



**MSF Architecture for WiMAX Access Network
Tile**

MSFR4-ARCH-WIMAX-FINAL

MultiService Forum Implementation Agreement

Contribution Number: msf2008.017.05

Document Filename: MSFR4-ARCH-WIMAX-FINAL

Working Group: Architecture

Title: Architectural Framework for the WiMAX Access Tile

Editor: Mary Chion

mchion@zteusa.com

Francisco de Carvalho

francisco.carvalho@bt.com

Anil Gupta

argupta@alcatel-lucent.com

Working Group Chairperson: Stuart Walker

Date: July 9, 2008

Abstract:

The MultiService Forum (MSF) is responsible for developing Implementation Agreements or Architectural Frameworks which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements are formally ratified via a Straw Ballot and then a Principal Member Ballot.

Draft MSF Implementation Agreements or Architectural Framework may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement or Architectural Framework is given a document number in the same manner as an Implementation Agreement.

Draft Implementation Agreements may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement or Architectural Framework remains published until the Technical Committee votes to withdraw it.

After being ratified by a Principal Member Ballot, the Draft Implementation Agreement or Architectural Framework becomes final. Earlier Draft Implementation Agreements or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The use of capitalization of the key words "MUST", "SHALL", "REQUIRED", "MUST NOT", "SHOULD NOT", "SHOULD", "RECOMMENDED", "NOT RECOMMENDED", "MAY" or

“OPTIONAL” is as described in section V-B of the MSF Technical Committee Operating Procedures.

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

Note: Attention is called to the possibility that use or implementation of this MSF Implementation Agreement may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Implementation Agreement, no position is taken by MSF as its Members with respect to the existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MSF of this Implementation Agreement. Moreover, the MSF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MSF Implementation Agreement, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention.

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements

are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum
48377 Fremont Blvd., Suite 117
Fremont, CA 94538 USA
Phone: +1 510 492-4050
Fax: +1 510 492-4001
info@msforum.org
<http://www.msforum.org>

I. The MultiService Forum

The MultiService Forum (MSF) is a global association of service providers, system suppliers and other organizations committed to developing and promoting open-architecture, multiservice communication systems. Founded in 1998, the MSF is an open-membership organization comprised of the world's leading telecommunications companies.

The MSF's activities include developing implementation agreements, promoting worldwide compatibility and interoperability, and encouraging input to appropriate national and international standards bodies.

As part of MSF's effort to drive and promote interoperability, the MSF has created a number of programs geared toward accelerating real world network deployments:

1. Global MSF Interoperability (GMI) events. GMI events provide a real-world setting for vendors to test their solutions and provide evidence that vendor products meet the interoperability standards set forth by MSF Implementation Agreements. Each MSF GMI event is built around a set of capabilities defined for a given release of the MSF Architecture.
2. Next Generation Network (NGN) Test Bed. The NGN test bed provides a facility to enable carriers and vendors to perform in-depth testing of a specific interface as defined in a given release of the MSF architecture.
3. Certification Programs. For more mature technologies the MSF can provide Certification of compliance to a given Implementation Agreement where MSF members believe that it is of value to the industry to do so.

II. An introduction to MSF documentation and GMI 2008

This document is part of the MSF Release 4 set of architectural, protocol and test documentation.

The MSF Release 4 Architecture is a physical implementation of the functional architectures that have been proposed by the key Standards Development Organizations. As such the MSF Release 4 Architecture represents the current state of the industry and it identifies current open interfaces between physically separate network elements.

MSF Implementation Agreements define the protocols to be used over specific open interfaces. Where possible MSF Implementation Agreements are based on industry standard protocols augmented with additional information so as to ensure interoperability between communicating network elements. This level of interoperability is achieved by closing any gaps and tightening any optional capabilities in those industry standards to remove the danger of mutually incompatible selections by vendors. An MSF Implementation Agreement is targeted at a given

release of the MSF architecture but can be used in any circumstance where an operator wishes to deploy the open interface and its functionality within their own network.

The MSF Release 4 architecture and its associated implementation agreements are used as the basis for GMI 2008. GMI 2008 is a global test event executed to demonstrate multi-vendor, multi-service interoperability based around IMS and includes IPTV and web based services.

As part of GMI 2008 a number of detailed test scenarios have been developed and a number of test plans defined. Test plans contain the set of test cases required to demonstrate a given MSF Release 4 capability and serve to exercise and validate the set of Implementation Agreements required to realize the capability.

Following the completion of GMI 2008 the MSF Release 4 architecture and individual implementation agreements will be updated if the testing identifies any deficiencies in the documents.

For more information about the scope of GMI2008 please go to <http://www.msforum.org>

III. Impact on previously published MSF documents

This is a new specification for MSF release 4 and GMI 2008.

