. Indicates capabilities selected by the RADIUS server.	0	1	SHALL be generated with the following information: WiMAX-Release = 1.5 Accounting-Capabilities = 0 or 0x01. All other attributes omitted.	As per R3.
NAS-Identifier	32	RFC2865	0	1	SHOULD be set to the FQDN of the NAS whose IP address appears in the NAS-IP-Address. If this is not possible, then both NAS-IP-Address and the NAS-Identifier SHALL be set to the NAS-IP-Address and NAS-Identifier of the AIF.	
NAS-Port-Type	61	RFC2865	0	1	AIF SHALL set to the value of 19 (Wireless 802.11)	
GMT-Time-	26/3	The offset in seconds from	0	1	SHALL be generated by with the GMT Offset	

Attribute	TYPE	Description	WRIX Access-Request	R3 Access-Request	AIF Processing Instruction	VAAA or HAAA Processing Instructions
Zone-Offset		GMT at the NAS.			where the Hotspot is physically located, if not know then to the GMT Offset where of the AIF.	
Visited-Framed-IP-Address	26/79	WiMAX	0	0		
WiMAX-Session-Id	26/4	WiMAX	0	0-1	As per WiMAX. The AIF shall receive the WiMAX-Session-Id in the access-accept and shall use it for all subsequent Access-Request for this session.	
BS-ID	26/46	WiMAX	0	0		
BS-Location	26/88	WiMAX	0	0		
NAP-ID	26/45	WiMAX	0	0		
NSP-ID	26/57	WiMAX	0	0		
PMIP-Authenticated-Network-Identity	26/78	WiMAX	0	0		
State	24	RFC2865	0	0-1	Usage as per RFC and WiMAX	
Visited-Framed-IPv6-Prefix	26/80	WiMAX	0	0		
Visited-Framed-Interface-Id	26/81	WiMAX	0	0		
Operator-Name	126	RFC5580 and WiMAX	0	0-1	FFS: Included if AIF can convert WRIX Location-Name to Operator-Name	
NAS-IPv6-Address	95	NAS-IPv6 address.	0	0-1	As per WiMAX usage	

Table 20-2 – Access-Accept Mapping From WiMAX R3 to WRIX Access-Accept

Attribute	TYPE	Description	R3 Access-Accept	WRIX Access-Accept	AIF Processing Instruction	VAAA or HAAA Processing Instructions
User-Name	1		0	0		HAAA MUST not send User-Name in Access-Accept even if allowed by WiMAX R3.
Service-Type	6		0-1	0	AIF SHALL ignore Service-Type received in Access-Accept	HAAA SHOULD NOT send service type to WRIX.
Framed-MTU	12		0-1	0	AIF SHALL ignore Framed-MTU	HAAA server SHOULD NOT send Framed-MTU
EAP-Message	79		1-n	1-n	As per RFC3579	As per WiMAX
Message-Authenticator	80		1	1	As per RFC3579	As per WiMAX
WiMAX-Capability	26/1	WiMAX	1	0	Processed locally by AIF.	As per WiMAX. WiMAX-Release(1): 1.5 WiMAX-Release: 1.4 WiMAX-Accounting-Capabilities(2): No-Accounting(0) WiMAX-Accounting-Capabilities: No-
Chargeable-User-Identity	89	RFC 4372	0-1	0-1	Forward to WRIX	As per WiMAX
Class	25	IETF	0-1	0-1	Forward to WRIX	As per WiMAX
Framed-IP-Address	8	IETF	0	0		MUST NOT send Framed-IP address.
Visited-Framed-IP-Address	26/79	WiMAX	0-1	0	MUST NOT Forward	As per WiMAX
Session-Timeout	27		0-1	0-1	Forward. According to WRIX Session-Timeout is used to terminate the session and not to trigger reauthentication.	As per WiMAX
Terminati	29		0-1	0-1	. If not received over	If included,

