ARIB STD-T94

OFDMA Broadband Mobile Wireless Access System (WiMAX™ applied in Japan)

ARIB STANDARD

ARIB STD-T94 Version 1.4 (1/2)

Version 1.0	December	12th	2007
Version 1.1	March	19th	2008
Version 1.2	June	6th	2008
Version 1.3	September	25th	2008
Version 1.4	March	18th	2009

Association of Radio Industries and Businesses

General Notes to the ARIB Standards and Technical Reports

4. The establishment, revision and abolishment of ARIB Standards and Technical Reports are approved at the ARIB Standard Assembly, which meets several times a year. Approved ARIB Standards and Technical Reports are made publicly available in hard copy, CDs or through web posting, generally in about one month after the date of approval.
   This document may have been further revised therefore users are encouraged to check the latest version at an appropriate page under the following
   URL: http://www.arib.or.jp/english/index.html
5. The note about IPR (Industrial Property Rights) of the standard applies to the use of Essential IPR for the ARIB Standard in Japan. If the ARIB Standard is adopted outside Japan, Essential IPR will be treated in accordance with policies stated by each IPR owner. The IPR owners are, however, expected to apply the rules of the preface of the "Guidelines for Treatment of Industrial Property Rights in connection with the ARIB standard" (September 5, 1995, approved by the 1st Standard Assembly Meeting). In the preface of the Guidelines, it is stated that it is "desirable that the Essential IPR which relates to any or all parts of the contents of the ARIB Standards should be used free of charge by anyone and that it would not block the uses of such Essential IPR in any other country where such an ARIB Standard is adopted"

Preface

INTRODUCTION

Association of Radio Industries and Businesses (hereinafter ARIB) investigates and summarizes the basic technical requirements for various radio systems in the form of “technical standard (ARIB STD)”. These standards are being developed with the participation of, and through discussions amongst various radio equipment manufacturers, operators and users.

ARIB standards include “government technical standards” (mandatory standards) that are set for the purpose of encouraging effective use of frequency resources and preventing interference, and “private technical standards” (voluntary standards) that are defined in order to guarantee compatibility between radio facilities, to secure adequate transmission quality as well as to offer greater convenience to radio equipment manufacturers and users, etc.

An ARIB STANDARD herein is published as " OFDMA Broadband Mobile Wireless Access System (WiMAX™ applied in Japan)". In order to ensure fairness and transparency in the defining stage, the standard was set by consensus of the standard council with participation of interested parties including radio equipment manufacturers, telecommunication operators, broadcasters, testing organizations, general users, etc. with impartiality.

ARIB sincerely hopes that this standard be utilized actively by radio equipment manufacturers, telecommunications operators, and users, etc.

INDUSTRIAL PROPERTY RIGHTS (IPRs)

Although this ARIB Standard contains no specific reference to any Essential Industrial Property Rights relating thereto, the holders of such Essential Industrial Property Rights state to the effect that the rights listed in Attachment 1 and 2, which are the Industrial Property Rights relating to this standard, are held by the parties also listed therein, and that to the users of this standard, in the case of Attachment 1 (selection of option 1), such holders shall not assert any rights and shall unconditionally grant a license to practice such Industrial Property Rights contained therein, and in the case of Attachment 2 (selection of option 2), the holders shall grant, under the reasonable terms and conditions, a non-exclusive and non-discriminatory license to practice the Industrial Property Rights contained therein. However, this does not apply to anyone who uses this ARIB Standard and also owns and lays claim to any other Essential Industrial Property Rights of which is covered in whole or part in the contents of provisions of this ARIB Standard.

List of Essential Industrial Property Rights (IPRs)

The lists of Essential Industrial Property Rights (IPRs) are shown in the following. Attachments.

Attachment 1　List of Essential Industrial Property Rights (selection of option 1)
Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

Contents

― Fascicle 1 ―

Chapter 1 General Descriptions

1.1 Outline

This standard specifies requirements of the radio equipment of radio stations stipulated in the Ministry of Internal Affair and Communications (MIC) Ordinance Regulating Radio Equipment, Article 49.28 (this refers to the radio equipment of radio stations of OFDMA Broadband Mobile Wireless Access System) using 2.5 GHz band with 5 ms of transmission burst repetition period. It also specifies the radio communication for OFDMA Broadband Mobile Wireless Access System using 2.5 GHz band with 5 ms of transmission burst repetition period (hereinafter referred to as "Mobile WiMAX™ System") defined as the technology for personal wireless broadband services based on all-IP core network.

The standard shall be in accordance with MIC Ordinance Regulating Radio Equipment, Article 49.28 (including related notifications) when the Mobile WiMAX facilities are used in Japan. The system shall also conform to the WiMAX™ mobile System Profile and the WiMAX End-to-End Network Systems Architecture specified by WiMAX Forum®. It should be noted that the mobile System Profile refers to IEEE802.16-2004 and IEEE802.16e-2005 for the specifications of physical layer and MAC layer.

1.2 Scope of the Standard

The Mobile WiMAX network consists of Mobile Station(MS), Access Service Network (ASN) and Connectivity Service Network (CSN) , and the scope of the standard is shown in Figure 1-1.

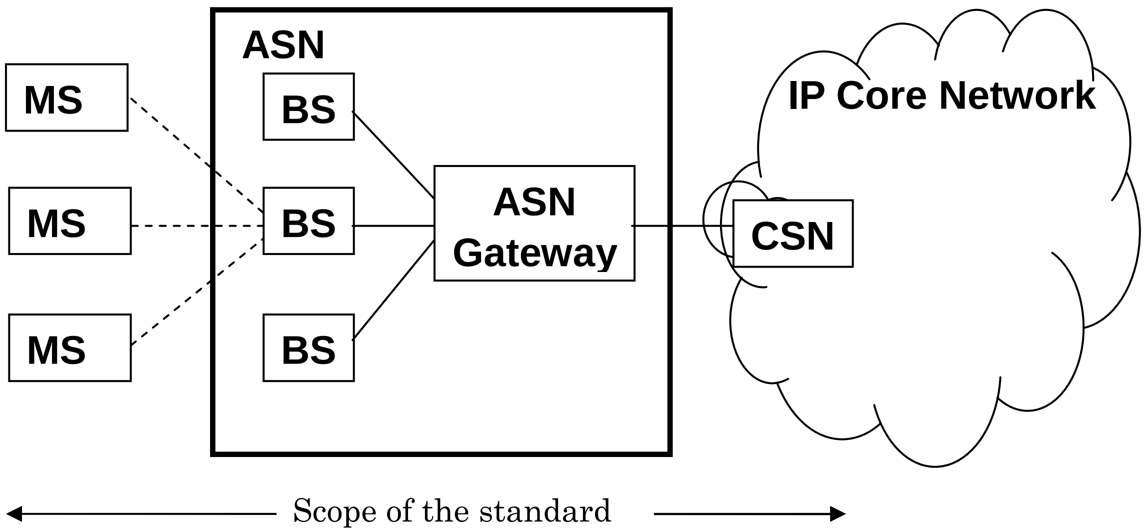


Figure 1-1 Configuration of Mobile WiMAX Network

MS is used by the end users to access the network. ASN comprises base stations (BS) and ASN gateways. BS is responsible for providing the air interface to the MS, while ASN gateway typically acts as layer 2 traffic aggregation within an ASN. CSN provides IP connectivity and all IP core network functions.

This standard defines the minimum level of specifications required for connection and services for the Mobile WiMAX system. This consists of three different specifications, i.e., Japanese regulatory specifications applied for radio systems, Physical and MAC layers specifications and Upper layers specifications. The Japanese regulatory specifications are developed by national regulatory administration, i.e. MIC. The physical and MAC layers specifications and the Upper layers specifications are developed by international standardization organization, i.e. IEEE802.16 Working group and WiMAX Forum, respectively.

This standard is intended to combine the national regulations and the international specifications, however in case of inconsistency between them, the national regulations shall prevail. The national regulations are the mandatory requirements for operation of the Mobile WiMAX in Japan.

The physical layer and MAC layer specifications are produced by IEEE802.16 Working Group in two documents, IEEE802.16-2004 and IEEE802.16e-2005. These documents offer a variety of fundamentally different design options in physical layer and MAC layer. For practical reasons of interoperability, WiMAX Forum defined a limited number of system profiles from these documents and summarized in WiMAX mobile system profile.

Since IEEE802.16-2004 and IEEE802.16e-2005 specifications do not define the end-to-end WiMAX network, WiMAX Forum has developed a network reference model called End-to-End Network Systems Architecture, to serve as an architecture framework for WiMAX deployment and to insure interoperability among various WiMAX equipment and operators.

1.3 Reference Regulations

The acronyms of the referenced regulations used in this standard are as follows;

ORE : Ordinance Regulating Radio Equipment

NT: Notification of the Ministry of Posts and Telecommunications if issued in 2000 or earlier, and a Notification of the Ministry of Internal Affairs and Communications if issued in 2001 or later

1.4 Reference Documents

- WiMAX Forum mobile System Profile v1.40
- WiMAX End-to-End Network Systems Architecture Stage 2-3 Release 1.1.0

Chapter 2 System overview

The IEEE802.16 Working Group develops and supports the IEEE802.16 air interface standard for Broadband Wireless Access systems. The amendment IEEE Std 802.16e-2005 along with the base IEEE Std 802.16-2004 provides the basis for the Mobile WiMAX air interface for combined fixed and mobile broadband wireless access.

IEEE Std 802.16 offers a flexible set of parameters and features to meet a range of global requirements. Due to this flexibility, interoperability with respect to the required features needs to be to ensured. Interoperability testing is a key function of the WiMAX Forum. Therefore, the WiMAX Forum has developed profiles specifying particular features and parameter sets from IEEE 802.16 sufficient to ensure interoperability.

The Mobile WiMAX RTT is consistent with the WiMAX Forum Mobile System Profile being commercialized by members of WiMAX Forum under the name “Mobile WiMAX ™”. The WiMAX Forum Mobile System Profile as illustrated in Figure 2-1, is derived from the mandatory and optional feature sets described in IEEE Std 802.16. This profile is used for air interface certification to foster global interoperability. WiMAX Forum Mobile profiles include recommended 5 and 10 MHz bandwidth, aligned with Mobile WiMAX proposal, for global deployment.

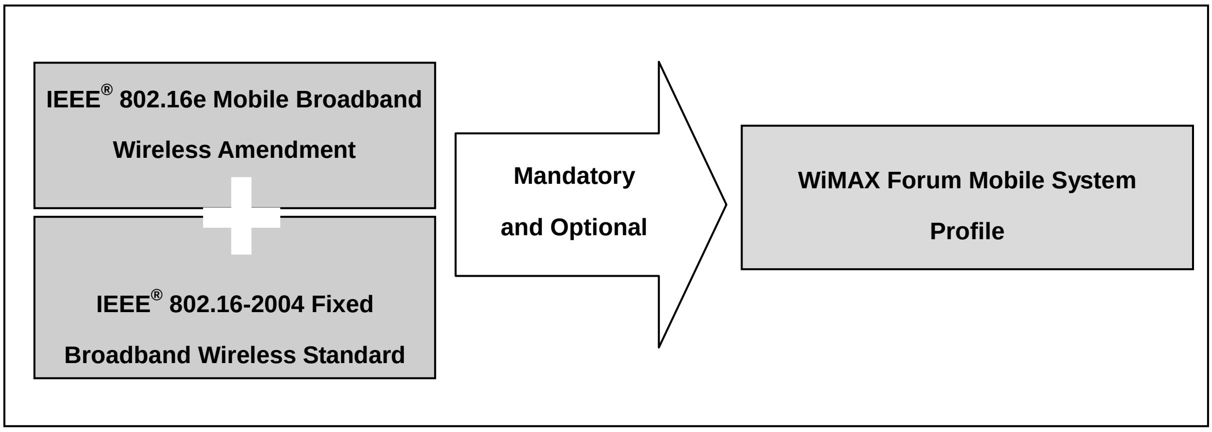


Figure 2-1 WiMAX Forum Mobile System Profile

The WiMAX Mobile System Profile supports the deployment of fully interoperable systems compatible with Mobile WiMAX. The profile includes optional Base Station features providing flexibility for various deployment scenarios and regional requirements to enable optimization for capacity, coverage, etc.[1]

2.1 Mobile WiMAX Network Architecture

The Mobile WiMAX radio interface is suitable for use in an all-IP architecture, with support for IP-based packet services. This allows for scalability and rapid deployment since the networking functionality is primarily based on software services.

In order to deploy successful and operational commercial systems, there is need for support beyond the IEEE802.16 air interface specifications, which only address layers 1 and 2 (PHY and MAC). The WiMAX Forum specifies the Mobile WiMAX Network Architecture describing the upper layer of the Radio Access Network and Core Network. Furthermore, the systems can also operate with core network of other IMT-2000 systems.

2.1.1 Architecture Principles

The following basic tenets have guided the Mobile WiMAX Network Architecture development.

1. The architecture is based on a packet-switched framework, including native procedures based on IEEE Std 802.16, appropriate IETF RFCs and Ethernet standards.
2. The architecture permits decoupling of access architecture (and supported topologies) from

[1] Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation.
http://www.wimaxforum.org/technology/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf

connectivity IP service. Network elements of the connectivity system are independent of the IEEE802.16 radio specifics.

3. The architecture allows modularity and flexibility to accommodate a broad range of deployment options such as:
   - Small-scale to large-scale (sparse to dense radio coverage and capacity) networks
   - Urban, suburban, and rural radio propagation environments
   - Licensed and/or licensed-exempt frequency bands
   - Hierarchical, flat, or mesh topologies, and their variants
     - Co-existence of fixed, nomadic, portable and mobile usage models

Support for Services and Applications: The end-to-end Mobile WiMAX Network Architecture includes a) Support of voice, multimedia services and other mandated regulatory services such as emergency services and lawful interception, b) Access to a variety of independent Application Service Provider (ASP) networks in an neutral manner, c) Mobile telephony communications using VoIP, d) Support interfacing with various interworking and media gateways permitting delivery of incumbent/legacy services translated over IP (for example, SMS over IP, MMS, WAP) to WiMAX access networks and e) Support delivery of IP Broadcast and Multicast services over WiMAX access networks.

Interworking and Roaming is another key strength of the end-to-end Mobile WiMAX Network Architecture with support for a number of deployment scenarios. In particular, there will be support of a) Loosely-coupled interworking with existing wireless networks such as those specified in 3GPP and 3GPP2 or existing wireline networks such as DSL and MSO, with the interworking interface(s) based on a standard IETF suite of protocols, b) Global roaming across WiMAX operator networks, including support for credential reuse, consistent use of AAA for accounting and billing, and consolidated/common billing and settlement, c) A variety of user authentication credential formats such as subscriber identify modules (SIM/USIM, R-UIM), username/password, digital certificates.

2.2 WiMAX Network Reference Model

IEEE Std 802.16 specifies a radio interface but not the network in which it is to be used, instead leaving an open interface to higher network layers. The WiMAX Forum specifies the Network Reference Model (NRM) to describe a practical and functional network making use of the Mobile WiMAX air interface. This NRM is described here because it serves as a framework for evaluating the performance of the Mobile WiMAX radio interface.

The NRM is a logical representation of the network architecture. The NRM identifies functional entities and reference points over which interoperability is achieved between functional entities. The architecture has been developed with the objective of providing unified support of functionality needed in a range of network deployment models and usage scenarios (ranging from nomadicity to full mobility).

Figure 2-2 illustrates the NRM, consisting of the logical entities MS, ASN, and CSN, as well as clearly identified reference points for interconnection of the logical entities. The figure depicts the key normative reference points R1-R5. Each of the entities, MS, ASN and CSN, represents a grouping of functional entities. Each of these functional entities may be realized in a single physical device or may be distributed over multiple physical devices according to allocation defined by ASN profiles[2].

The intent of the NRM is to allow multiple implementation options for a given functional entity, and yet achieve interoperability among different realizations of functional entities. Interoperability is based on the definition of communication protocols and data plane treatment between functional entities to achieve an overall end-to-end function, for example, security or mobility management. Thus, the functional entities on either side of a reference point represent a collection of control and bearer plane end-points.