Table of Contents

| | | |
|--------|--|----|
| 1. | Introduction..... | 9 |
| 1.1. | Scope..... | 9 |
| 1.2. | Tile Prefix | 9 |
| 1.3. | References..... | 9 |
| 1.4. | Definitions and Abbreviations | 9 |
| 1.4.1. | Definitions..... | 9 |
| 1.4.2. | Abbreviations..... | 11 |
| 2. | Purpose..... | 12 |
| 3. | Relationship with the MSF Architectural Framework..... | 12 |
| 4. | WiMAX Access Tile Architecture Overview..... | 14 |
| 5. | Trust | 14 |
| 6. | Element Definition..... | 15 |
| 6.1. | Mobile Station..... | 15 |
| 6.2. | Access Service Network | 15 |
| 6.2.1. | Base Station | 15 |
| 6.2.2. | Backhaul Network | 16 |
| 6.2.3. | ASN Gateway | 16 |
| 6.2.4. | Foreign Agent | 17 |
| 6.3. | Connectivity Service Network..... | 17 |
| 6.3.1. | Home Agent..... | 18 |
| 6.3.2. | AAA Server/Proxy..... | 18 |
| 6.3.3. | Policy Function (PF)..... | 18 |
| 6.3.4. | Access Location Server (ALS) | 19 |
| 7. | Principal Mode of Operation | 19 |
| 7.1. | Network Entry..... | 20 |
| 7.1.1. | Without PCC..... | 20 |
| 7.1.2. | With PCC | 22 |
| 7.2. | Authentication..... | 22 |
| 7.3. | QoS | 23 |
| 7.3.1. | Static QoS Management | 23 |
| 7.3.2. | Dynamic QoS Management..... | 23 |
| 7.4. | Mobility Management..... | 23 |
| 7.4.1. | Intra-ASN Mobility Management..... | 23 |
| 7.4.2. | Inter-ASN Mobility Management | 24 |
| 8. | Interface Description and Reference..... | 25 |
| 8.1. | External Interface..... | 25 |
| 8.2. | Internal Interface..... | 25 |

Table of Figures

| | |
|---|----|
| Figure 1: Generic Relationship of an Access Network Tile with MSF Architectural Framework | 13 |
| Figure 2: WiMAX Access Tile Architecture based on NWG | 14 |

1. Introduction

1.1. Scope

The MSF architecture required for the access domain can vary significantly depending on the technology which is being connected. However in order that the objective of a multi-service network can be realised it is necessary that whilst the architecture within the domain will vary, the interfaces towards the MSF Core Architecture Domain must be standardised. Each separate access architecture supporting a different technology is referred to as an Access Tile.

This document defines the Access Tile Architecture for a WiMAX access network.

1.2. Tile Prefix

The Tile Prefix for the Baseband access tile SHALL be “WM”

1.3. References

- [1] MSF Release 4 Architecture (MSF-ARCH-004.00-FINAL)
- [2] WiMAX Forum Network Architecture – Stage 2 Release 1.0.0, February, 2007
- [3] WiMAX Forum Network Architecture – Stage 3 Release 1.0.0, March, 2007
- [4] WiMAX Forum Network Architecture: Policy and Charging Control Release 1.5, Feb. 11, 2008
- [5] 3GPP TS 23.203: Policy Control and Charging Architecture
- [6] WiMAX Forum Network Architecture – NWG_LBS_baseline_v7

1.4. Definitions and Abbreviations

1.4.1. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", "OPTIONAL", "CONDITIONAL" and "IF" in this document are to be interpreted as described in the MSF Technical Committee Operating Procedures.

| | |
|----------------------|---|
| Access Network Block | The part of the MSF overall architecture framework that generically represents an access network, independent of its technology |
| Access Network Tile | A specification of the architecture for a specific access network technology or a grouping of similar access technologies. |

| | |
|-------------------------------|---|
| Access Services Network | The ASN is the access network within a WiMAX architecture |
| Connectivity Services Network | The CSN provides the core network functions of a service provider such as Authentication, IP Address allocation and routing to the Applications Plane |
| Diameter | A computer networking protocol for AAA (Authentication, Authorization and Accounting). It is a successor to RADIUS . |
| Internet Service Provider | The business entity that retails broadband service to the end customers. |
| MSF Core Architecture Blocks | The functionality contained in the Transport, Session and Common Blocks defines in the MSF Architecture [1] |
| Network Access Provider | The business entity that wholesales broadband service to ISPs. |
| Network Service Provider | The business entity that owns the WiMAX CSN and provides service to users. |

1.4.2. Abbreviations

| | |
|--------|---|
| A-PCEF | Access Network Policy and Charging Control Enforcement Function |
| ALS | Access Location Server |
| ASN | Access Service Network |
| BS | Base Station |
| CSN | Connectivity Service Network |
| DHCP | Dynamic Host Configuration Protocol |
| FA | Foreign Agent - A mobile IP Foreign Agent entity |
| HA | Home Agent - A mobile IP Home Agent entity |
| LBS | Location Base Service |
| MS | Mobile Station |
| NAP | Network Access Provider |
| NSP | Network Service Provider |
| NWG | WiMAX Network Working Group |
| PCEF | Policy and Charging Control Enforcement Function |
| PMIP | Proxy MIP |
| RADIUS | Remote Authentication Dial-In User Service |
| SFA | Service Flow Agent - Establishes the default service flows for a subscriber, ready for use when sessions are established |

2. Purpose

The purpose of this document is to allow for the initial integration of a WiMAX network with the MSF R4 Framework and to support the GMI 2008 event.

It is anticipated that the following will be in scope:

- Network entry authentication
- IMS applications such as VoIP compliance to existing MSF Implementation Agreements, e.g. VoIP
- Non IMS applications which do not require core network authentication or which can authentication with MSF HSS directly
- Applications which can authentication directly with the Access Tile AAA component
- QoS management within a WiMAX access network only
- WiMAX Forum Profile C will be used as the primary focus to describe functional components but this does not affect the interfaces to the MSF R4 Core.
- IEEE 802.16e Standard will be used for L2 Radio Interface.