Attribute	TYPE	Description	R3 Access-Accept	WRIX Access-Accept	AIF Processing Instruction	VAAA or HAAA Processing Instructions
on-Action					R3 the AIF shall insert this attribute and set the value to 0.	SHALL set the value to 0.
WiMAX-Session-Id	26/4		1	0	MUST Store locally to be used for subsequent Access-Request messages for this session.	As per WiMAX
MSK	26/5		0-1	0	MUST be converted to MS-MPPE-Send-Key and MS-MPPE-Receive-Key	As per WiMAX
MS-MPPE-Send-Key	26/17 Vendor id = 311		0	0-1	AIF MUST converts MSK received in Access-Accept to MS-MPPE-Send-Key as per RFC TBD	
MS-MPPE-Recv-Key	26/17 Vendor id = 311		0	0-1	AIF MUST converts MSK received in Access-Accept to MS-MPPE-Recv-Key as per RFC TBD	
Packet-Flow-Descriptor-V2	26/84		0	0		
QoS-Descriptor	26/29		0	0		
VLANTag Processing-Descriptor	26/211		0	0		
Mobility-Access-Classifier	26/89		0	0		
Acct-Interim-Interval	85		0-1	0-1	Forward	As per WiMAX
Time-Of-Day-Time	26/20		0	0		
PIMP-Authenticated-Identity	26/78		0	0		
DNS	26/52		0	0		
State	24		0-1	0	MUST conform to RFC2865	As per WIMAX
Framed-IPv6-Prefix	97		0	0		

Attribute	TYPE	Description	R3 Access-Accept	WRIX Access-Accept	AIF Processing Instruction	VAAA or HAAA Processing Instructions
Framed-Interface-Id	96		0	0		
Visited-Framed-IPv6-Prefix	26/80		0	0		
Visited-Framed-Interface-Id	26/81		0	0		
MS-Authenticated	26/90		0	0		
Operator-Name	126		0-1	0	AIF stores locally to be included in Accounting	As per WiMAX
Certified-MS-Feature-List-For-GW	26/139		0	0		
Certified-MS-Feature-List-For-BS	26/140		0	0		
Port-Limit	62		0-1	0-1	Forward	As per RFC2865
Reply-Message	18		0-1	0-1	Forward	As per RFC2865 or RFC3579
Idle-Timeout	28		0-1	0-1	Forward	As per RFC2865
Acct-Session-ID	44		0	0		
Error-Cause	101		0	0		

Table 20-3 – Access-Challenge Mapping From WiMAX® R3 to WRIX Access-Accept

Attribute	TYPE	Description	R3 Access-Challenge	WRIX Access-Accept	AIF Processing Instruction	VAAA or HAAA Processing Instructions
EAP-Message	79		1-n	1-n		
Message-Authenticator	80		1	1		
Session-	27		0	0		

Attribute	TYPE	Description	R3 Access-Challenge	WRIX Access-Accept	AIF Processing Instruction	VAAA or HAAA Processing Instructions
Timeout						
WiMAX-Session-Id	26/4		0-1	0		
State	24		0	0-1	Store by AIF which complies with RFC2865 usage.	

19.1.2 Accounting Message Mapping From WRIX to WiMAX® R3

Only accounting stop messages are shown. Translation of Accounting Start messages and Interim are trivial. In the case of Accounting Request Start message, the AIF MUST always insert Beginning-of-Session (26/22) set to True.