2 An ASN profile represents an allocation of functional entities (e.g. authenticator, radio resource manager, etc.) to the various elements belonging to the access network.

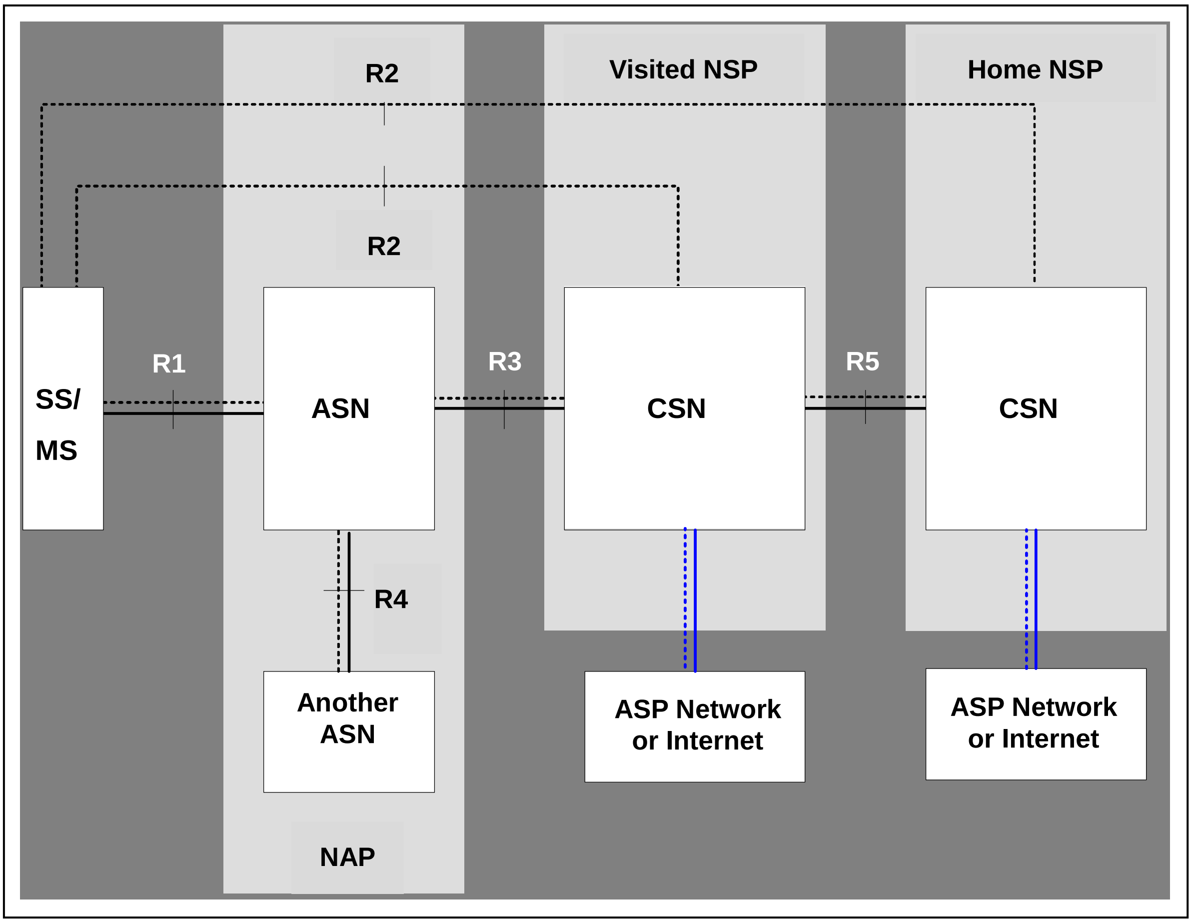


Figure 2-2 WiMAX Network Reference Model

The ASN defines a logical boundary and represents a convenient way to describe aggregation of functional entities and corresponding message flows associated with the access services. The ASN represents a boundary for functional interoperability with WiMAX clients, connectivity service functions, and aggregation of functions embodied by different vendors. Mapping of functional entities to logical entities within ASNs as depicted in the NRM may be performed in different ways. The Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the subscriber stations. A CSN may comprise network elements such as routers, AAA proxy/servers, user databases and Interworking gateway devices. Figure 2-3 provides a more basic view of the many entities within the functional groupings of ASN and CSN.

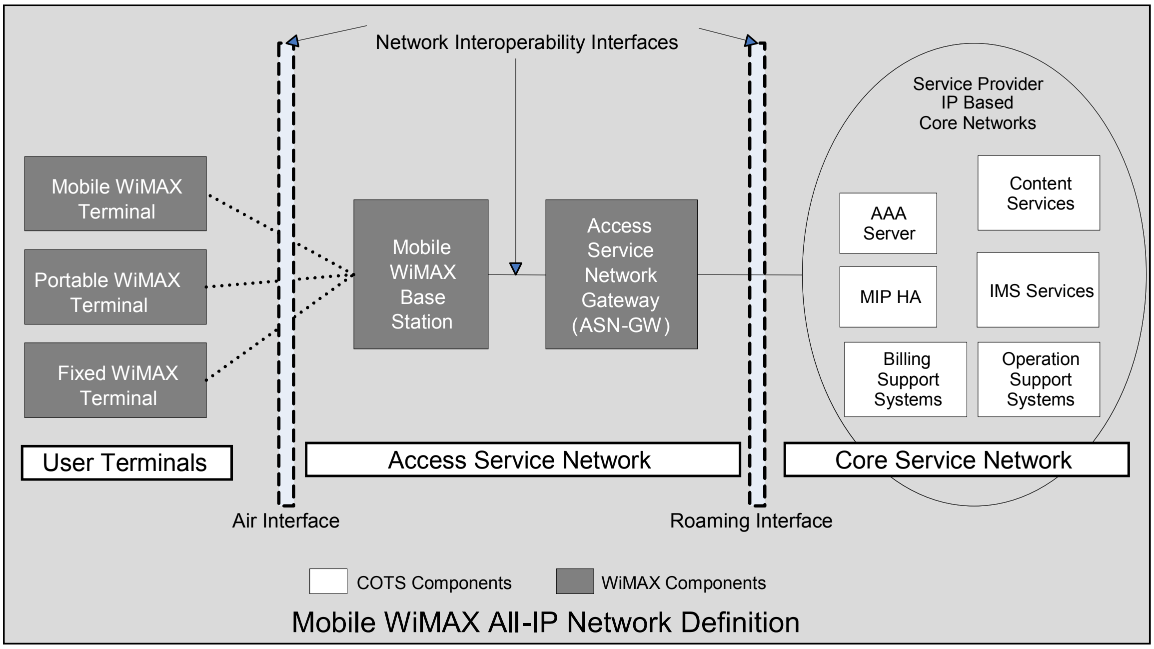


Figure 2-3 ASN and CSN Entities

Some general tenets have guided the development of the Network Architecture and include the following: a) Logical separation of IP addressing, routing and connectivity management procedures and protocols, to enable use of the access architecture primitives in standalone and inter-working deployment scenarios, b) Support for sharing of ASN(s) of a NAP among multiple NSPs, c) Support of a single NSP providing service over multiple ASN(s) – managed by one or more NAPs, d) Support for the discovery and selection of accessible NSPs by an MS, e) Support of NAPs that employ one or more ASN topologies, f) Support of access to incumbent operator services through internetworking functions as needed, g) Specification of open and well-defined reference points between various groups of network functional entities (within an ASN, between ASNs, between an ASN and a CSN, and between CSNs), and in particular between an MS, ASN and CSN to enable multi-vendor interoperability, h) Support for evolution paths between the various usage models subject to reasonable technical assumptions and constraints, i) Enabling different vendor implementations based on different combinations of functional entities on physical network entities, as long as these implementations comply with the normative protocols and procedures across applicable reference points, as defined in the network specifications and j) Support for the most basic scenario of a single operator deploying an ASN together with a limited set of CSN functions, so that the operator can offer basic Internet access service without consideration for roaming or interworking.

The Mobile WiMAX architecture also supports IP services, in a standard mobile IP compliant network. The flexibility and interoperability supported by this network architecture provides operators with the opportunity for a multi-vendor implementation of a network even with a mixed deployment of distributed and centralized ASN's in the network. The Mobile WiMAX network architecture has the following major features:

Security

The end-to-end Network Architecture is based upon a security framework that is independent of the ASN topology and applies consistently across both new and internetworking deployment models and various usage scenarios. In particular, it supports: a) Strong mutual device authentication between an MS and the network, based on the IEEE802.16 security framework, b) All commonly deployed authentication mechanisms and authentication in home and visited operator network scenarios based on a consistent and extensible authentication framework, c) Data integrity, replay protection, confidentiality and non-repudiation using applicable key lengths, d) Use of MS initiated/terminated security mechanisms such as Virtual Private Networks (VPNs), and e) Standard secure IP address management mechanisms between the MS and its home or visited NSP.

Mobility and Handovers

The end-to-end Network Architecture has extensive capabilities to support mobility and handovers. It a) supports IPv4 or IPv6 based mobility management. Within this framework, and as applicable, the architecture accommodates MS equipment with multiple IP addresses and simultaneous IPv4 and IPv6 connections, b) supports roaming between NSPs, c) utilizes mechanisms to support seamless handovers at up to vehicular speeds— satisfying well-defined bounds of service disruption. Some of the additional capabilities for mobility include the support of: i) dynamic and static home address configurations, ii) dynamic assignment of the Home Agent in the service provider network as a form of route optimization, as well as in the home IP network as a form of load balancing and iii) dynamic assignment of the Home Agent based on policies.

Scalability, Extensibility, Coverage and Operator Selection

The end-to-end Network Architecture has extensive support for scalable, extensible operation and flexibility in operator selection. In particular, it a) enables a user to manually or automatically select from available NAPs and NSPs, b) enables ASN and CSN system designs that easily scale upward and downward – in terms of coverage, range or capacity, c) accommodates a variety of ASN topologies - including hub-and-spoke, hierarchical, and/or multi-hop interconnects, d) accommodates a variety of backhaul links, both wireline and wireless with different latency and throughput characteristics, e) supports incremental infrastructure deployment, f) supports phased introduction of IP services that in turn scale with increasing number of active users and concurrent IP services per user, g) supports the integration of base stations of varying coverage and capacity - for example, pico, micro, and macro base stations and e) supports flexible decomposition and integration of ASN functions in ASN deployments in order to enable use of load balancing schemes for efficient use of radio spectrum and network resources.

Additional features pertaining to manageability and performance of the Network Architecture include: a) Support for a variety of online and offline client provisioning, enrollment, and management schemes based on open, broadly deployable, IP-based, industry standards, b) Accommodation of Over-The-Air (OTA) services for MS terminal provisioning and software upgrades, and c) Accommodation of the use of header compression/suppression and/or payload compression for efficient use of the radio resources.

Multi-Vendor Interoperability

Another key aspect of the Network Architecture is the support of interoperability between equipment from different manufacturers within an ASN and across ASNs. This includes interoperability between: a) BS and backhaul equipment within an ASN, and b) Various ASN elements (possibly from different vendors) and CSN, with minimal or no degradation in functionality or capability of the ASN.

Quality of Service

The Network Architecture has provisions for support of the QoS mechanisms defined in IEEE Std 802.16. In particular, it enables flexible support of simultaneous use of a diverse set of IP services. The architecture supports: a) differentiated levels of QoS, coarse-grained (per user/terminal) and/or fine-grained (per service flow), b) admission control, c) bandwidth management and d) implementation of policies as defined by various operators for QoS based on their SLAs (including policy enforcement per user and user group as well as factors such as location, time of day, etc.). Extensive use is made of standard IETF mechanisms for managing policy definition and policy enforcement between operators.

Interworking with Other Networks

The Network Architecture supports loosely coupled interworking with existing wireless or wireline core networks such as GSM/GPRS, UMTS, HSDPA, CDMA2000, RLAN, DSL, and cable modem operator networks on the basis of the IP/IETF suite of protocols.

2.3 Physical Layer Description

2.3.1 OFDMA Basics

OFDM is a multiplexing technique that subdivides the bandwidth into multiple frequency sub-carriers as shown in Figure 2-4. In an OFDM system, the input data stream is divided into several parallel sub-streams of reduced data rate (thus increased symbol duration) and each sub-stream is modulated and transmitted on a separate orthogonal sub-carrier. The increased symbol duration improves the robustness of OFDM to delay spread. Furthermore, the introduction of the cyclic prefix (CP) can completely eliminate Inter-Symbol Interference (ISI) as long as the CP duration is longer than the channel delay spread. The CP is typically a repetition of the last samples of data portion of the block that is appended to the beginning of the data payload as shown in Figure 2-5. The CP prevents inter-block interference and makes the channel appear circular and permits low-complexity frequency domain equalization. A perceived drawback of CP is that it introduces overhead, which effectively reduces bandwidth efficiency. While the CP does reduce bandwidth efficiency somewhat, the impact of the CP is similar to the "roll-off factor" in raised-cosine filtered single-carrier systems. Since OFDM signal power spectrum has a very sharp fall of at the edge of channel, a larger fraction of the allocated channel bandwidth can be utilized for data transmission, which helps to moderate the loss in efficiency due to the cyclic prefix.

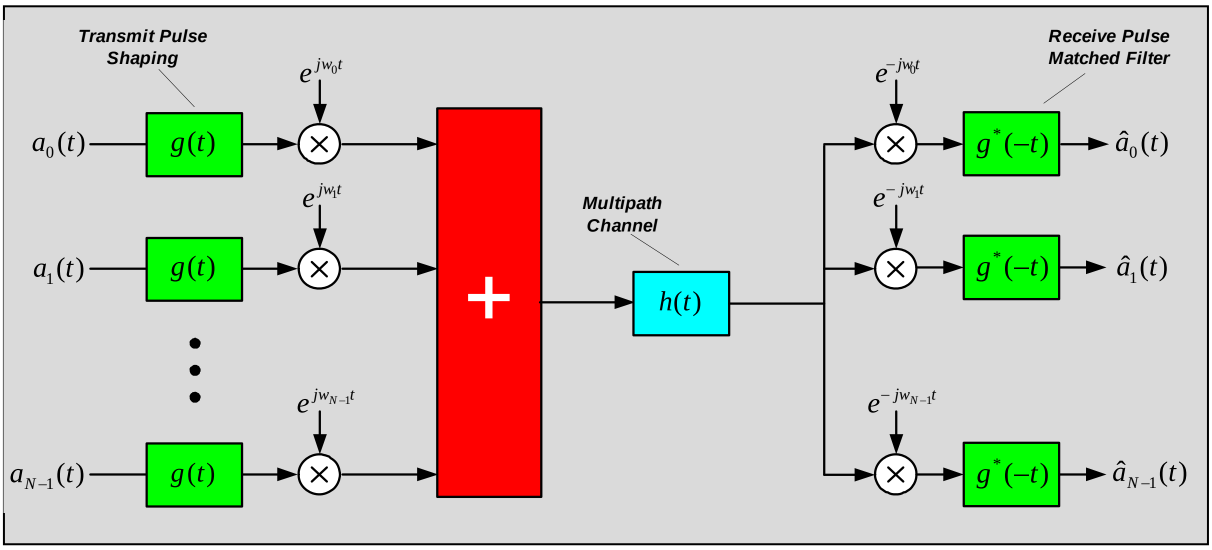


Figure 2-4 Basic Architecture of an OFDM System

OFDM exploits the frequency diversity of the multipath channel by coding and interleaving the information across the sub-carriers prior to transmissions. OFDM modulation can be realized with efficient Inverse Fast Fourier Transform (IFFT), which enables a large number of sub-carriers with low complexity. In an OFDM system, resources are available in the time domain by means of OFDM symbols and in the frequency domain by means of sub-carriers. The time and frequency resources can be organized into subchannels for allocation to individual users. Orthogonal Frequency Division Multiple Access (OFDMA) is a multiple-access/multiplexing scheme that provides multiplexing operation of data streams corresponding to multiple users onto the downlink subchannels. It also supports multiple access of various users by means of uplink subchannels.