The following is may be performed as part interoperability

- End-End QoS/Application driven QoS which makes use of a TISpan RACS or 3GPP PCC component.
- Location service

3. Relationship with the MSF Architectural Framework

The MSF Release 4 architecture [1] introduced an Access Network Domain into its architectural framework (see Figure 1). The Access Network Domain has a number of standard interfaces defined that are independent of the network access technology. This allows the architectural framework to define the interaction between MSF core architecture domain and access network entities in order to support common capabilities such as extracting location information associated with access network attachment and managing access bandwidth allocation. As access technologies differ from one another, so do the mechanisms internal to that access network domain that support these interfaces. To accommodate this, a generic access domain is defined with the MSF architectural framework with common interfaces. To facilitate adding different and multiple access networks to the overall architecture, each access network technology or group of similar technologies is defined in its own 'Access Network Tile' architecture that can be substituted for the generic access domain. Each Access Network Tile specifies how it operates internally and supports the common interfaces with the MSF Core Architecture Domain.

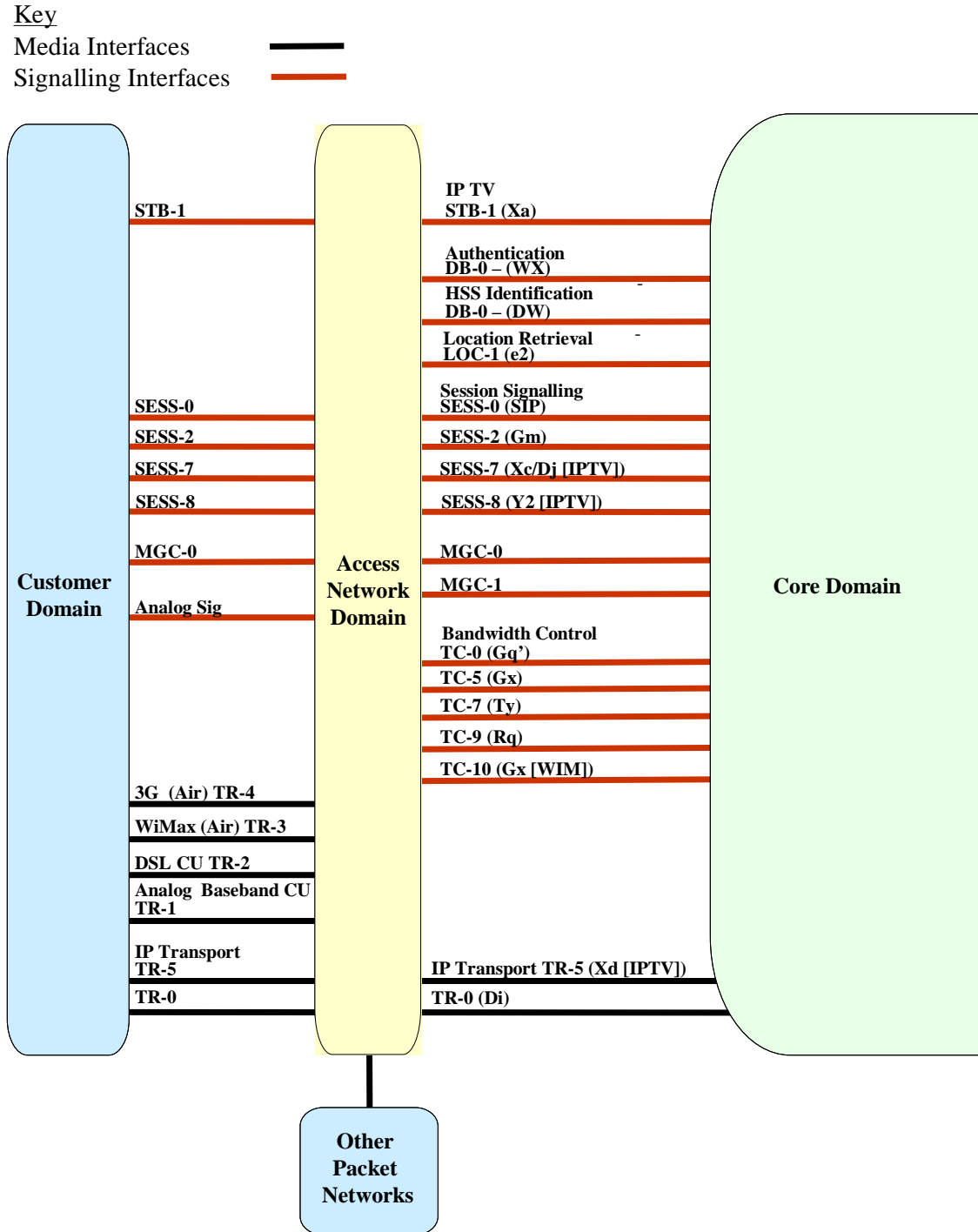


Figure 1: Generic Relationship of an Access Network Tile within MSF Architectural Framework

The common interfaces between the MSF Core Architecture Domain and the Access Domain are for Location Retrieval (LOC-1) and Bandwidth Control (TC-10) and are defined in the current Architectural Framework document for the release.

4. WiMAX Access Tile Architecture Overview

The WiMAX Access Tile architecture is shown below (Figure 2).