Table 20-4 – Accounting Message Mapping From WRIX to WiMAX® R3

Attribute	TYPE	Description	WRIX Acct-Request	R3 Acct-Request	AIF Processing Instruction	HAAA Processing Instructions
User-Name	1		1	1		
Acct-Multi-Session-Id	50		0	1	AIF SHALL insert the WiMAX-Session-Id received in Access-Accept	
Acct-Link-Count	51		0	0		
PDFID	26/26		0	0		
SDFID	26/27		0	0		
Framed-IP-Address	8		0	1	If the IP address is not available then the AIF SHALL set the IP address to ALL ZERO.	
Framed-IPv6-Prefix	97		0	0		
Framed-Interface-Id	96		0	0		
Visited-Framed-IP-Address	26/79		0	0		
Visited-Framed-IPv6-Prefix	26/80		0	0		
Visited-Framed-Interface-Id	26/81		0	0		

MSID	BUG WIMAX MISSING ID		0	0		
MCBCS-Transmission-Zone-ID	26/113		0	0		
Calling-Station-Id			0	0-1	MAY be available from Access-Request message. If provided it SHALL be formatted as per R3 and forwarded. If not provided then the AIF SHALL populate calling Station Id with the MAC address set to the following string: 00-00-00-00-00-00. (Note: The WiMAX H-AAA must ignore this value.)	
NAS-IP-Address	4		1	1	Must be included since NAS-ID is not included	
Acct-Status-Type	40		1	1		
Acct-Input-Octets	42		1	1		
Acct-Output-Octets	43		1	1		
Acct-Session-ID	44		1	1		
Acct-Session-Time	46		1	1		
Acct-Input-Packets	47		1	1		
Acct-Output-Packets	48		1	1		
Acct-Terminate-Cause	49		1	1		
Acct-Input-Gigawords	52		0-1	0-1		
Acct-Output-Gigawords	53		0-1	0-1		
Class	25		0-1	0-1		
Event-Timestamp	55		1	1		

Location-Name	26/2 vendor id = 14122		1	0	Convert to Operator-name if possible.	
Chargeable-User-Id	89		0-1	0-1		
Venue-Class			0-1	0		
Session-Continue	26/21		0	0		
Network-Technology	26/23		0	0	AIF does not know the network technology and thus must omit this attribute.	
Hotline-Indication	26/24		0	0		
Prepaid-Indicator	26/25		0	0		
Idle-Mode-Transition	26/44		0	0		
Count-Type	26/59		0	1	AIF must set the value to 0x00 indicating uncompressed counts. Note AIF has no way to determine if this is true.	
NAS-Port-Type	61		0	0-1		
MCBCS-Service-Type	111		0	0		
Transport-Type	112		0	0		
NAS-ID	32		0	0		
NAS-Port-Type	61		0	0-1	If provided SHALL be set to the value of 19 (Wireless 802.11)	
HA-IP-MIP4	26/6		0	0		
HA-IP-MIP6	26/7		0	0		
NAS-IPv6-Address	95		0	0		
NAP-ID	26/45		0	1	AIF must insert a NAP-ID	
BS-ID	26/46		0	0		
Location	26/47 or IETF attribute		0	0		

NSP-ID	26/57		0	0-1	Either the AIF MUST insert the id of the NSP or be delegated t the VCSN	
Operator-Name	126		0	0-2	If the AIF included the Operator-Name in the Access-Request packet, it SHALL include it in the accounting packets. If the AIF received the Operator-Name attribute (containing the Home operator's WRI-Code) in an Access-Accept, it SHALL include it in the Accounting Start packet. If the attribute is included in the Accounting Start packet, it SHALL also be included in the Accounting Interim-Update (if used) and Accounting Stop packets.	
Active-Time	26/39		0	0		
Acct-Delay-Time	41		0	0		
Control-Packets-In	26/31		0	0		
Control-Octets-In	26/32		0	0		
Control-Packets-Out	26/33		0	0		
Control-Octets-Out	26/34		0	0		
Acct-Input-Packets-Gigaword	26/48		0	0		
Acct-Output-Packets-Gigaword	26/49		0	0		
Uplink Flow-Description	26/50		0	0		
Downlink Flow-Description	26/62		0	0		
Uplink-Granted-QoS	26/30		0	0		

Downlink-Granted-QoS	26/63		0	0		
Flow-Descriptor-V2	26/83		0	0		