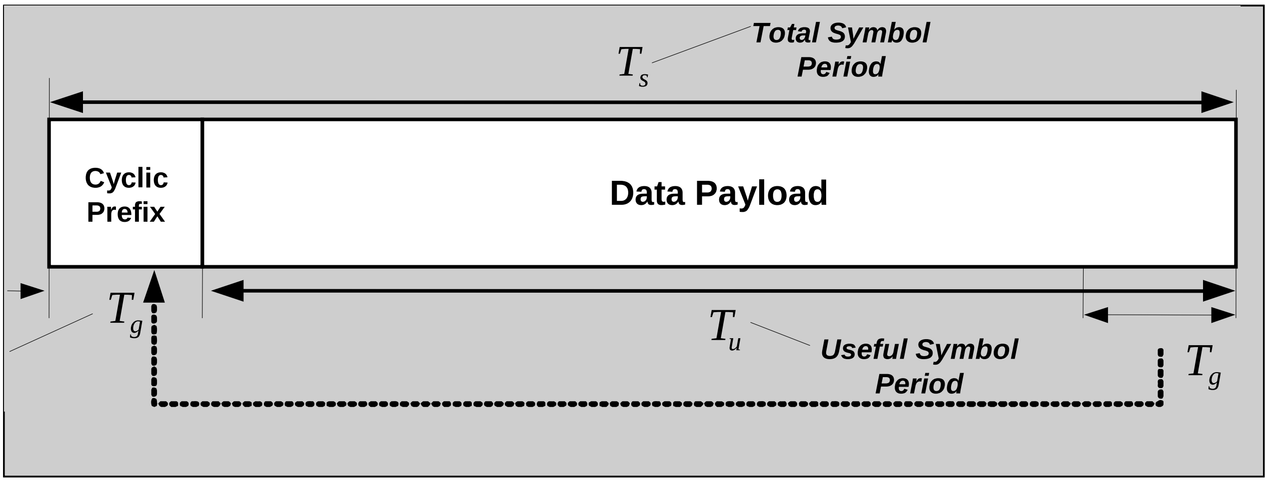


Figure 2-5 Insertion of Cyclic Prefix (CP)

2.3.2 OFDMA Symbol Structure and Subchannelization

The OFDMA symbol structure consists of three types of sub-carriers as shown in Figure 2- 6.

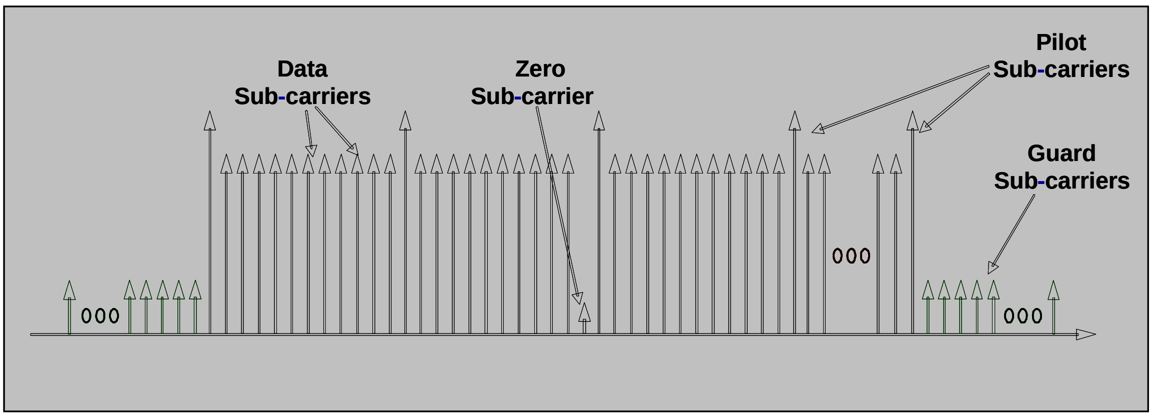


Figure 2-6 OFDMA Sub-Carrier Structure

- Data sub-carriers for data transmission.
- Pilot sub-carriers for estimation and synchronization purposes.
- Null sub-carriers for no transmission; used for guard band and zero Hertz sub-carriers.

Active (data and pilot) sub-carriers are grouped into subsets of sub-carriers called subchannels. The Mobile WiMAX PHY supports subchannelization in both DL and UL. The minimum frequency-time resource unit of subchannelization is one slot, which is equal to 48 data tones (sub-carriers).

There are two types of sub-carrier permutations for subchannelization; diversity and contiguous. The diversity permutation draws sub-carriers pseudo-randomly to form a subchannel. It provides frequency diversity and inter-cell interference averaging. The diversity permutations include DL FUSC, DL PUSC and UL PUSC and additional optional permutations. With DL PUSC, for each pair of OFDM symbols, the available or usable sub-carriers are grouped into clusters containing 14 contiguous sub-carriers per symbol, with pilot and data allocations in each cluster in the even and odd symbols as shown in 2- 7.

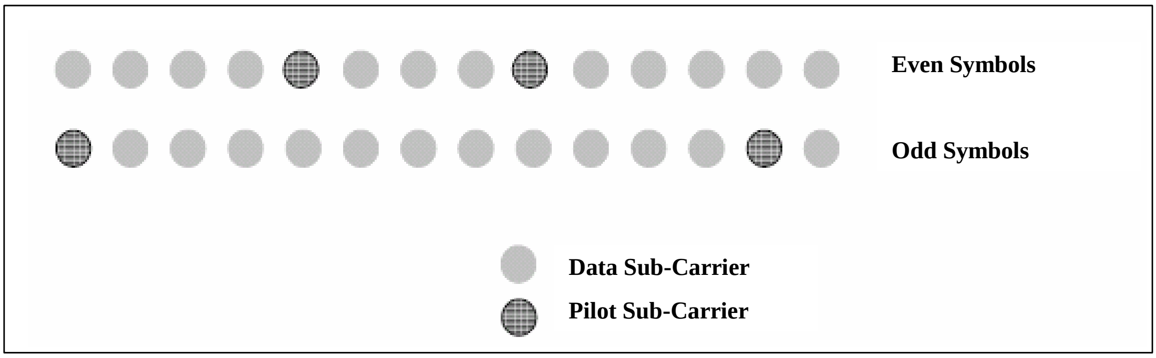


Figure 2-7 DL Frequency Diverse Subchannel

A re-arranging scheme is used to form groups of clusters such that each group is made up of clusters that are distributed throughout the sub-carrier space. A subchannel in a group contains two (2) clusters and is comprised of 48 data sub-carriers and eight (8) pilot sub-carriers. The data subcarriers in each group are further permuted to generate subchannels in the group. Therefore, only the pilot positions in the cluster as shown in 2- 7. The data subcarriers in the cluster are distributed to multiple subchannels.

Analogous to the cluster structure for DL, a tile structure is defined for the UL PUSC whose format is shown in Figure 2-8.

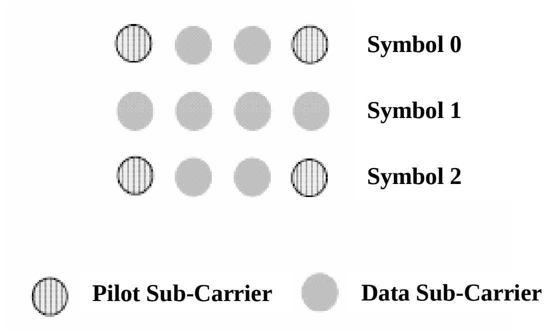


Figure 2-8　Tile Structure for UL PUSC

The available sub-carrier space is split into tiles and six (6) tiles, chosen from across the entire spectrum by means of a re-arranging/permutation scheme, are grouped together to form a slot. The slot is comprised of 48 data sub-carriers and 24 pilot sub-carriers in 3 OFDM symbols.

The contiguous permutation groups a block of contiguous sub-carriers to form a subchannel. The contiguous permutations include DL AMC (Adaptive Modulation and Coding) and UL AMC, and have the same structure. A bin consists of 9 contiguous sub-carriers in a symbol, with 8 assigned for data and one assigned for a pilot.　A slot in AMC is defined as a collection of bins of the type (N x M = 6), where N is the number of contiguous bins and M is the number of contiguous symbols. Thus the allowed combinations are (6 bins, 1 symbol), (3 bins, 2 symbols), (2 bins, 3 symbols) or (1 bin, 6 symbols). AMC permutation enables multi-user diversity by choosing the subchannel with the best frequency response.

In general, diversity sub-carrier permutations perform well in mobile applications while contiguous sub-carrier permutations are well suited for fixed, nomadic, or low mobility environments. These options enable the system designer to trade-off mobility for throughput.

Following figure demonstrates the physical and Logical subchannel allocation in a OFDMA frame.

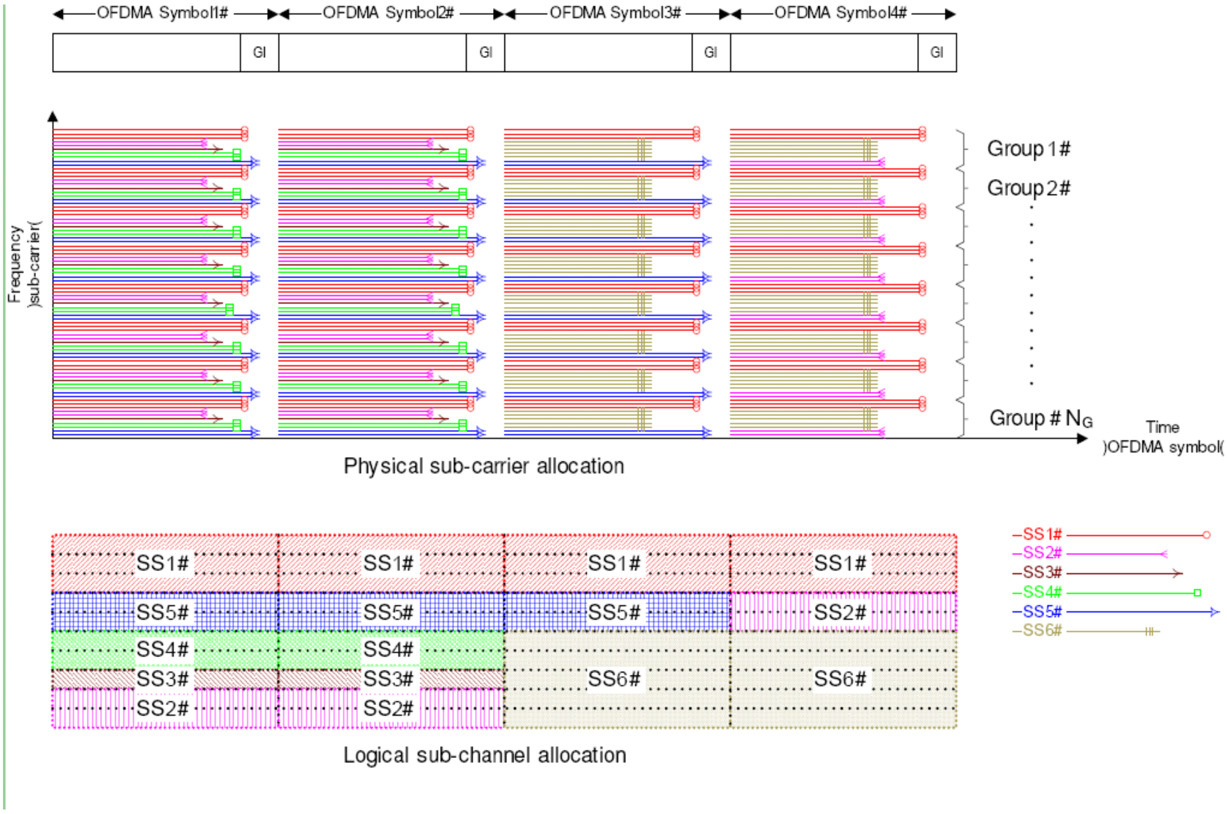


Figure 2-9 Physical and Logical Subchannel allocation

2.3.3 Scalable OFDMA

Mobile WiMAX mode is based upon the concept of Scalable OFDMA. The scalability is supported by adjusting the FFT size while fixing the sub-carrier frequency spacing at 10.94 kHz. Since the resource unit sub-carrier bandwidth and symbol duration is fixed, the impact to higher layers is minimal when scaling the bandwidth. The Mobile WiMAX parameters are listed in Table 2-2.

Table 2-1 OFDMA Scalability Parameters

Parameters	Values	
System Channel Bandwidth (MHz)	5	10
Sampling Frequency (F_p in MHz)	5.6	11.2
FFT Size (N_{FFT})	512	1024
Number of Subchannels	8	16
Sub-Carrier Frequency Spacing	10.94 kHz	

Useful Symbol Time ($T_b = 1/f$)	91.4 μs
Guard Time ($T_g = T_b/8$)	11.4 μs
OFDMA Symbol Duration ($T_s = T_b + T_g$)	102.9 μs
Number of OFDMA Symbols (5 ms Frame)	48 (including ~1.6 symbols for TTG/RTG)

2.3.4 TDD Frame Structure

The Mobile WiMAX PHY makes use of Time Division Duplexing. To counter interference issues, TDD does require system-wide synchronization; nevertheless, TDD has numerous advantages:

- TDD enables adjustment of the downlink/uplink ratio to efficiently support asymmetric downlink/uplink traffic, while with FDD, downlink and uplink always have fixed and, generally, equal DL and UL bandwidths. As shown in Table 2-3, recommended number of UL/DL OFDM symbols can flexibly realize a range of asymmetric downlink/uplink traffic ratio.

Table 2-2 Number of OFDM Symbols in DL and UL

Description	Base Station Values
Number of OFDM Symbols in DL and UL for 5 and 10 MHz BW	(35: 12), (34: 13), (33: 14), (32: 15), (31: 16), (30: 17), (29: 18), (28: 19), (27: 20), (26: 21)

- TDD assures channel reciprocity for better support of link adaptation, MIMO and other closed loop advanced antenna technologies. Also, TDD is the preferred mode of operation with respect to the beamforming systems using phased array antennas.
- Unlike FDD, which requires a pair of channels, TDD only requires a single channel for both downlink and uplink, providing greater flexibility for adaptation to varied global spectrum allocations.
- Transceiver designs for TDD implementations are less complex.

Figure 2-10 illustrates the OFDM frame structure for a TDD implementation. Each frame is divided into DL and UL sub-frames, separated by Transmit/Receive and Receive/Transmit Transition Gaps (TTG and RTG, respectively) to prevent DL and UL transmission collisions. In a frame, the following control information is used:

- Preamble: The preamble, used for synchronization, is the first OFDM symbol of the frame.
- Frame Control Header (FCH): The FCH follows the preamble. It provides the frame configuration information, such as MAP message length, coding scheme, and usable subchannels.
- DL-MAP and UL-MAP: The DL-MAP and UL-MAP provide subchannel allocation and other control information for the DL and UL sub-frames respectively.
- UL Ranging: The UL ranging subchannel is allocated for MSs to perform closed-loop time, frequency, and power adjustment as well as bandwidth requests. Four types of ranging are defined. The different types of ranging are identified by a code and a 2D region in the UL subframe.
    - Initial Ranging- when MS enters (or re-enters) the network,
    - Periodic Ranging once the connection is set up between the MS and the BS,
    - Hand Over Ranging (in case of Hard HO in drop situations) and
    - Bandwidth Request.
- UL CQICH: The UL CQICH channel is allocated for the MS to feedback channel-state information.
- UL ACK: The UL ACK is allocated for the MS to feedback DL HARQ acknowledgement.