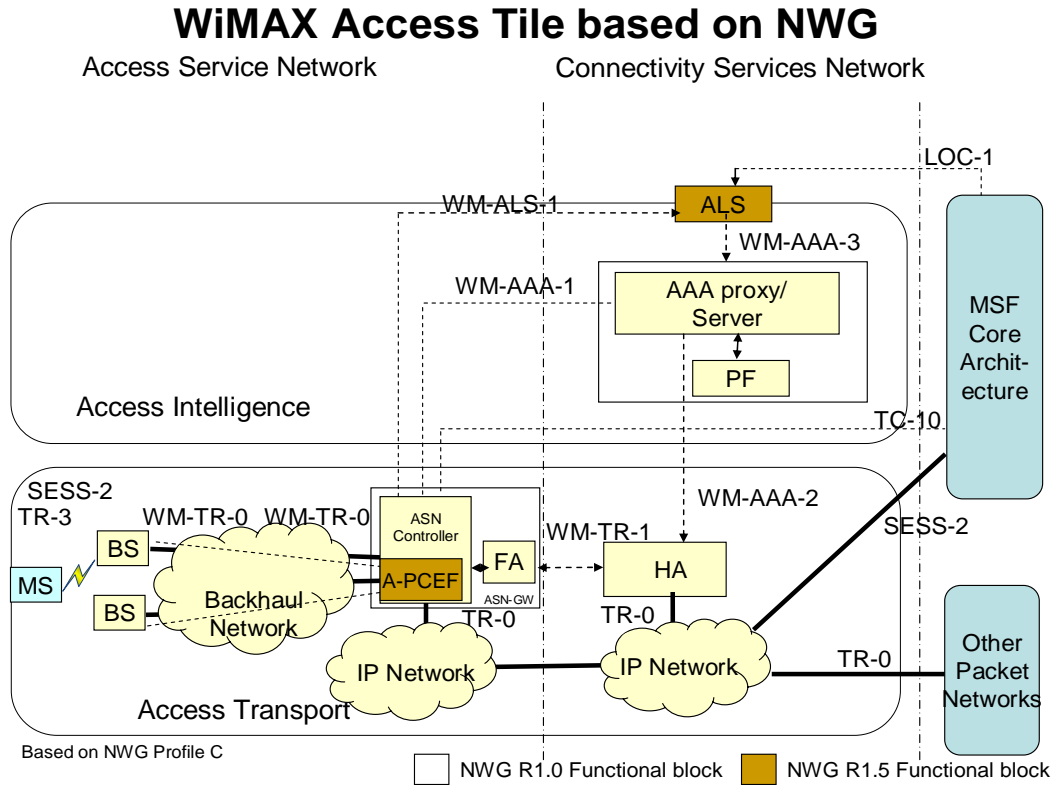


Figure 2: WiMAX Access Tile Architecture based on NWG

5. Trust

The WiMAX Access Tile may be part of the core trust domain or in a different trust domain depending on the deployment scenarios.

Where an ASN is being deployed in a Wholesale scenario, specific Trust/Security rules may need to be applied more strictly. For the purposes of this first release, both the ASN and CSN are assumed to be trusted with appropriate rules in the Firewall.

6. Element Definition

6.1. Mobile Station

Generalized mobile equipment set providing connectivity between subscriber equipment and a base station (BS). The Mobile Station MAY be a host or a CPE type of device that supports multiple hosts.

6.2. Access Service Network

Access Service Network (ASN) is defined as a complete set of network functions needed to provide radio access to a WiMAX subscriber. The ASN provides the following mandatory functions:

- WiMAX Layer-2 (L2) connectivity with WiMAX MS using 802.16(e)
- Network discovery and selection of the WiMAX subscriber's preferred NSP
- Transfer of AAA messages to WiMAX subscriber's Home Network Service Provider (H-NSP) for authentication, authorization and session accounting for subscriber sessions
- DHCP Relay or Proxy functionality for establishing Layer-3 (L3) connectivity with a WiMAX MS (i.e. IP address allocation)
- Quality of Service (e.g., Differentiated levels of QoS, Admission Control, Bandwidth management);
- Radio Resource Management

In addition to the above mandatory functions, for a portable and mobile environment, an ASN also supports ASN anchored mobility, CSN anchored mobility, Paging and ASN-CSN tunneling. An ASN comprises network elements such as one or more Base Station(s) and one or more ASN Gateway(s). The functional blocks supported by ASN are mapped into each network element according to NWG defined profiles. In WiMAX NWG Release 1.0.0 Stage 2 specification [2], three profiles are defined for ASN, Profile A, B and C. Each profile consists of different distribution of functional block within ASN, mainly between ASN GW and BS. Each profile consists of a different R6 interface (interface between BS and ASN GW). In NWG Release 1.5, only Profile B and C are still defined while Profile A was removed. The following sections define ASN entities based on Profile C. Other profiles may be considered in future versions of this document.

6.2.1. Base Station

The WiMAX Base Station (BS) is a logical entity that embodies a full instance of the WiMAX MAC and PHY in compliance with the IEEE 802.16 suite of applicable standards. A BS instance represents one sector with one frequency assignment. It incorporates scheduler functions for uplink and downlink air link resources.. Connectivity of a single BS to more than one ASN-GW may be required for load balancing or a redundancy option. BS is logical entity and one physical implementation of BS can have multiple BSs.

A BS supports the following key functions in addition to WiMAX MAC and PHY:

- Radio resource management
- Handover control (i.e. decision point of handover in controlled HO mode¹)
- Service flow management: service flow is defined within the scope of ASN
- Data path management

6.2.2. Backhaul Network

The backhaul network aggregates BS connections to an ASN-GW. This network can use IP Metro Solution, MPLS Network, or Microwave backhaul.