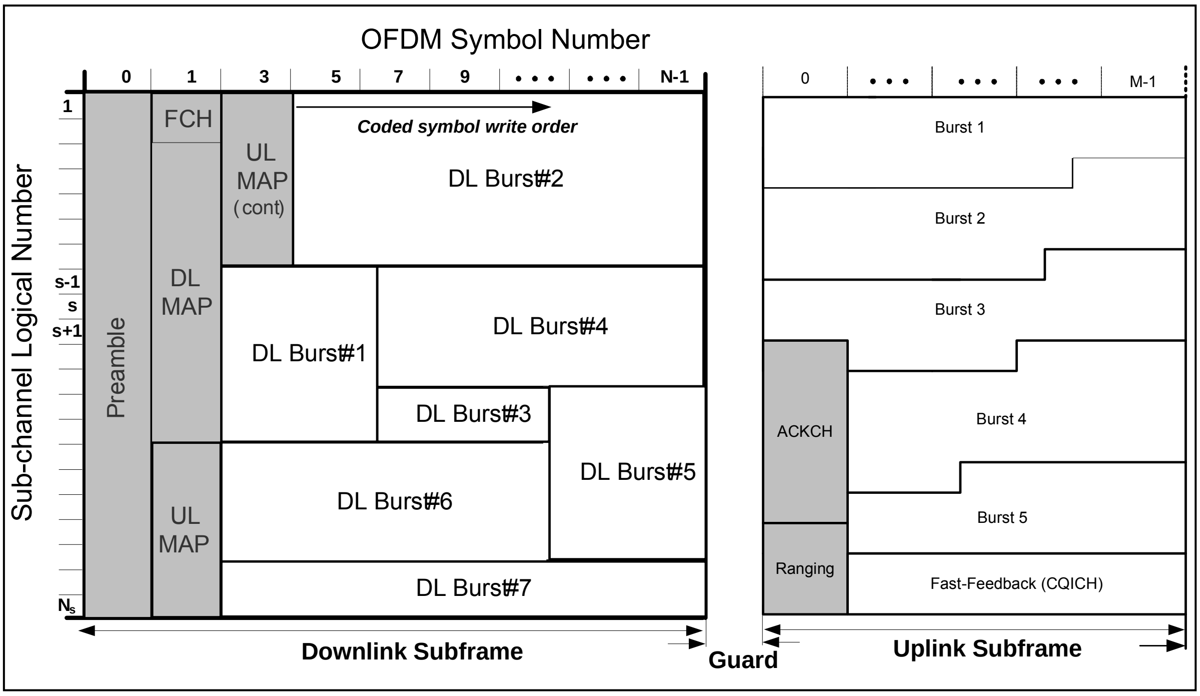


Figure 2-10 Mobile WiMAX Frame Structure

2.3.5 Other Advanced PHY Layer Features

Adaptive modulation and coding, HARQ, CQICH, and multiple antenna technologies provide enhanced coverage and capacity in mobile applications.

Support for QPSK, 16QAM and 64QAM are mandatory in the DL. In the UL, 64QAM is optional. Both Convolutional Code (CC) and Convolutional Turbo Code (CTC), with variable code rate and repetition coding, are supported. Table 2-4 summarizes the coding and modulation schemes supported in Mobile WiMAX.

Table 2-3 Supported Coding and Modulation Schemes

		DL	UL
Modulation		QPSK, 16QAM, 64QAM	QPSK,16QAM, (64QAM optional)
Rate	CC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, (5/6 optional)
	CTC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, (5/6 optional)
	Repetition	x2, x4, x6	x2, x4, x6

The combinations of various modulations and code rates provide a fine resolution of data rates, as shown in Table 2-4. Table 2-6 assumes PUSC subchannels with frame duration of 5 milliseconds. Each frame has 48 OFDM symbols, with 44 OFDM symbols available for data transmission. The highlighted values indicate data rates for optional 64QAM in the UL.

Table 2-4 Mobile WiMAX PHY Numerology

Parameter	Downlink	Uplink	Downlink	Uplink
System Bandwidth	5 MHz		10 MHz	
FFT Size	512		1024	
Null Sub-Carriers	92	104	184	184
Pilot Sub-Carriers	60	136	120	280
Data Sub-Carriers	360	272	720	560
Subchannels	15	17	30	35
Symbol Period, T_S	102.9 μs			

Frame Duration	5 ms
OFDM Symbols/Frame	48 (including ~1.6 symbols for TTG/RTG)
Data OFDM Symbols	44

Table 2-5 Mobile WiMAX PHY Data Rates with PUSC Subchannel[3]

Modulation	Code Rate	5 MHz Channel		10 MHz Channel	
		Downlink Rate, Mbit/s	Uplink Rate, Mbit/s	Downlink Rate, Mbit/s	Uplink Rate, Mbit/s
QPSK	1/2 CTC, 6x	0.53	0.38	1.06	0.78
	1/2 CTC, 4x	0.79	0.57	1.58	1.18
	1/2 CTC, 2x	1.58	1.14	3.17	2.35
	1/2 CTC, 1x	3.17	2.28	6.34	4.70
	3/4 CTC	4.75	3.43	9.50	7.06
16QAM	1/2 CTC	6.34	4.57	12.07	9.41
	3/4 CTC	9.50	6.85	19.01	14.11
64QAM	1/2 CTC	9.50	6.85	19.01	14.11
	2/3 CTC	12.67	9.14	26.34	18.82
	3/4 CTC	14.26	10.28	28.51	21.17
	5/6 CTC	15.84	11.42	31.68	23.52

The base station scheduler determines the appropriate data rate (or burst profile) for each burst allocation based on the buffer size, channel propagation conditions at the receiver, etc. A Channel Quality Indicator (CQI) channel is utilized to provide channel-state information from the user terminals to the base station scheduler. Relevant channel-state information can be fed back by the CQICH including: Physical CINR, Effective CINR, MIMO mode selection and frequency selective subchannel selection. Because the implementation is TDD, link adaptation can also take advantage of channel reciprocity to provide a more accurate measure of the channel condition (such as sounding).

---

3 PHY Data Rate=(Data sub-carriers/Symbol period)x(information bits per symbol).

HARQ is enabled using N channel “Stop and Wait” protocol, which provides fast response to packet errors and improves cell edge coverage. Chase Combining and, optionally, Incremental Redundancy are supported to further improve the reliability of the retransmission. A dedicated ACK channel is provided in the uplink for HARQ ACK/NACK signaling. Multi-channel HARQ operation is supported. Multi-channel stop-and-wait ARQ with a small number of channels is an efficient, simple protocol that minimizes the memory required for HARQ and stalling. Mobile WiMAX provides signaling to allow fully asynchronous operation. The asynchronous operation allows variable delay between retransmissions, which gives more flexibility to the scheduler at the cost of additional overhead for each retransmission allocation. HARQ combined together with CQICH and adaptive modulation and coding provides robust link adaptation in mobile environments at vehicular speeds in excess of 120 km/hr.

Multiple antenna technologies typically involve complex vector or matrix operations on signals due to the presence of multiple antenna links between the transmitter and receiver. OFDMA allows multiple antenna operations to be performed on a per-subcarrier basis, where the vector-channels are flat fading. This fact makes the multiple antenna signal processing manageable at both transmitter and receiver side since complex transmitter architectures and receiver equalizers are not required to compensate for frequency selective fading. Thus, OFDMA is very well-suited to support multiple antenna technologies. Mobile WiMAX supports a full range of multiple antenna technologies to enhance system performance. The supported multiple antenna technologies include:

- Beamforming (BF) for both the uplink and the downlink: With BF, the system uses multiple-antennas to both receive and transmit signals to improve the coverage and capacity of the system and reduce the outage probability. The BS is usually equipped with two or more antennas, with a typical number being four antennas, and determines so-called antenna weights for both uplink reception and downlink transmission, while the MS is usually equipped with one or two antennas for downlink reception and one antenna for uplink transmission. Note that different BF techniques can be applied in Mobile WiMAX since there is no limitation imposed either to the distance among the antenna elements of the BS or the algorithm employed at the BS transceiver; the possibility of beamforming the pilot subcarriers during downlink transmission (feature of dedicated pilots in the mobile WiMAX system profiles) makes the application of specific BF algorithms transparent to the MS receiver.
- Space-Time Coding (STC) for the downlink: Two-antenna transmit diversity is enabled in Mobile WiMAX through the use of a space-time block coding code widely known as the

Alamouti code. STC is a powerful technique for implementing open-loop transmit diversity, while its performance is further increased in Mobile WiMAX since a second antenna is mandated to be present at the MS receiver. Further, STC offers favorable performance in all propagation environments, i.e., it is not constrained by the MIMO channel quality usually represented by the spread of the MIMO channel eigenvalues. As in the BF case where one spatial stream is transmitted over one OFDMA symbol per subcarrier, STC cannot lead to link throughput increase because it transmits two spatial streams over two OFDMA symbols per subcarrier.

- Spatial Multiplexing (SM) for the downlink: Spatial multiplexing is supported to apply higher peak rates and increased throughput whenever this is possible. With spatial multiplexing, two data streams are transmitted over one OFDMA symbol per subcarrier. Since the MS receiver is also equipped with two receive antennas, it can separate the two data streams to achieve higher throughput compared to single antenna, BF, and STC systems. In Mobile WiMAX, with 2x2 MIMO SM increases the peak data rate two-fold by transmitting two data streams.
- Collaborative Spatial Multiplexing (CSM), also referred to as virtual spatial multiplexing, for the uplink: In the uplink, each MS is equipped with a single transmit antenna. To increase the uplink performance, two users can transmit collaboratively in the same frequency and time allocation as if two streams were spatially multiplexed from two antennas of the same user. The advantage of the uplink CSM compared to the downlink SM is related to the fact that the transmitted spatial streams are uncorrelated since they originate from spatially displaced MS's. By additionally considering that the channel correlation factor at the BS can be kept at lower values than that at the MS receiver (space limitations at the MS usually apply leading to smaller inter-antenna distances and, thus, higher correlation values, especially if cross-polarized antennas are not employed), an improved performance of the spatial stream demultiplexing is expected in the uplink compared to the downlink.

Regarding the MIMO operation in the downlink (use of the STC and SM modes), Mobile WiMAX supports adaptive switching between STC and SM to maximize the benefit of MIMO depending on the channel conditions. For instance, SM improves peak throughput. However, when channel conditions are poor, e.g., when the signal-to-interference ratio is low or the channel correlation factor is relatively high, the packet error rate (PER) can be high and thus the coverage area where the target PER is met may be limited. STC on the other hand provides large coverage regardless of the channel condition but does not improve the peak data rate. Mobile WiMAX supports adaptive switching between multiple MIMO modes to maximize spectral efficiency without compromising on the coverage area.

2.4 MAC Layer Description

Mobile WiMAX supports the delivery of broadband services, including voice, data, and video. The MAC layer can support bursty data traffic with high peak rate demand while simultaneously supporting streaming video and latency-sensitive voice traffic over the same channel. The resource allocated to one terminal by the MAC scheduler can vary from a single time slot to the entire frame, thus providing a very large dynamic range of throughput to a specific user terminal at any given time. Furthermore, since the resource allocation information is conveyed in the MAP messages at the beginning of each frame, the scheduler can effectively change the resource allocation on a frame-by-frame basis to adapt to the bursty nature of the traffic.

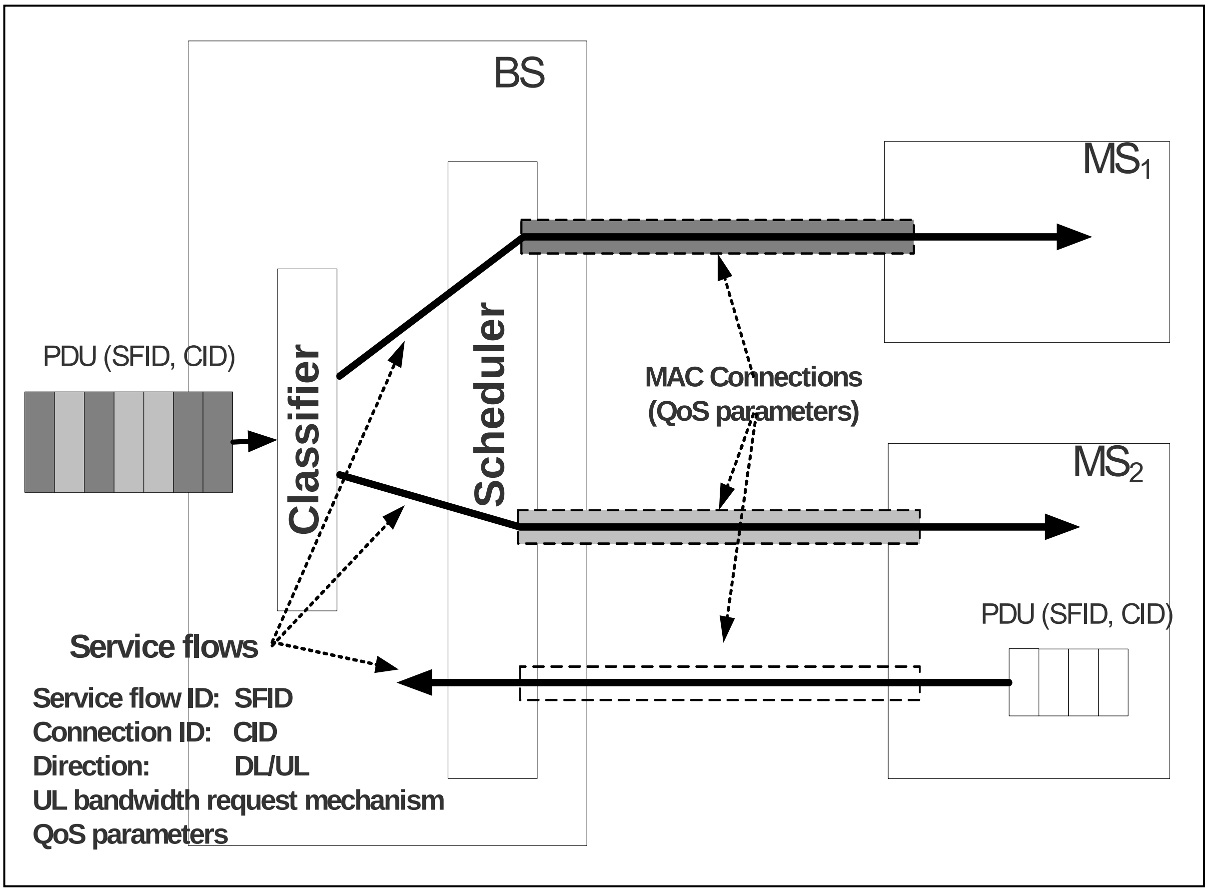


Figure 2-11 Mobile WiMAX QoS Support

2.4.1 Quality of Service (QoS) Support

With fast air link, symmetric downlink/uplink capacity, fine resource granularity and a flexible resource allocation mechanism, Mobile WiMAX can meet QoS requirements for a wide range of data services and applications.

In the Mobile WiMAX MAC layer, QoS is provided via service flows as illustrated in Figure 2-11. A service flow is a unidirectional flow of packets provided with a particular set of QoS parameters. Before providing a certain type of data service, the Base Station and Mobile Station first establish a unidirectional logical link between the peer MACs, called a connection. The outbound MAC then associates packets traversing the MAC interface into a service flow to be delivered over the connection. The QoS parameters associated with the service flow define the transmission ordering and scheduling on the air interface. The connection-oriented MAC can therefore provide accurate QoS control over the air interface. Since the air interface is usually the bottleneck, the connection-oriented MAC can effectively enable end-to-end QoS control. The service flow parameters can be dynamically managed through MAC messages to accommodate the dynamic service demand. The service flow based QoS mechanism applies to both DL and UL to provide improved QoS in both directions. Mobile WiMAX supports a wide range of data services and applications with varied QoS requirements. These are summarized in Table 2-7.

Table 2-6 Mobile WiMAX Applications and Quality of Service

QoS Category	Applications	QoS Specifications
UGS: Unsolicited Grant Service	VoIP	Maximum Sustained Rate Maximum Latency Tolerance Jitter Tolerance
rtPS: Real-Time Packet Service	Streaming Audio or Video	Minimum Reserved Rate Maximum Sustained Rate Maximum Latency Tolerance Traffic Priority
ErtPS: Extended Real-Time Packet Service	Voice with Activity Detection (VoIP)	Minimum Reserved Rate Maximum Sustained Rate Maximum Latency Tolerance Jitter Tolerance Traffic Priority
nrtPS: Non-Real-Time Packet Service	File Transfer Protocol (FTP)	Minimum Reserved Rate Maximum Sustained Rate Traffic Priority
BE: Best-Effort Service	Data Transfer, Web Browsing, etc.	Maximum Sustained Rate Traffic Priority

2.4.2 MAC Scheduling Service

The Mobile WiMAX MAC scheduling service is designed to efficiently deliver time-sensitive broadband data services including voice, data, and video over time-varying broadband wireless channel. The MAC scheduling service has the following properties that enable this real-time broadband data service:

- Fast Data Scheduler: The MAC scheduler must efficiently allocate available resources in response to bursty data traffic and time-varying channel conditions. The scheduler is located at each base station to enable rapid response to traffic requirements and channel conditions. The data packets are associated to service flows with well defined QoS parameters in the MAC layer so that the scheduler can correctly determine the packet transmission ordering over the air interface. The CQICH channel provides fast channel information feedback to enable the scheduler to choose the appropriate coding and modulation for each allocation. The adaptive modulation/coding combined with HARQ provide robust transmission over the time-varying channel.
- Scheduling for both DL and UL: The scheduling service is provided for both DL and UL traffic. In order for the MAC scheduler to make an efficient resource allocation and provide the desired QoS in the UL, the UL must feed back accurate and timely information as to the traffic conditions and QoS requirements. Multiple uplink bandwidth request mechanisms (such as bandwidth request through ranging channel, piggyback request, and polling) are specified. The UL service flow defines the feedback mechanism for each uplink connection to ensure predictable UL scheduler behavior. Furthermore, with orthogonal UL subchannels, there is no intra-cell interference. UL scheduling can allocate resource more efficiently and better enforce QoS.
- Dynamic Resource Allocation: The MAC supports frequency-time resource allocation in both DL and UL on a per-frame basis. The resource allocation is delivered in MAP messages at the beginning of each frame. Therefore, the resource allocation can be changed on frame-by-frame in response to traffic and channel conditions. Additionally, the amount of resource in each allocation can range from one slot to the entire frame. The fast and fine granular resource allocation allows superior QoS for data traffic.
- UL and DL QoS: The MAC scheduler handles data transport on a connection-by-connection basis. Each connection is associated with a single data service with a set of QoS parameters that quantify the aspects of its behavior. With the ability to dynamically allocate resources in both DL and UL, the scheduler can provide QoS for both DL and UL traffic.
- Frequency Selective Scheduling: The scheduler can operate on different types of subchannels. For frequency-diverse subchannels such as PUSC permutation, where

sub-carriers in the subchannels are pseudo-randomly distributed across the bandwidth, subchannels are of similar quality. Frequency-diversity scheduling can support a QoS with fine granularity and flexible time-frequency resource scheduling. With contiguous permutation such as AMC permutation, the subchannels may experience different attenuation. The frequency-selective scheduling can allocate mobile users to their corresponding strongest subchannel. The frequency-selective scheduling can enhance system capacity with a moderate increase in CQI overhead in the UL.

- Admission Control: Admission Control admits service flows based on resource availability. That is, a service flow is either admitted or rejected during service flow creation transaction. Admission Control is implemented on the various network elements: Server, BS and MS.
- Policing: A service flow is prohibited from injecting data traffic that exceeds its Maximum Sustained Traffic Rate. Policing enforces this restriction.

2.4.3 Power control and boosting

Mobile WiMAX defines two modes of power control.

- Closed Loop Power Control, in which the Base Stations regularly adjusts the transmission level of each terminals based on the measurements done on received data from this terminal.
- Open Loop Power Control, in which the terminal adjusts its transmission level based on the signal strength measured on the received preamble from the serving Base Station. The serving Base Station is furthermore allowed to correct this transmission level, based on received signal strength. This correction is normally performed at very low frequency rate, enough to meet the requirement of the base station.

Furthermore, power boosting on data is a mechanism that can be used by the Base Station in order to extend its coverage. It is particularly convenient in an OFDMA scheme, where some subchannels can be boosted and some others attenuated, on the same OFDM symbol(s). The base station is hence able to use such boosting for further increasing the granularity of its link adaptation and the network load balancing.

2.4.4 Mobility Management

Battery life and handover are two critical issues for mobile applications. Mobile WiMAX supports Sleep Mode and Idle Mode to enable power-efficient MS operation. Mobile WiMAX also supports seamless handover to enable the MS to switch from one base station to another at vehicular speeds without interrupting the connection.

2.4.5 Power Management

Mobile WiMAX supports two modes for power efficient operation – Sleep Mode and Idle Mode. Sleep Mode is a state in which the MS conducts pre-negotiated periods of absence from the Serving Base Station air interface. These periods are characterized by the unavailability of the MS, as observed from the Serving Base Station, to DL or UL traffic. Sleep Mode is intended to minimize MS power usage and minimize the usage of the Serving Base Station air interface resources. The Sleep Mode also provides flexibility for the MS to scan other base stations to collect information to assist handover during the Sleep Mode.

Idle Mode provides a mechanism for the MS to become periodically available for DL broadcast traffic messaging without registration at a specific base station as the MS traverses an air link environment populated by multiple base stations. Idle Mode benefits the MS by removing the requirement for handover and other normal operations and benefits the network and base station by eliminating air interface and network handover traffic from essentially inactive MSs while still providing a simple and timely method (paging) for alerting the MS about pending DL traffic.

2.4.6 Handover

There are three handover methods supported within the IEEE 802.16 standard – Hard Handover, Fast Base Station Switching, and Macro Diversity Handover. Of these, the HHO is mandatory.

WiMAX Forum Mobile System Profile specifies a set of techniques for optimizing handover within the framework of the IEEE 802.16 standard. These improvements have been developed with the goal of keeping Layer 2 handover delays to less than 50 milliseconds.

When FBSS is supported, the MS and BS maintain a list of BSs that are involved in FBSS with the MS. This set is called an Active Set. In FBSS, the MS continuously monitors the base stations in the Active Set. Among the BSs in the Active Set, an Anchor BS is defined. When operating in FBSS, the MS communicates only with the Anchor BS for uplink and downlink messages, including management and traffic connections. Transition from one Anchor BS to another (i.e. BS switching) is performed without invocation of explicit HO signaling messages. Anchor update procedures are enabled by communicating signal strength of the serving BS via the CQICH. A FBSS handover begins with a decision by an MS to receive or transmit data from the Anchor BS that may change within the active set. The MS scans the neighbor BSs and selects those that are suitable to be included in the active set. The MS reports the selected BSs and the active set update procedure is performed by the BS and MS. The MS continuously monitors the signal strength of the BSs that are in the active set and selects one BS from the set to be the Anchor BS. The MS reports the selected Anchor BS on CQICH or MS initiated HO request message. An important requirement of FBSS is that the data is simultaneously transmitted to all members of an active set of BSs that are able to serve the MS.

2.4.7 Security

Mobile WiMAX supports mutual device/user authentication, flexible key management protocol, strong traffic encryption, control and management plane message protection, and security protocol optimizations for fast handovers.

The usage aspects of the security features are:

- Key Management Protocol: Privacy and Key Management Protocol Version 2 is the basis of Mobile WiMAX security as defined in the IEEE 802.16 standard. This protocol manages the MAC security using PKM-REQ/RSP messages. PKM EAP authentication, Traffic Encryption Control, Handover Key Exchange, and Multicast/Broadcast security messages all are based on this protocol.
- Device/User Authentication: Mobile WiMAX supports Device and User Authentication using the IETF EAP protocol, providing support for credentials that are based on a SIM, USIM, Digital Certificate, or UserName/Password. Corresponding EAP-SIM, EAP-AKA, EAP-TLS, or EAP-MSCHAPv2 authentication methods are supported through the EAP protocol. Key deriving methods are the only EAP methods supported.
- Traffic Encryption: AES-CCM is the cipher used for protecting all the user data over the Mobile WiMAX MAC interface. The keys used for driving the cipher are generated from the EAP authentication. A Traffic Encryption state machine with a periodic key refresh mechanism enables sustained transition of keys to further improve protection.
- Control Message Protection: Control data is protected using AES based CMAC or MD5-based HMAC schemes.
- Fast Handover Support: A 3-way handshake scheme is supported by Mobile WiMAX to optimize the re-authentication mechanisms for supporting fast handovers. This mechanism is also useful to prevent man-in-the-middle-attacks.

Chapter 3 Technical Requirements for WiMAX Systems

For the mobile communications system of a WiMAX system using the 2.5 GHz band, the following prerequisites shall be satisfied.

This chapter is translated into English from the original regulations contained in MIC Ordinances and related Notifications. The original in Japanese shall prevail if any ambiguity exists between the following requirements and the original in Japanese.

3.1 Overview

It is assumed that the types of radio equipment are as follows:

<1> Mobile station

<2> Base station

<3> Relay station (radio station that relays a signal when direct broadband mobile radio communications between a base station and a mobile station is not possible. The technical prerequisites for mobile stations shall apply to the upstream lines, while those for the base station shall apply to the downstream lines.)

3.2 General condition

(1) Communications system

Time Division Duplex (TDD) system

(2) Frequency (ORE, Article 49.28)

2545MHz – 2625MHz

(3) Multiplexing system

a Mobile station (upstream line)

Orthogonal Frequency Division Multiple Access (OFDMA) system

b Base station (downstream line)

Composite system using an Orthogonal Frequency Division Multiplexing (OFDM) system and a Time Division Multiplexing (TDM) system

(4) Modulation system (ORE, Article 49.28)

a Mobile station (upstream line)

QPSK or 16QAM

b Base station (downstream line)

BPSK, QPSK, 16QAM, or 64QAM

(5) Transmission synchronization

a Transmission burst repetition period

5 ms

b The transmission burst lengths for mobile stations and base stations in Table 3-1 (NT No.651,2007)

Table 3-1 Maximum Permissible Transmission Burst Length

Maximum permissible transmission burst length [ms]	
Base station	Mobile station
3.65	1.35
3.55	1.45
3.45	1.55
3.35	1.65
3.25	1.75
3.15	1.85
3.05	1.95
2.95	2.05
2.85	2.15
2.75	2.25

Transmission Burst Lengths Tolerance

Base Station +10μs or less, -90μs or over

Mobile Station +10μs or less, -130μs or over

(6) Authentication, secrecy, and information security

The assignment of numbers specific to mobile station equipment so as to prevent unauthorized use, the application of authentication procedures, the use of secrecy functions for communications information, and other appropriate measures shall be implemented.

(7) Electromagnetic measures

Sufficient consideration shall be given to the mutual electromagnetic interference between mobile stations and automotive electronic devices and medical electronic devices.

(8) Conformance to the radio radiation protection guidelines

Mobile stations, as well as devices using radio waves shall conform to Regulations for Enforcement of the Radio Law, Article 21.3 and Ordinance Regulating Radio Equipment, Article 14.2.

(9) Mobile station identification numbers

It is preferable for the procedures for assigning and subsequently sending identification numbers to mobile stations be established with sufficient consideration given to the selection of networks by users, roaming, the assurance of communications security, the supervision of radio stations, and so on.

(10) Stopping radio emissions in the event of a fault in a mobile station's transmission equipment

The functions below shall be executed at the same time, but independently of each other.

a Function whereby, if a base station detects an error in a mobile station, the base station issues a request to that mobile station to stop transmission.

b Function whereby, if a mobile station itself detects an internal error, the mobile station stops transmission upon the timeout of the error detection timer.

(11) Structure of transmitter

The main part of the transmit device (RF and Modem devices, except Antenna device) shall not be opened easily.

(12) Functions to ensure Model-1 mobile station to be used only indoor coverage

As a general rule, input power source for Model-1 mobile station shall be AC (alternate current). However, for mobile station that require DC power source shall not start its operation before it receive operation starting signal from the parent device. (PC etc.)

(13) Definitions of the Models for Fixed Wireless Access system with antenna gain for mobile station more than 2dBi.

17dBi or less;

- Model-1 mobile station: Radio equipment with more than 2dBi and 10dBi or less antenna gain.
- Model-2 mobile station: Radio equipment with more than 10dBi antenna gain.

In case of the mobile station communicating with the base station whose antenna gain is more than 17dBi.

Model-3 mobile station: Radio equipment with more than 17dBi and 25dBi and less antenna gain.

(14) Restrictions on FWA system deployment (NT No651, 2007)

a Restrictions in base stations

Note1: Following base stations shall be limited for use in depopulated areas, mountain villages, isolated island areas or the areas authorized by Minister of Internal Affairs and Communications.

- The base station that communicates with the mobile station with 2dBi or greater antenna gain or repeater station.
- The base station whose antenna gain is greater than 17dBi.

Note2: The base station whose antenna gain is greater than 17dBi shall only communicate with only a single radio station.

b Restrictions in mobile stations

In case of mobile station that communicates with the base station with the antenna gain of 17dBi or less.

Note1: Mobile station with the antenna gain of greater than 2dBi but not exceeding 10dBi shall be limited for use in a closed environment or equivalent place.

Note2: Mobile station whose antenna gain is more than 2dBi shall be limited for use in depopulated areas, mountain villages, isolated islands or the areas authorized by Minister of Internal Affairs and Communications.

Note3: Mobile station whose antenna gain is greater than 2dBi shall not start its operation under any base station that is installed in places other than those specified in Note 2. At least one of the functions below should be implemented for this purpose.

- Function to enable the mobile station with high gain antenna to determine, by using WiMAX broadcast message, whether the area is authorized or not.

- Function to enable terminal authentication on the network side to deny the network entry by the high gain antenna mobile stations within the unauthorized area, if it is agreed upon between WiMAX operators.

- Other functions which have been agreed upon between the WiMAX operators.

In case of mobile station that communicates with the base station whose antenna gain is greater than 17dBi

Note1: Mobile station shall be limited for use in depopulated areas, mountain villages, isolated islands or the areas authorized by Minister of Internal Affairs and Communications.

Note2: Mobile station shall not start operation under any base station that is installed in places other than those specified in Note1. At least one of the functions below should be implemented for this purpose.

- Function to enable the mobile station to determine, by using WiMAX broadcast message, whether the area is authorized or not.

- Function to enable terminal authentication on the network side to deny the network entry by the mobile stations within the unauthorized area, if it is agreed upon between WiMAX operators.

- Other functions which have been agreed upon between the WiMAX operators.

3.2.1 Transmitter requirement

3.2.1.1 Frequency tolerance (ORE, Article 5,Table 1)

Mobile station	Within 2 x 10^{-6}
Base station	Within 2 x 10^{-6}

3.2.1.2 Occupied band width (ORE, Article 6,Table 2)

5 MHz system	4.9 MHz or less
10 MHz system	9.9 MHz or less

3.2.1.3 Output power (ORE, Article 49.28)

Mobile station	200 mW or less
Base station	20 W or less

3.2.1.4 Output power tolerance (ORE, Article 14)

Mobile station	±50%
Base station	±50%

3.2.1.5 Adjacent channel leakage power (NT No.651,2007)

(1) Mobile station

(i) 5MHz system

Channel space: 5MHz

Occupied bandwidth : 4.8MHz

Permissible adjacent channel leakage power: 2dBm or less

(ii) 10MHz system

Channel space: 10MHz

Occupied bandwidth : 9.5MHz

Permissible adjacent channel leakage power: 0dBm or less

(2) Base station

(i) 5MHz system

Channel space: 5MHz

Occupied bandwidth : 4.8MHz

Permissible adjacent channel leakage power: 7dBm or less

(ii) 10MHz system

Channel space: 10MHz

Occupied bandwidth : 9.5MHz

Permissible adjacent channel leakage power: 3dBm or less

3.2.1.6 Spectrum mask (NT No.651, 2007)

(1) Mobile station

(i) 5MHz system

offset frequency : Δf	Permissible level
7.5MHz or more and less than 8MHz,	less than -20-2.28x(Δf-7.5) dBm/MHz
8MHz or more and less than 17.5MHz,	less than -21-1.68x(Δf-8) dBm/MHz
17.5MHz or more and less than 22.5MHz,	less than -37dBm/MHz

(ii) 10MHz system

offset frequency : Δf	Permissible level
15MHz or more and less than 20MHz,	less than -21-32/19x(Δf-10.5) dBm/MHz
20MHz or more and less than 25MHz,	less than -37dBm/MHz

(2) Base station

(i) 5MHz system

offset frequency : Δf	Permissible level
7.5MHz or more and less than 12.25MHz,	less than -15-1.4x(Δf-7.5) dBm/MHz
12.25MHz or more and less than 22.5MHz,	less than -22dBm/MHz

(ii) 10MHz system

offset frequency : Δf	Permissible level
15MHz or more and less than 25MHz,	less than -22dBm/MHz

3.2.1.7 Spurious emission (NT No.651,2007)

(1) Mobile station

9kHz or more and less than 150kHz,	less than -13dBm/kHz
150kHz or more and less than 30MHz,	less than -13dBm/10kHz
30MHz or more and less than 1000MHz,	less than -13dBm/100kHz
1000MHz or more and less than 2505MHz,	less than -13dBm/MHz
2505MHz or more and less than 2530MHz,	less than -37dBm/MHz

2530MHz or more and less than 2535MHz,	less than 1.7f-4338 dBm/MHz
2535MHz or more and less than 2630MHz,	less than -18dBm/MHz
2630MHz or more and less than 2630.5MHz,	less than -13-8/3.5x(f-2627) dBm/MHz
2630.5MHz or more and less than 2640MHz,	less than -21-16/9.5x(f-2630.5) dBm/MHz
2640MHz or more and less than 2655MHz,	less than -37dBm/MHz
2655MHz or more,	less than -13dBm/MHz

Permissible level for 2535MHz or more and less than 2630MHz should be applied to the frequency range where a frequency offset from the center frequency of a carrier is equal to or more than 2.5 times of the system frequency bandwidth.