6.2.3. ASN Gateway

The ASN Gateway (ASN-GW) is a logical entity that represents an aggregation of Control Plane functional entities that are either paired with a corresponding function in the ASN (e.g. BS instance), a resident function in the CSN or a function in another ASN. The ASN-GW may also perform Bearer Plane routing or bridging function. An ASN-GW MUST support the following functions:

- Data path management function
- PMIP client (if PMIP is used)
- AAA Client
- Paging Controller
- Location register within ASN
- Authenticator/Key Distributor
- DHCP Proxy/Relay (DHCP Relay is optional in NWG R1.0.)
- Service Flow management

An ASN-GW MAY support the following functions:

- Foreign Agent (FA is mandatory in NWG R1.0)
- Access Network Policy and Charging Control Enforcement Function (A-PCEF)
- To support location update service, ASN-GW may generate an accounting recording which includes MS location information (i.e. BS ID is one option for a low density location service) when MS handover from one BS to another BS.

¹ For controlled HO mode ,the decision point in BS; for uncontrolled HO, the terminal can decide the target BS (but the selected BS can refuse)

- For a high density location service, WiMAX NWG R1.5 LBS Specification will be available in the future but is outside of the scope of MSF R4.

For every MS, a BS is associated with exactly one default ASN GW. However, ASN-GW functions for every MS may be distributed among multiple ASN-GWs located in one or more ASN(s). This component is considered to be fully resilient and failover to an ASN-GW at a different cluster and physical location is outside of the scope of this document.

6.2.4. Foreign Agent

A Mobile IP Foreign Agent is essentially a router which stores information about mobile nodes (Mobile Stations) visiting network for which it provides IP connectivity and control. Foreign agents advertise care-of addresses which are used by the Mobile IP protocol to route packets destined for a mobile node. The FA component provides IP mobility and manages a mapping between the Public Address (PoA) identifying the MS and its (current) layer 2 address & location routing IP packets to the final destination once it has unwrapped the outer IP in IP header arriving from the Home Agent.

Foreign Agent functionality is one function of ASN GW and MAY be provided as an independent router or as an integrated part of the ASN-GW

6.3. Connectivity Service Network

Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the WiMAX subscriber(s). A CSN MUST provide the following functions:

- MS IP address and endpoint parameter allocation for user sessions
- AAA proxy
- Policy, Admission and Charging Control based on user subscription profiles
- ASN-CSN tunneling support,
- WiMAX subscriber billing and inter-operator settlement records
- Inter-CSN tunneling for roaming
- Inter-ASN mobility

CSN MAY comprise network elements such as routers, AAA proxy/servers, user databases, Interworking gateway MSs. A CSN MAY be deployed as part of a Greenfield WiMAX NSP or as part of an incumbent WiMAX NSP.

An ASN-GW MAY support the following functions:

- AAA Server
- Internet access

- WiMAX services such as location based services, connectivity for peer-to-peer services, provisioning, authorization and/or connectivity to IP multimedia services and facilities to support lawful intercept services such as those compliant with Communications Assistance Law Enforcement Act (CALEA) procedures.

6.3.1. Home Agent

In Mobile Internet Protocol (Mobile IP), a home agent is a router on a mobile node's home network that maintains information about the device's current location, as identified in its care-of address. The home agent uses tunneling mechanisms to forward Internet traffic so that the device's IP address doesn't have to be changed each time it connects from a different location. A home agent may work in conjunction with a foreign agent, which is a router on the visited network.

In WiMAX, under the consideration of local breakout services, a home agent can also be assigned in the visited network based on the dynamic HA assignment. The user registers to the HA via TR-3, HA will apply for AAA to authorize the user, and assign an IP address to the user if successful and not have IP address.

6.3.2. AAA Server/Proxy

An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. The current standards by which devices or applications communicate with an AAA server are the RADIUS or DIAMETER.

An AAA Proxy is actually an AAA server which is located in the visited network. The function of AAA proxy is only distribution of the information of AAA server in the home network. The AAA proxy will also allow the NAP to police the AAA attributes received from the visited CSN and add additional AAA attributes that MAY be required by the NASs in the ASN. The AAA server/proxy supports user authentication/authorization for WiMAX access and maintains user information/profile related only to the access network. Addition authentication may occur through other network elements for service level registration.

To support location update/information, AAA may create an accounting record and transfer to the Access Location Server via AAA-3 when it receives MS events (registration, change of BS) and location from ASN-GW. Note that there are limitations with this approach and only a low granularity location (BS location and not x,y co-ordinates) is possible.

When Location R1.5 , higher granularity will be supported.

6.3.3. Policy Function (PF)

For WiMAX NWG R1.0, policy function is defined to maintain NSP's general policy rules and as well as application dependant policy rules. The PF is in charge of evaluating service requests again these policies when service flows are being established. As defined in NWG R1.0, the AAA may provision the PF with user's QoS profile and its associated policies. As the interface between AAA and PF is undefined in WiMAX NWG R1.0, PF is, in general, implemented as part of AAA.

6.3.4. Access Location Server (ALS)

Location service is currently being defined in WiMAX NWG R1.5. However, a simple location registration and update mechanism is being proposed which is aligned with the Broadband Access Tile approach.