(2) Base station

9kHz or more and less than 150kHz,	less than -13dBm/kHz
150kHz or more and less than 30MHz,	less than -13dBm/10kHz
30MHz or more and less than 1000MHz,	less than -13dBm/100kHz
1000MHz or more and less than 2505MHz,	less than -13dBm/MHz
2505MHz or more and less than 2535MHz,	less than -42dBm/MHz
2535MHz or more and less than 2630MHz,	less than -13dBm/MHz
2630MHz or more and less than 2634.75MHz,	less than -15-7/5x(f-2629.75) dBm/MHz
2634.75MHz or more and less than 2655MHz,	less than -22dBm/MHz
2655MHz or more,	less than -13dBm/MHz

Permissible level for 2535MHz or more and less than 2630MHz should be applied to the frequency range where a frequency offset from the center frequency of a carrier is equal to or more than 2.5 times of the system frequency bandwidth.

3.2.1.8 Intermodulation (NT No.651, 2007)

(1) 5 MHz System

Intermodulation emission generated by mixing a desirable emission within regulated power and disturbing waves at ±5MHz offset and at ±10 MHz offset from the desired emission with powers of 30dB less than that of desirable emission should be less than permissible level of the spurious emission and adjacent channel leakage power.

(2) 10 MHz system

Intermodulation emission generated by mixing a desirable emission within regulated power and disturbing waves at ±10MHz offset and at ±20 MHz offset from the desired emission with powers of 30dB less than that of desirable emission should be less than permissible level of the spurious emission and adjacent channel leakage power.

3.2.1.9 Standby output power (ORE, Article 49.28)

Mobile station: -30dBm or less

Base station: -30dBm or less

3.2.1.10 Antenna gain (ORE, Article 49.28)

Mobile station: 2dBi or less

Base station: 17dBi or less

3.2.1.11 Cabinet radiation

Cabinet radiation shall be 4nW/MHz in e.i.r.p. or the permissible spurious emission value* in the spurious region measured at the antenna terminal plus 0dBi.

(* Refer to subclause 3.2.1.7 for the spurious emission.)

3.2.2 Receiver requirement

3.2.2.1 Reception sensitivity

(1) Definition

The reception sensitivity shall be defined by the minimum receiver input level (dBm) which yields a bit error rate (BER) of 1x10-6 for the QPSK case under AWGN channel. This is the definition for the specified reception sensitivity as well.

(2) Specification

5MHz bandwidth system

Mobile station :-91.3dBm or less

Base station :-91.3dBm or less

10MHz bandwidth system

Mobile station :-88.3dBm or less

Base station :-88.3dBm or less

3.2.2.2 Spurious response rejection ratio

(1) Definition

The spurious response rejection ratio shall be defined as the level ratio of the interfering signal to the desired signal, specified by the following statement:

The level of desired signal shall be set to +3 dB higher than the level of the specified reception sensitivity*. The level of interfering signal shall be the one yielding a bit error rate of 1x10-6 on the desired signal for the QPSK case. The interference signal shall not be modulated.

(* Refer to subclause 3.2.2.1 for the specified reception sensitivity.)

(2) Specification

Mobile stations : The spurious response rejection ratio shall be 11dB or more.

Base station : The spurious response rejection ratio shall be 11dB or more.

3.2.2.3 Adjacent signal selectivity

(1) Definition

The adjacent signal selectivity shall be defined as the level ratio of the interfering signal to the desired signal, specified by the following statement:

The level of desired signal shall be set to +3 dB higher than the level of the specified reception sensitivity*. The level of interfering signal shall be the one yielding a bit error rate of 1x10-6 on the desired signal for the 16QAM case. The interference signal shall be 16QAM and tuned on the first adjacent channel.

(* Refer to Section 3.2.2.1 for the specified reception sensitivity)

(2) Specification

Mobile stations : The adjacent signal selectivity shall be 11dB or more.

Base station : The adjacent signal selectivity shall be 11dB or more.

3.2.2.4 Intermodulation performance

(1) Definition

The intermodulation performance shall be defined as the level of the interfering signal, specified by the following statement:

The level of desired signal shall be set to +3 dB higher than the level of the specified reception sensitivity*. The level of each one of two interfering signals shall be the one yielding a bit error rate of 1x10-6 on the desired signal. The interference signals shall be tuned on the first and second adjacent channel.

(* Refer to Section 3.2.2.1 for the specified reception sensitivity)

(2) Specification

Mobile stations :

The non-modulated interference signal on the first adjacent channel shall be -55dBm.

The modulated interference signal on the second adjacent channel shall be -55dBm.

Base station :

The non-modulated interference signal on the first adjacent channel shall be -45dBm.

The modulated interference signal on the second adjacent channel shall be -45dBm.

3.2.2.5 Conducted Spurious (ORE, Article 24)

Less than 1GHz	:	4nW or less
1GHz or more	:	20nW or less

3.2.3 Transmitter requirement for FWA equipment

3.2.3.1 Frequency tolerance (ORE, Article 5,Table 1)

Land mobile station	Within 2×10^{-6}
Base station	Within 2×10^{-6}

3.2.3.2 Occupied band width (ORE, Article 6,Table 2)

5 MHz system	4.9 MHz or less
10 MHz system	9.9 MHz or less

3.2.3.3 Output power (ORE, Article 49.28)

Land mobile station

Model-1 :	200mW or less
Model-2 :	
Antenna gain	
20dBi or less	200mW or less
More than 20dBi and 23dBi or less	100mW or less
More than 23dBi and 25dBi or less	63mW or less

Model-3 :

Antenna gain	
23dBi or less	200mW or less
More than 23dBi and 25dBi or less	126mW or less

Base station

Antenna gain	
17dBi or less	20W or less

However that only for Model-3, output power is specified as follows.

More than 17dBi and 20dBi or less	10W or less
More than 20dBi and 23dBi or less	5W or less
More than 23dBi and 25dBi or less	3.2W or less

3.2.3.4 Output power tolerance(ORE, Article 14)

Land mobile station	±50%
Base station	±50%

3.2.3.5 Adjacent channel leakage power (NT No.651, 2007)

(1) Mobile station

(i) 5MHz system

Channel space: 5MHz

Occupied bandwidth: 4.8MHz

Permissible adjacent channel leakage power: 2dBm or less

(ii) 10MHz system

Channel space: 10MHz

Occupied bandwidth: 9.5MHz

Permissible adjacent channel leakage power: 0dBm or less

(2) Base station

(i) 5MHz system

Channel space: 5MHz

Occupied bandwidth: 4.8MHz

Permissible adjacent channel leakage power: 7dBm or less

(ii) 10MHz system

Channel space: 10MHz

Occupied bandwidth : 9.5MHz

Permissible adjacent channel leakage power: 3dBm or less

3.2.3.6 Spectrum mask (NT No.651,2007)

(1) Mobile station

(i) 5MHz system

offset frequency : Δf	Permissible level
7.5MHz or more and less than 8MHz,	less than -20-2.28x(Δf-7.5) dBm/MHz
8MHz or more and less than 17.5MHz,	less than -21-1.68x(Δf-8) dBm/MHz
17.5MHz or more and less than 22.5MHz,	less than -37dBm/MHz

(ii) 10MHz system

offset frequency : Δf	Permissible level
15MHz or more and less than 20MHz,	less than -21-32/19x(Δf-10.5) dBm/MHz
20MHz or more and less than 25MHz,	less than -37dBm/MHz

(2) Base station

(i) 5MHz system

offset frequency : Δf	Permissible level
7.5MHz or more and less than 12.25MHz,	less than -15-1.4x(Δf-7.5) dBm/MHz
12.25MHz or more and less than 22.5MHz,	less than -22dBm/MHz

(ii) 10MHz system

offset frequency : Δf	Permissible level
15MHz or more and less than 25MHz,	less than -22dBm/MHz

3.2.3.7 Spurious emission (NT No.651,2007)

(1) Mobile terminal

9kHz or more and less than 150kHz,	less than -13dBm/kHz
150kHz or more and less than 30MHz,	less than -13dBm/10kHz
30MHz or more and less than 1000MHz,	less than -13dBm/100kHz
1000MHz or more and less than 2505MHz,	less than -13dBm/MHz

2505MHz or more and less than 2535MHz,	
For model-1	less than -70dBm/MHz
For model-2	less than -68dBm/MHz
For model-3	less than -61dBm/MHz
2535MHz or more and less than 2630MHz,	less than -18dBm/MHz
2630MHz or more and less than 2630.5MHz,	less than -13-8/3.5x(f-2627) dBm/MHz
2630.5MHz or more and less than 2640MHz,	less than -21-16/9.5x(f-2630.5) dBm/MHz
2640MHz or more and less than 2655MHz,	less than -37dBm/MHz
2655MHz or more,	less than -13dBm/MHz

Permissible level for 2535MHz or more and less than 2630MHz should be applied to the frequency range where a frequency offset from the center frequency of a carrier is equal to or more than 2.5 times of the system frequency bandwidth.

(2) Base station

9kHz or more and less than 150kHz,	less than -13dBm/kHz
150kHz or more and less than 30MHz,	less than -13dBm/10kHz
30MHz or more and less than 1000MHz,	less than -13dBm/100kHz
1000MHz or more and less than 2505MHz,	less than -13dBm/MHz
2505MHz or more and less than 2535MHz,	less than -42dBm/MHz
2535MHz or more and less than 2630MHz,	less than -13dBm/MHz
2630MHz or more and less than 2634.75MHz,	less than -15-7/5x(f-2629.75) dBm/MHz
2634.75MHz or more and less than 2655MHz,	less than -22 dBm/MHz
2655MHz or more,	less than -13 dBm/MHz

Permissible level for 2535MHz or more and less than 2630MHz should be applied to the frequency range where a frequency offset from the center frequency of a carrier is equal to or more than 2.5 times of the system frequency bandwidth.

3.2.3.8 Intermodulation (NT No.651,2007)

(1) 5 MHz System

Intermodulation emission generated by mixing a desirable emission within regulated power and disturbing waves at ±5MHz offset and at ±10 MHz offset from the desired emission with powers of 30dB less than that of desirable emission should be less than permissible level of the spurious emission and adjacent channel leakage power.

(2) 10 MHz system

Intermodulation emission generated by mixing a desirable emission within regulated power and disturbing waves at ±10MHz offset and at ±20 MHz offset from the desired emission with powers of 30dB less than that of desirable emission should be less than permissible level of the spurious emission and adjacent channel leakage power.

3.2.3.9 Standby output power (ORE, Article 49.28)

Mobile station: -30dBm or less

Base station: -30dBm or less

3.2.3.10 Antenna gain (ORE, Article 49.28)

Mobile station:

Model-1 :	10dBi or less
Model-2 :	25dBi or less
Model-3 :	25dBi or less

Base station:

17dBi or less. However that only for Model-3, it shall 25dBi or less.

3.2.3.11 Cabinet radiation

During idol mode cabinet radiation shall not greater than following level.

Spectrum band	Permissible level
1000MHz or less	-54dBm/MHz
More than 1000MHz and less than 2505MHz	-47dBm/MHz
2505MHz or more and 2535MHz or less;	
Model-1	-62dBm/MHz
Model-2	-50dBm/MHz
Model-3	-47dBm/MHz

3.2.4 Receiver requirement for FWA equipment

3.2.4.1 Reception sensitivity

(1) Definition

The reception sensitivity shall be defined by the minimum receiver input level (dBm) which yields a bit error rate (BER) of 1x10-6 for the QPSK case under AWGN channel.

This is the definition for the specified reception sensitivity as well.

(2) Specification

5MHz bandwidth system

Mobile station : -91.3dBm or less

Base station : -91.3dBm or less

10MHz bandwidth system

Mobile station : -88.3dBm or less

Base station : -88.3dBm or less

3.2.4.2 Conducted Spurious (ORE, Article 24)

During reception mode, output power level at the antenna port shall not greater than following level.

Mobile station

Spectrum band	Permissible level
9kHz or more and less than 150kHz	-54dBm/kHz
150kHz or more and less than 30MHz	-54dBm/10kHz
30MHz or more and less than 1000MHz	-54dBm/100kHz
1000MHz or more and less than 2505MHz	-47dBm/MHz
2505MHz or more and 2535MHz or less;	
Model-1	-70dBm/MHz
Model-2	-68dBm/MHz
Model-3	-61dBm/MHz
More than 2535MHz	-47dBm/MHz

Base station

(i) Antenna gain is 17dBi or less

Spectrum band	Permissible level
1GHz or less	4nW
More than 1GHz	20nW

(ii) Antenna gain is more than 17dBi

Spectrum band	Permissible level

9kHz or more and less than 150kHz	-54dBm/kHz
150kHz or more and less than 30MHz	-54dBm/10kHz
30MHz or more and less than 1000MHz	-54dBm/100kHz
1000MHz or more and less than 2505MHz	-47dBm/MHz
2505MHz or more and 2535MHz or less	-61dBm/MHz
More than 2535MHz	-47dBm/MHz

Chapter 4 System Profile

The system profile of the 2.5 GHz Mobile WiMAX is defined in "WiMAX Forum™ Mobile System Profile" provided by WiMAX Forum as shown in Attachment 3 which is linked to the following electrical document.

Attachment 3 wimax_forum_mobile_system_profile_release 1.0 v1.40.pdf

Chapter 5. Network Architecture

The End-to-End Network Systems Architecture of the 2.5 GHz Mobile WiMAX is defined in "WiMAX forum network architecture Stage 2-3" provided by WiMAX Forum as shown in Attachment 4 which is linked to the following electrical documents.

Attachment 4-1 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-Abbreviations.pdf

Attachment 4-2 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-Part 0.pdf

Attachment 4-3 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-Part 1.pdf

Attachment 4-4 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-Part 2.pdf

Attachment 4-5 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-Part 3.pdf

Attachment 4-6 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-WiMAX Interworking with DSL.pdf

Attachment 4-7 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-3GPP - WiMAX Interworking.pdf

Attachment 4-8 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-2-3GPP2 - WiMAX Interworking.pdf

Attachment 4-9 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-3.pdf

Attachment 4-10 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-3-Annex-3GPP-Interworking.pdf

Attachment 4-11 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-3-Annex-3GPP2-Interworking.pdf

Attachment 4-12 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-3-Annex-

Prepaid-Accounting.pdf

Attachment 4-13 End-to-End Network Systems Architecture Stage 2 R1.1.0-Stage-3-Annex-R6-R8-ASN-Anchored-Mobility-Scenarios.pdf

Chapter 6. Measurement Method

As for the items stipulated in Ordinance Concerning Technical Regulations Conformity Certification etc. of Specified Radio Equipment Appendix Table No.1 item 1(3), measurement methods are specified by MIC Notification(Note) or a method that surpasses or is equal to the method.

Note: This Notification refers to MIC Notification No.88 "The Testing Method for the Characteristics Examination"(January 26, 2004) as of the date of the revision of this standard version 1.0 (issued at December , 2007). Thereafter, the latest version of Notification would be applied if this Notification or contents of this Notification would be revised.

Attachment 1　List of Essential Industrial Property Rights (selection of option 1)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO. 〔Applied in Japan 〕	備考 （出願国名） REMARKS
(N/A)	(N/A)	(N/A)	(N/A)

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
NOKIA Corporation *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		
NTT DoCoMo Inc. *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		
Motorola, Inc. *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		
Qualcomm Inc. *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		
FUJITSU LIMITED *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		
KDDI CORPORATION *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
NEC Corporation *10	(1) 可変変調通信方法	特許第2776094号	
	(2) 多方向多重通信システムの送信出力電力制御方法	特許第2982724号	
	(3) 直交周波数分割多重変復調回路	特許第3786129号	
	(4) 送信電力制御方法、送信電力制御装置、移動局、基地局及び制御局	特許第3358565号	
	(5) 移動通信システム及び通信制御方法並びにそれに用いる基地局、移動局	特許第3675433号	
	(6) 位置登録方法および位置登録方式	特許第2748871号	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　(Reference: Not applied in Japan)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
Motorola, Inc. *10	Multiple user communication system, device and method with overlapping uplink carrier spectra	US5828660A	
	Synchronous coherent orthogonal frequency division multiplexing system, method, software and device	US5867478A	
	Multicarrier reverse link timing synchronization system, device and method	US5802044A	
	Communication system having a packet structure field	US4860003A	
	Method and apparatus for providing cryptographic protection of a data stream in a communication system	US5319712A	
	Wideband signal synchronization	US5272724A	
	Communication signal having a time domain pilot component	US5519730A	
	Dynamic control of a data channel in a TDM wireless communication system	US5598417A	
	Method for authentication and protection of subscribers in telecommunications systems	US5572193A	
	Communication unit and method for performing neighbor site measurements in a communication system	US6249678B1	
	Variable rate spread spectrum communication method and apparatus	US6275488B1	
	Apparatus and method for providing separate forward dedicated and shared control channels in a communications system	US6934275B1	
	Multi-mode hybrid ARQ scheme	US7096401B2	
	Adaptive hybrid ARQ using turbo code structure	US6308294B1	
	Method and apparatus for transmission and reception of narrowband signals within a wideband communication system	US7047006B2	
	Multi channel stop and wait ARQ communication method and apparatus	US7065068B2	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0..

Approved by the 69th Standard Assembly

Attachment 2　List of Essential Industrial Property Rights　　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./APPLICATION NO.	備考 （出願国名） REMARKS
NTT DoCoMo Inc. *11	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.1		

*11: This patent is applied to the revised part of ARIB STD-T94 Ver.1.1.

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
Motorola, Inc. *10	パケット構造フィールドを有する通信システム	特表平3-501079	WO, AT, AU, BE, CH, DE, FR, GB, IT, KR, LU, NL, NO, SE,US
	電話通信システムにおける加入者の真正証明および保護のための方法	特表平5-503816	WO, AT, AU, BE, CA, CH, DE, DK, ES, FR,U, NL, SE
	時間領域パイロット成分を有する通信信号	特表平5-501189	WO, AT, AU, BE, BR, CA, CH, DE, DK, ES, FR, GB, GR, IT, KR, LU, NL, SE, US
	電気通信システムにおける加入者の真正証明及び保護のための方法	特表平5-508274	WO, CA, US
	QAM通信システムにおけるピーク対平均電力比の軽減方法	特表平6-504175	WO, AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE, US
	時間領域パイロット成分を有する通信信号	特表平6-504176	WO, AU, BR, CA, GB, KR
	通信システムにおいてデータ・ストリームの暗号化保護を提供する方法および装置	特表平8-503113	WO, CA, FI, KR, AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, US

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
Motorola, Inc. *10	ターボコード構造を使用する適応ハイブリッドARQ	特表2003-515268	WO, BR, CA, KR, AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR, US
	マルチチャネル・ストップ・アンド・ウェイトARQ通信のための方法および装置	特表2003-514486	WO, BR, CA, KR, AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR, US
	通信システムにおいて別個の順方向専用チャネル及び共用制御チャネルを与える装置及び方法	特表2003-531534	WO, AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
Motorola, Inc. *10	広帯域の通信システム内で狭帯域の信号を送信および受信するための方法および装置	特表2007-525930	WO, AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW
	Multi-mode hybrid ARQ scheme	WO2006055171A1	WO, AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Approved by the 70th Standard Assembly

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
NOKIA CORPORATION *10	多重アクセス通信システム及び多重アクセス通信方法、並びにその通信装置	特許第 3090300 号	
	無線電話システム、及び無線電話ネットワーク内でのデータ送信方法、無線電話器並びに固定局	特許第 3842805 号	
	無線電話ＴＤＭＡシステムにおいてパケットデータを伝送するシステム	特許第 3880642 号	
	ＴＤＭＡシステムにおける無線容量の動的割り振り方法	特許第 3155010 号	
	ハンドオーバ方法及びセルラ無線システム	特許第 3825049 号	
	情報の暗号化方法およびデータ通信システム	特開 2006-262531	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
NOKIA CORPORATION *10	アイドルタイムを割り振る方法、移動及びネットワーク	特許第 3943253 号	
	データ伝送を暗号処理する方法とその方法を利用するセルラ無線システム	特開 2006-271010	
	無線資源制御方法	特許第 3542705 号	
	移動通信システムにおいてある複数プロトコルに従ってある複数層でデータを処理するための方法と装置	特許第 3445577 号	
	複数アンテナ送信用の非ゼロ複素重み付けした空間－時間符号	特表 2005-503045	
	移動局の内部タイミングエラーを補償する方法及び回路	特許第 3923571 号	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Approved by the 71st Standard Assembly

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
KDDI株式会社 *10 株式会社KDDI研究所 *10 京セラ株式会社 *10	(1) OFDM信号復調装置	特願平11-159320	
	(2) OFDM信号復調用シンボルタイミング検出回路	特願2000-022459	
	(3) OFDM受信装置の周波数及び位相誤差補正装置	特願2000-070186	
	(4) OFDM信号復調用シンボルタイミング検出方法及び装置	特願2000-246978	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
KDDI株式会社 *10	(5) 無線パケット通信システム及び基地局	特願2000-368610 特許3731469 米国特許7012910	 US
	(6) 多ビームセルラ無線基地局､移動機及びスペクトル拡散信号送信方法	特願2001-115422	
	(7) 無線基地局	特願2001-190109	
	(8) フレーム同期回路	特願2002-037926 特許3826810	
	(9) 直交周波数分割多重方式の受信装置及び受信方法	特願2002-114677 特許3846356	
	(10) OFDM信号の周波数誤差を補正する受信装置	特願2002-135473 特許3885657	
	(11) 伝搬路推定を行うOFDM受信装置	特願2002-229887 特許3791473	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
KDDI株式会社 *10 小林英雄 *10	(12) 伝送路特性推定装置および伝送路特性推定方法、無線復調装置、コンピュータプログラム	特願2002-373986	
	(13) 伝送路特性推定装置および伝送路特性推定方法、無線復調装置、コンピュータプログラム	特願2003-025910	
	(14) CNR推定装置、CNR推定方法、CNR推定プログラム、適応伝送無線システム、無線装置	特願2003-067938	
KDDI株式会社 *10	(15) 伝送路特性推定装置、コンピュータプログラム 受信装置及び受信方法	特願2003-204611	
	(16) 伝達関数推定装置及び、伝達関数推定方法	特願2006-082414	
	(17) 受信装置、送信装置	特願2006-094340	
	(18) 無線フレーム制御装置、無線通信装置及び無線フレーム制御方法	特願2006-192128	
	(19) 無線フレーム制御装置、無線フレーム制御方法、および無線通信装置	特願2007-93760	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
三菱電機株式会社 *10	データ伝送方法、データ受信方法、データ伝送システム、送信機及び受信機	特許第 3,895,745 号	EP(DE,FR,IT,PT,GB), US, CA, AU

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Approved by the 73rd Standard Assembly

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 PATENT HOLDER	発明の名称 NAME OF PATENT	出願番号等 REGISTRATION NO./ APPLICATION NO.	備考 （出願国名） REMARKS
株式会社　日立コミュニケーションテクノロジー *10	A comprehensive confirmation form has been submitted with regard to ARIB STD-T94 Ver.1.0		

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　　(selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
QUALCOMM Incorporated *10	Method and apparatus for measuring channel state information	JP2003-530010	US, AU, BR, CA, EP, HK, ID, IL, IN, JP, KR, MX, NO, WO, RU, SG, TW, UA
	Multiplexing of real time services and non-real time services for OFDM systems	JP2004-503181	US, BR, CN, EP, HK, KR, TW, WO
	Method and apparatus for utilizing channel state information in a wireless communication system	JP2005-502223	US 6,771,706, US 20040165558, BE, BR, CN, DE, EP, ES, FI, FR, GB, HK, IE, IT, JP, KR, LU, NL, SE, TW, WO
	Rate selection for an OFDM system	JP2005-533402	US 7,012,883, US 20060087972, BR, CN, EP, HK, KR, TW, WO
	Diversity Transmission Modes for MIMO OFDM Communication Systems	JP2005-531219	US 7,095,709, US 20060193268, AU, BR, CA, CN, EP, HK, ID, IL, IN, KR, MX, NO, RU, SG, TW, UA, WO
	Random Access for Wireless Multiple-Access Communication Systems	JP2006-504338	US, AU, BR, CA, CN, EP, HK, ID, IL, IN, KR, MX, RU, TW, UA, WO
	Reverse Link Automatic Repeat Request	JP2006504337	US, AU, BR, CA, CN, EP, HK, ID, IL, IN, KR, MX, RU, TW, UA, WO

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights (selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
QUALCOMM Incorporated *10	MIMO System with Multiple Spatial Multiplexing Modes	JP2006-504339	US 20040136349, US 12/115,522, US 12/115,523, AU, BR, CA, CN, EP, HK, ID, IL, IN, KR, MX, RU, TW, UA, WO
	Transmit Diversity Processing for a Multi-Antenna Communication System	JP2006-504366	US 7,002,900, US 20060039275, AU, BR, CA, CN, EP, HK, ID, IL, IN, KR, MX, RU, TW, UA, WO
	A method and apparatus of using a single channel to provide acknowledgement and assignment messages	JP2007-520169	US, AU, CN, HK, IN, KR, WO
	Shared signaling channel for a communication system	JP2008-507896	US, CA, CL, CN, EP, HK, IN, KR, MY, TW, WO
	Apparatus and Method for Reducing Message Collision Between Mobile Stations Simultaneously Accessing a Base Station in a CDMA Cellular Communications System	JP3152353	US 5,544,196, US 6,615,050, AT, AU, BE, BR, BG, CA, CH, DE, DK, KP, EP, ES, FI, FR, GB, GR, HK, HU, IE, IL, IT, KR, MX, NL, WO, CN, PT, RU, ZA, SE, SK

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 （出願国名） REMARKS
QUALCOMM Incorporated *10	Method and apparatus for performing mobile assisted hard handoff between communications Systems	JP2001-508625	US, AM, AU, AZ, BR, BY, CA, CL, IL, DE, EPC, EP, ES, FI, FR, GB, HK, ID, IE, IN, IT, KG, KR, KZ, MD, MX, NL, NZ, WO, CN, TW, RU, ZA, SE, SG, TJ, TM, UA
	Method and Apparatus for High Rate Packet Data Transmission	JP2001522211	US 7,079,550, US 20060280160, US 20070066320, US 20070019567, US 20070025267, AR, AT, AU, BE, BR, CA, CH, CL, CN, CY, CZ, EP, HK, NZ, DE, DK, ES, FI, FR, GB, GR, HU, ID, IE, IL, IN, IT, JP, KR, LU, MY, MC, MX, NL, NO, WO, PL, PT, RO, RU, ZA, SE, SG, UA, VN
	Method and Apparatus for Coordinating Transmission of Short Messages with Hard Handoff Searches in a Wireless Communications System	JP2002-514844	AU, BR, US 20060120490, US 20070153941, CA, DE, EP, FI, FR, GB, HK, IL, IT, JP, KR, MX, NO, WO, CN, TW, SE, SG
	Reservation Multiple Access	JP2002-528017	US, CN, EP, HK, KR, WO

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　(selection of option 2)

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 (出願国名) REMARKS
Panasonic Corporation *10	直交周波数分割多重信号の伝送方法ならびにその送信装置および受信装置	特許第3539522号	
	受信装置、送信装置及び送信方法	特許第 3836019 号	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0.

Attachment 2　List of Essential Industrial Property Rights　（Reference: Not applied in Japan）

特許出願人 (PATENT HOLDER)	発明の名称 (NAME OF PATENT)	出願番号等 (REGISTRATION NO. / APPLICATION NO.)	備考 (出願国名) REMARKS
QUALCOMM Incorporated *10	Mobile Station Assisted Soft Handoff in a CDMA Cellular Communications System	US5,640,414	US 5,267,261
	Method and Apparatus for Utilizing Channel State Information in a Wireless Communication System	US 7,006,848	
	Remote Transmitter Power Control in a Contention Based Multiple Access System	US 5,604,730	

*10: These patents are applied to the part defined by ARIB STD-T94 Ver. 1.0

Attachment 3

WiMAX Forum™ Mobile System Profile

Release 1.0 v1.40

WiMAX Forum™ Mobile System Profile

Release 1.0 Approved Specification

(Revision 1.4.0: 2007-05-02)

TABLE OF CONTENTS

LIST OF TABLES

Participants

This document was developed by the WiMAX Forum™ Technical Working Group (TWG).

Co-chair; Wonil Roh, Samsung
Co-chair: Vladimir Yanover, Alvarion
Editor: Hassan Yaghoobi, Intel Corp.

Following is the list of voting member companies during the development of this document.

Adaptix, Agilent, Airspan, Alcatel, Alvarion, Amicus, Aperto Networks, ArrayComm, Beceem, British Telecom, Broadcom, AT4 Wireless, Nextwave, Ericsson, ETRI, Fujitsu, Huawei Technologies, Intel Corp., KDDI, KT Corp., LG Electronics, Lucent Technologies, Marvell, Mitsubishi Electronics, Motorola, Navini, NEC, Nokia, Nortel Networks, PMC Sierra, Posdata, Redline, Rhode and Schwartz, Runcom Technologies Ltd., Samsung, SEQUANS Communications, Siemens Mobile, Soma Networks, Sprint, SR Telecom, Telecom Italia, Texas Instruments, Wavesat and ZTE Corp.

Revision History

Table 1. Change Control Revision History

Version	Date	Comment
1.4.0	2007-05-02	Applied CRs SYP-0001 and SYP-0002.

Abstract

This document is prepared by the Technical Working Group (TWG) to provide the descriptions of the OFDMA based system profiles of Mobile WiMAX.

1. Scope

The main objective of this document is to provide OFDMA System Profile specification of mobile network, complementary to 802.16-2004 as amended by 802.16e-2005 standard, primarily for the purpose of certification of conformant Subscriber Stations and Base Stations.

2. References

[1] **IEEE Standard 802.16-2004**, IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Wireless Access Systems.

[2] **IEEE Standard 802.16e-2005**, Amendment to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems- Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

[3] **WiMAX Forum™ Mobile Certification Profile**, WiMAX, Certification Working Group, April 2006

[4] **IEEE 802.16-2004/Cor2 Ballot Commentary 80216-06_066r2.cmt,** IEEE 802.16 Working Group, November 2006

3. Definitions

For the purposes of the present document, the following terms and definitions apply:

3.1 *Abbreviations*

3.2 *Definitions of system profiles*

Profile definitions of different devices/usage models and releases are provided in this subsection.