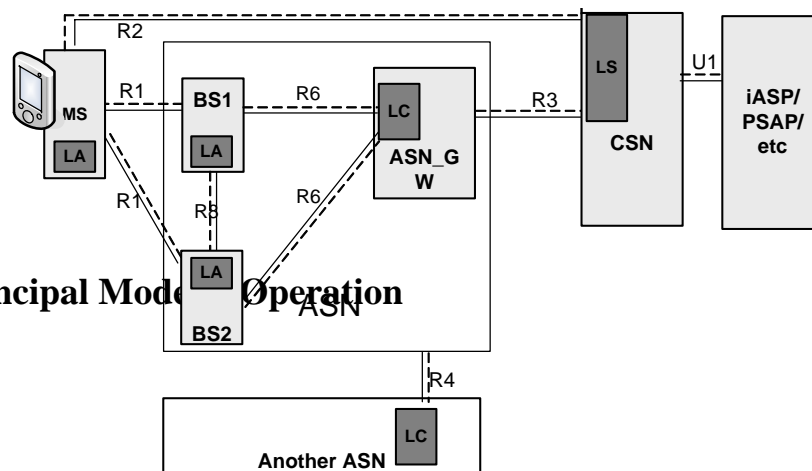
To support location update, the AAA may generate an accounting record containing MS location information and send to ALS. The accounting record shall contain:

- Mobile Station Identifier, e.g. MAC Address/X.509 certificate identified
- IP address allocated to the MS
- Base Station Identifier (BS ID)
- Date/Time

The ALS should forward MS location information to network elements in MSF core network over LOC-1 interface. The detailed definition may be vendor specific and is not subject to interoperability.

In addition, WiMAX NWG R1.5 is working on specification for the operation of location service (LBS). In the current baseline document [7] for LBS in WiMAX NWG R1.5, Location Server and Location Client are defined with Location Server located in CSN and Location Client as a functional block in ASN GW. The detail architecture and operation will be included after the specification is finalized and will replace the above description of ALS.

7. Principal Mode of Operation



7.1. Network Entry

7.1.1. Without PCC

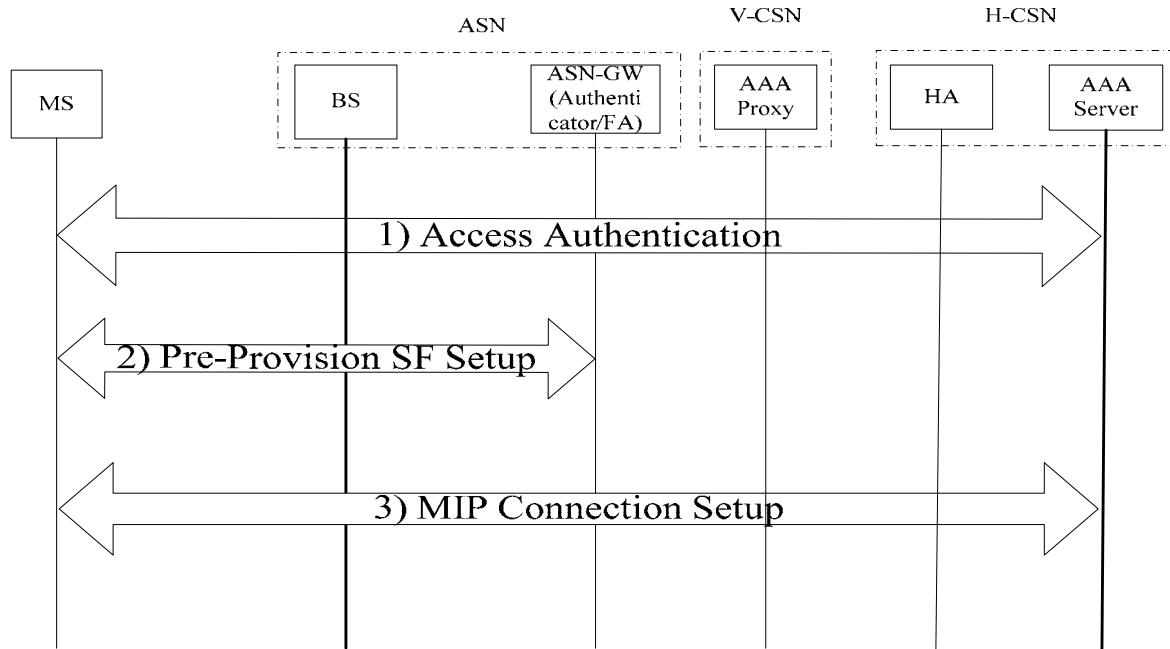


Figure 3: Network Entry Procedure

The initial network entry procedure for MS can be divided into three groups of steps as shown in Figure 3.

- 1) **Access Authentication:** In this procedure, the MS performs network scanning and acquires the network by establishing management connections with BS. After establishing management connection, authentication is performed by MS, authenticator function in ASN-GW and AAA server based on EAP. EAP messaging is carried in AAA-1 interface using RADIUS from Authenticator in ASN-GW to AAA server.
- 2) **Pre-Provision Service Flow setup:** As part of network entry operation, pre-provision service flows can be established by ASN. After MS is successfully authenticated/authorized and registered by the network, the authenticator in ASN GW initiates the procedure for pre-provisioned service flow establishment. The pre-provision service flows are defined as service flows that must be activated by the network after successful MS access authentication. A service flow is defined by IEEE 802.16 standard as a unidirectional flow of MAC service data units on a connection that is provided a particular QoS.

Among the set of pre-provisioned unicast service flows, the very first pair of service flows (i.e. for uplink and downlink) that are initiated by the ASN-GW are called the Initial Service Flows (ISF). ISF is a special kind of a Pre-Provisioned Service Flow which is used by the MS and the ASN to transfer delay tolerant control traffic such as standards-based IP configuration management and IP client application signaling (e.g.

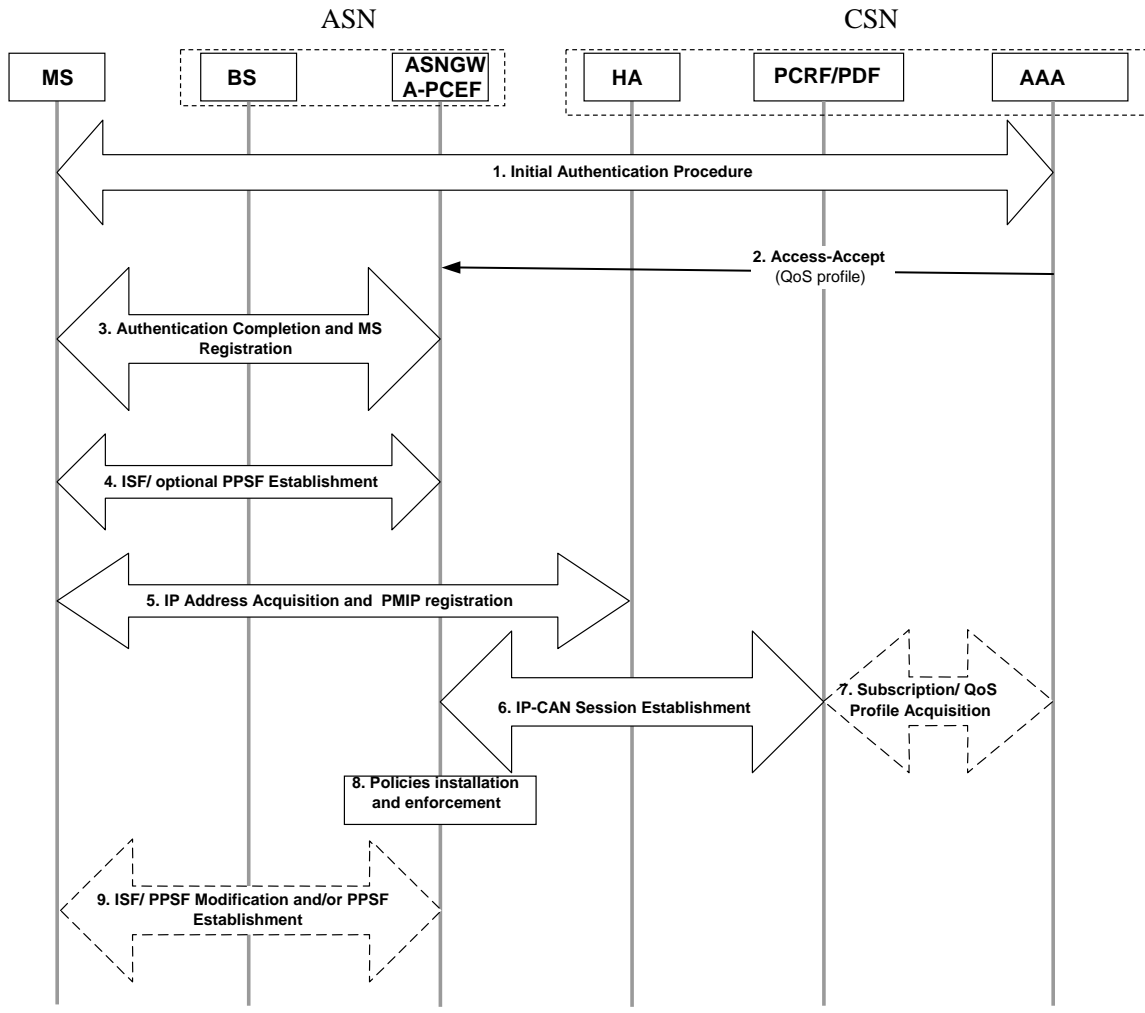
DHCP DISCOVERY, FA Advertisement, Mobile IP Registration, Router Advertisement, SIP signaling etc.) in case of IP as well as configuration management signaling required for Ethernet in case of Ethernet.

- 3) **MIP Connection Setup:** After the completion of ISF setup, MIP connection setup can be performed. In WiMAX NWG, PMIP and CMIP are both defined and can be optionally supported.

With PMIP solution, PMIP client resides within ASN GW and perform MIP mobility management on behalf of MS. During MIP connection setup, MS obtains PoA assignment and IP configuration from network using DHCP messaging carried over ISF. DHCP relay or proxy function is supported by ASN-GW to manage DHCP exchange between MS and DHCP server. At the completion of MS PoA assignment and IP configuration, DHCP relay/proxy function in ASN GW initiates PMIP client to start MIP registration with FA and HA. MIP registration exchange is performed between PMIP client, FA and HA. After completion of MIP registration, PMIP client triggers DHCP relay/proxy function to send DHCP ACK to MS.

With CMIP solution, MIP client resides within MS or host behind MS. MIP registration message exchange is performed by MS,FA and HA relaying through ASN.

7.1.2. With PCC



- 1, ~5 These steps are the same as described in previous section step 1-3.
6. The ASN-GW sends a PCC rule request to the PCRF/PDF.
7. PCRF may request user subscription profile from AAA.
8. The ASN-GW receives the PCC rules from the PDF/ PCRF.
9. For pre-provisioned service flows, if the PCC rules are different from the QoS profile received from AAA, the ASN-GW SHALL modify the initial service flow and/or pre-provisioned service flows per PCC rules. In addition, the ASN-GW may trigger pre-provisioned service flow setup according to PCC policy received from PCRF.

7.2. Authentication

In the architecture specified within WiMAX NWG R1.0.0 document, authentication and authorization must be based on EAP (Extensible Authentication Protocol, compliant to RFC 2904). EAP must be used for Device and User Authentication which must generate the MSK

and EMSK key. PKMv2 must be used to perform over-the-air User Authentication. PKMv2 transfers EAP over the IEEE 802.16 air interface between MS and BS in ASN. Depending on the Authenticator location in the ASN, a BS may forward EAP messages over Authentication Relay protocol to Authenticator. The AAA client on the Authenticator encapsulates the EAP in AAA protocol packets and forwards them via one or more AAA proxies to the AAA Server in the CSN of the home NSP, which holds the subscription with the Supplicant. In roaming scenarios, one or more AAA brokers with AAA proxies may exist between Authenticator and AAA Server. All AAA sessions always exist between the Authenticator and AAA server with optional AAA brokers just providing conduit for NAI realm based routing.

7.3. QoS

7.3.1. Static QoS Management

Under static QoS management, only pre-provisioned QoS profiles can be supported and enforced by WiMAX network. For each MS, a QoS profile is pre-provisioned and stored in AAA server. During network entry, ASN-GW obtains MS' QoS profile from AAA after the MS is successfully authenticated. After retrieving the QoS profile, the ASN-GW initiates service flow establishment within ASN to support the pre-provisioned QoS profile at the end of network entry procedure. When created, the service flows are maintained as long as the MS is active in the network and the QoS parameters can not be modified. In WiMAX NWG R1,0 [2] [3], only static QoS management is supported.

7.3.2. Dynamic QoS Management

Dynamic QoS management is supported by WiMAX networking using Policy and Charging Control (PCC) framework as defined in 3GPP [5]. The PCC framework allows applications like IMS applications to dynamically request QoS and charging attributes for a specified IP-flow from the access network where the framework verifies the authorization for the requested QoS.

With WiMAX PCC architecture [4], A-PCEF function is implemented in ASN-GW which interfaces with PCRS in core network. A-PCEF function is the enforcement point of PCC rules in ASN. PCRS includes PCRF function as defined in 3GPP [5] and Policy Distribution Function (PDF) for WiMAX[4]. PCRF encompasses policy control decision and PDF provides interworking function between WiMAX ASN and 3GPP core network. With PCC architecture, PCRF and A-PCEF can trigger QoS parameter modifications and service flow set up based on requests from application. WiMAX PCC architecture is being defined as part of NWG R1.5.

7.4. Mobility Management

The WiMAX mobility management consists of two mobility levels: Intra-ASN mobility and Inter-ASN mobility.

7.4.1. Intra-ASN Mobility Management

Intra-ASN mobility or micro mobility is when the MS moves between Data Path Functions while maintaining the same anchor DPF/FA sitting at the northbound edge of the ASN network (not involving a CoA update). The data flow between CSN and Data Path Functions pivots at

the anchor DPF/ FA. CSN is unaware of any mobility that occurs between ASN Data Plane Functions.

7.4.2. Inter-ASN Mobility Management

Inter-ASN Anchored Mobility Management or macro mobility is when the MS changes to a new anchor FA. The new FA and CSN exchange signaling messages to establish data forwarding path.

8. Interface Description and Reference

8.1. External Interface

| Interface Designation | WiMAX Equivalent | Description | Based Standard | MSF IA |
|-----------------------|------------------|---|--|--|
| LOC-1 | N/A | Access Location Function ALS to MSC Core | Diameter | msf2008.001.03/ MSF-IA- DIAMETER.008 |
| TR-0 | N/A | CSN to MSF or other packet networks | | N/A |
| TR-3 | R1 | MS to ASN | IEEE 802.16 e IEEE 802.16 g/d | N/A |
| TC-10 | PCC-R3-P | ASN-GW to MSF core network (PCRS) | Diameter | msf2008.106.00 |
| SESS-2 | R3/R5 | ASN to CSN, VCSN to HCSN, including tunneling, Authentication/accounting/QoS requirements | IETF based MIPv4/v6, GRE, Radius/Diameter | MSF-IA-SIP.016- FINAL |

8.2. Internal Interface

| Interface Designation | WiMAX Equivalent | Description | Based Standard | MSF IA |
|--|---|---|---|--------|
| Transport Interfaces | | | | |
| | | | | |
| WM-TR-0 | R6 | Between BS and ASN-GW for Profile C | WiMAX NWG R1.0 | N/A |
| WM-TR-1 | R3 | ASN to CSN, including tunnelling and Authentication/Accounting/QoS requirements | IETF based MIPv4/v6, GRE, Radius/Diameter | N/A |
| | | | | |
| Authentication, Authorization and Accounting Interfaces | | | | |
| WM-AAA-1 | R3 | AGW/FA to AAA server/proxy | RADIUS or DIAMETER | N/A |
| WM-AAA-2 | R3 | HA to AAA server | RADIUS or DIAMETER | N/A |
| WM-AAA-3 | No WiMAX equivalent is defined | AAA to Access Location Server – Accounting record for location information | RADIUS or DIAMETER | N/A |
| WM-ALS-1 | R3 | ASN-GW to Access Location Server | RADIUS or DIAMETER or | N/A |

| | | | | |
|--|--|--|------|--|
| | | | DHCP | |
|--|--|--|------|--|

--- End of Document ---