3.3 *Conventions*

3.3.1 Item column

The Item column contains a number that identifies each description in the table.

3.3.2 Description column

The description column describes in free text each respective item (e.g., parameters, timers, etc.).

3.3.3 Reference column

The reference column indicates the section of [1] and [2] from which the requirement for the item is derived.

3.3.4 Status column

The following notations are used in the status column to indicate whether each item is mandatory or optional in IEEE standard based on 802.16-2004 [1] as amended by 802.16e-2005 [2].

Table 2. Status Column Entries

m	Explicitly shown as mandatory in the standard. It is required to implement
pm	Potentially mandatory, required for the system to perform basic operations (Not explicitly shown as mandatory in the standard). It is required to implement.
o	Explicitly mentioned as optional in the standard or is not explicitly mentioned but has capability negotiations. It may or may not be implemented.
oi	Qualified option – for mutually exclusive or selectable options from a set. One or more of the options from the set shall be supported.
po	Potentially optional. Not explicitly mentioned as mandatory, but from the standard we may conclude it is, though not really required for the system to perform basic operations. We have to decide whether it should be defined as optional
n/a	Not applicable – in the given context, it is impossible to use the capability.

3.3.5 BS/MS Required column

The Required column indicates whether the item is required for every BS/MS to implement for WiMAX certification purposes.

Table 3. Required Column Entries

Y or **y**.	Required to implement
N or **n**	Not required to implement.
IO-NNNN	Inter-operable Options: Item belongs to NNNN group of features for which it is requested to provide testing procedure and distinct labeling of BS equipment. More specifically ▪ The item is not required to get general “WiMAX certified” label and ▪ Is required to get distinct “WiMAX certified with NNNN capability” label.
n/a	Not applicable

The following Inter-operable Options are defined and used in this document.

1. IO-MIMO: Group of Inter-operable Option features related to Multiple Input Multiple Output (MIMO) operation.
2. IO-BF: Group of Inter-operable Option features related to Beam Forming (BF) operation.
3. IO-MBS: Group of Inter-operable Option features related to Multicast and Broadcast Services (MBS) operation.
4. IO-ETHx (x = 1, 2, 3): Groups of Inter-operable Option features related to Ethernet CS

3.3.6 BS/MS Values column

This column indicates the specific value or range of values for each BS/MS to implement for WiMAX certification purposes.

Table 4. Value Column Entries

xx	Set to value xx
aa - bb	Set to range aa - bb
n/a	Not applicable

3.3.7 Comment column

This column provides additional clarification and reasoning for each item.

4. PHY Profile

4.1 *Profiles of BS and MS*

4.1.1 System Parameters

4.1.1.1 *PHY Mode*

Table 5. PHY Mode

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	OFDMA	8.4	m	Y	Y	OFDMA is the sole PHY mode within the scope of this document.

4.1.1.2 Band Class Index

System profile requirements of this document are applied to the following band class indices. Each index shall specify one frequency range and one or more combinations of channel bandwidth, FFT size, channel raster and duplexing mode.

BS support for a particular band class requires support of a frequency range that is a subset of the complete frequency range defined by the band-class. The BS vendor shall provide a declaration of the supported frequency range. The supported frequency range shall be a minimum of three (3) times the largest supported channel bandwidth. MS must support the entire range of frequency defined by a band class (or sub-bands) while the BS is required to support only sub-range of the band class declared by vendor.

Table 6. Band Class Index

Band Class Index	Frequency Range (GHz)	Channel Frequency Step (kHz)	Channel Bandwidth(s) (MHz)	FFT Size	Duplexing Mode	Comments
1	2.3-2.4	250	5	512	TDD	Both bandwidths must be supported by the MS
			10	1024	TDD	
			8.75	1024	TDD	
2	2.305-2.320, 2.345-2.360	250	3.5	512	TDD	
			5	512	TDD	
			10	1024	TDD	
3	2.496-2.69	250 (200 KHz step size is also	5	512	TDD	Both bandwidths must be supported
			10	1024	TDD	

		recommended for band class 3 in Europe)				to by the MS
4	3.3-3.4	250	5	512	TDD	
			7	1024	TDD	
			10	1024	TDD	
5	3.4-3.8	250	5	512	TDD	
			7	1024	TDD	
			10	1024	TDD	
	3.4-3.6	250	5	512	TDD	
			7	1024	TDD	
			10	1024	TDD	
	3.6-3.8	250	5	512	TDD	
			7	1024	TDD	
			10	1024	TDD	

4.1.1.3 *Sampling Factor*

Table 7. Sampling Factor

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	If channel bandwidth is a multiple of 1.75MHz then n=8/7 else if channel bandwidth is a multiple of any of 1.25, 1.5, 2 or 2.75 MHz then n=28/25 else if not otherwise specified then n=8/7.	8.4.2.3	m	Y	Y	

4.1.1.4 *Cyclic Prefix*

Table 8. Cyclic Prefix

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	1/4	8.4.2.3	oi	N	N	
2	1/8	8.4.2.3	oi	Y	Y	
3	1/16	8.4.2.3	oi	N	N	
4	1/32	8.4.2.3	oi	N	N	

4.1.1.5 *Frame Length*

Table 9. Frame Length

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	20 ms	8.4.5.2	oi	N	N	
2	12.5	8.4.5.2	oi	N	N	
3	10	8.4.5.2	oi	N	N	

4	8	8.4.5.2	oi	N	N	
5	5	8.4.5.2	oi	Y	Y	
6	4	8.4.5.2	oi	N	N	
7	2.5	8.4.5.2	oi	N	N	
8	2	8.4.5.2	oi	N	N	

4.1.1.6 *TTG/RTG*

This parameter shall be applicable only to TDD mode.

Table 10. TTG/RTG

Item	Description	Reference	Status	BS Required	BS Values	MS Required	Comment
1	TTG	8.4.5.2	m	Y	296 PS for 10 MHz, 218 PS for 8.75 MHz, 376 PS for 7 MHz, 148 PS for 5 MHz and 188 PS for 3.5 MHz	n/a	5 us minimum specified in the referred section. The requirement is equivalent to "5 msec - (RTG+ Number of OFDM symols x symbol duration)" where "Number of OFDM symols" = 47 for 10 and 5 MHz, 42 for 8.75 MHz and 33 for 7 MHz.
2	RTG	8.4.5.2	m	Y	168 PS for 10 MHz, 186 PS for 8.75 MHz, 120 PS for 7 MHz, 84 PS for 5 MHz and 60 PS for 3.5 MHz	n/a	5 us minimum specified in the referred section. The requirement is equivalent to 60 us for 5, 10 and 7 MHz BW and 74.4 us for 8.75 MHz BW.

4.1.1.7 *Number of OFDM Symbols in DL and UL*

This feature shall be applicable to TDD operation only and specifies number of OFDM symbols in DL and UL subframes.

Table 11. Number of OFDM Symbols in DL and UL

Item	Description	Reference	Status	BS Required	BS Values	MS Required	MS Values	Comment

Item	Description	Reference	Status	BS Required	BS Values	MS Required	MS Values	Comment
1	Number of OFDM Symbols in DL and UL for 5 and 10 MHz BW	8.4.4.2	oi	Y	(35, 12), (34, 13), (33, 14), (32, 15), (31, 16), (30, 17), (29, 18), (28, 19), (27, 20), (26, 21)	Y	The same as BS values	
2	Number of OFDM Symbols in DL and UL for 8.75 MHz BW	8.4.4.2	oi	Y	(30, 12), (29, 13), (28, 14), (27, 15), (26, 16), (25, 17), (24, 18)	Y	The same as BS values	
3	Number of OFDM Symbols in DL and UL for 7 and 3.5 MHz BW	8.4.4.2	oi	Y	(24, 09), (23, 10), (22, 11), (21, 12), (20, 13), (19, 14), (18, 15)	Y	The same as BS values	

4.1.2 Subcarrier Allocation

4.1.2.1 DL Subcarrier Allocation

Table 12. DL Subcarrier Allocation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	PUSC	8.4.6.1.2.1	m	Y	Y	
2	PUSC w/ all subchannels	8.4.6.1.2.1	po	Y	Y	
3	PUSC w/ dedicated pilots	8.4.6.1.2.1 and 8.4.5.3.4	po	IO-BF	Y	Also refer [4]
4	FUSC	8.4.6.1.2.2	po	Y	Y	
5	FUSC w/ dedicated pilots	8.4.6.1.2.2 and 8.4.5.3.4	po	N	N	
6	Optional FUSC	8.4.6.1.2.3	o	N	N	
7	O-FUSC w/ dedicated pilots	8.4.6.1.2.3 and 8.4.5.3.4	o	N	N	
8	AMC 1x6	8.4.6.3	o	N	N	

	AMC 2x3	8.4.6.3	o	Y	Y	
	AMC 3x2	8.4.6.3	o	N	N	
	Default Type	8.4.6.3 and 6.3.2.3.43.2	o	N	N	Only applicable with HARQ_MAP
9	AMC 1x6 w/ dedicated pilots	8.4.6.3 and 8.4.5.3.4	o	N	N	
	AMC 2x3 w/ dedicated pilots	8.4.6.3 and 8.4.5.3.4	o	IO-BF	Y	Also refer [4]
	AMC 3x2 w/ dedicated pilots	8.4.6.3 and 8.4.5.3.4	o	N	N	
10	PUSC-ASCA	8.4.6.4.1	o	N	N	

4.1.2.2 *UL Subcarrier Allocation*

Table 13. UL Subcarrier Allocation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	PUSC	8.4.6.2.1	po	Y	Y	
2.	PUSC w/o subchannel rotation	11.3.1	o	IO-BF	Y	Also refer [4]
3.	Optional PUSC	8.4.6.2.5	o	N	N	
4.	AMC 1x6	8.4.6.3	o	N	N	
	AMC 2x3	8.4.6.3	o	Y	Y	Also refer [4]
	AMC 3x2	8.4.6.3	o	N	N	
5.	Mini-subchannel	8.4.6.2.4	o	N	N	Only for PUSC & O-PUSC

4.1.2.3 *Common SYNC Symbol*

Table 14. Common SYNC Symbol

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Support of the Common SYNC Symbol	8.4.6.1.1.1	o	N	N	

4.1.2.4 *UL Sounding*

Table 15. UL Sounding 1

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Type A w/ Cyclic shift - support for P values other than 9 and 18	8.4.6.2.7.1	o	IO-BF	Y	

Item	Description	Reference	Status	BS Required	MS Required	Comment
2	Type A w/ Cyclic shift – Support P values of 9 and 18	8.4.6.2.7.1	o	IO-BF	Y	
3	Type A w/ Decimation	8.4.6.2.7.1	o	IO-BF	Y	
4	Type B	8.4.6.2.7.1	o	N	N	
5	Send Sounding Report Flag	8.4.6.2.7.1	o	N	N	
6	Direct transmission of DL channel coefficients (Include additional feedback, option 0b01)	8.4.6.2.7.1 and 8.4.6.2.7.3	o	N	N	
7	Decimation with randomization	8.4.6.2.7.1	o	N	N	
8	Power Assignment Method: Equal Power (0b00)	8.4.6.2.7.1 and 8.4.6.2.7.	oi	IO-BF	Y	
9	Power Assignment Method: Interference dependent. Per subcarrier power limit; (0b10)	8.4.6.2.7.1 and 8.4.6.2.7.2	oi	N	N	
10	Power Assignment Method: Interference dependent. Total power limit.; (0b11)	8.4.6.2.7.1 and 8.4.6.2.7.2	oi	N	N	
11	Power Boost	8.4.6.2.7.1 and 8.4.6.2.7.2	o	N	N	
12	Feedback of Received Pilot Coefficients (include additional feedback option = 0b10)	8.4.6.2.7.1 and 8.4.6.2.7.4	o	N	N	
13	Feedback of message (include additional feedback option = 0b11)	8.4.6.2.7.1	o	N	N	

Table 16. UL Sounding 2

Item	Description	Reference	Status	MS Required	MS Value	Comment
1	Sounding response time capability	8.4.6.2.7.1 and 11.8.3.7.14	o	Y	Next Frame	
2	max number of simultaneous sounding	8.4.6.2.7.1 and 11.8.3.7.14	o	Y	2	This parameter specifies the max number of sounding transmutations

	instructions					by MS in a frame.

4.1.3 UL Control Channels

4.1.3.1 *Initial Ranging*

Table 17. Initial Ranging

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Initial Ranging in PUSC zone w/ 2 symbols	8.4.7.1	oi	Y	Y	
2	Initial Ranging in PUSC zone w/ 4 symbols	8.4.7.1	oi	N	N	
3	Initial Ranging in Optional PUSC zone w/ 2 symbols	8.4.7.1	oi	N	N	
4	Initial Ranging in Optional PUSC zone w/ 4 symbols	8.4.7.1	oi	N	N	
5	Initial Ranging in AMC zone w/ 2 symbols	8.4.7.1	oi	N	N	
6	Initial Ranging in AMC zone w/ 4 symbols	8.4.7.1	oi	N	N	

4.1.3.2 *HO Ranging*

Table 18. HO Ranging

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	HO Ranging in PUSC zone w/ 2 symbols	8.4.7.1	o	Y	Y	
2	HO Ranging in PUSC zone w/ 4 symbols	8.4.7.1	o	N	N	
3	HO Ranging in Optional PUSC zone w/ 2 symbols	8.4.7.1	o	N	N	
4	HO Ranging in Optional PUSC zone w/ 4 symbols	8.4.7.1	o	N	N	
5	HO Ranging in AMC zone w/ 2 symbols	8.4.7.1	o	N	N	
6	HO Ranging in AMC zone w/ 4 symbols	8.4.7.1	o	N	N	

4.1.3.3 *Periodic Ranging*

Table 19.Periodic Ranging

Item	Description	Reference	Status	BS Required	MS Required	Comment

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Periodic Ranging in PUSC zone w/ 1 symbols	8.4.7.2	oi	Y	Y	
2	Periodic Ranging in PUSC zone w/ 3 symbols	8.4.7.2	oi	N	N	
3	Periodic Ranging in Optional PUSC zone w/ 1 symbols	8.4.7.2	oi	N	N	
4	Periodic Ranging in Optional PUSC zone w/ 3 symbols	8.4.7.2	oi	N	N	
5	Periodic Ranging in AMC zone w/ 1 symbols	8.4.7.2	oi	N	N	
6	Periodic Ranging in AMC zone w/ 3 symbols	8.4.7.2	oi	N	N	

4.1.3.4 *BW Request*

Table 20. BW Request

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	BW Request in PUSC zone w/ 1 symbols	8.4.7.2	oi	Y	Y	
2	BW Request in PUSC zone w/ 3 symbols	8.4.7.2	oi	N	N	
3	BW Request in Optional PUSC zone w/ 1 symbols	8.4.7.2	oi	N	N	
4	BW Request in Optional PUSC zone w/ 3 symbols	8.4.7.2	oi	N	N	
5	BW Request in AMC zone w/ 1 symbols	8.4.7.2	oi	N	N	
6	BW Request in AMC zone w/ 3 symbols	8.4.7.2	oi	N	N	

4.1.3.5 *Fast-Feedback/CQI Channel Encoding*

Table 21. Fast-Feedback/CQI Channel Encoding

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	4 bits	8.4.5.4.10	po	N	N	
2	6 bits	8.4.5.4.10.5	o	Y	Y	This feature is needed for FBSS.
3	3 bits	8.4.5.4.10.5	o	N	N	
4	Primary/Secondary	8.4.5.4.10.12	o	N	N	

Note on Item 2: If the "Feedback Type" in CQICH_Alloc_IE() is set to "0b01 = Effective CINR Feedback" and the MS negotiation capability "Type 173, bit#1 = Enhanced FAST_FEEDBACK" is enabled which indicates support for "6-bit CQI", the reported effective CINR shall be in the 0b00xxxx format where the 4 LSBs is described in Table 298b of Section 8.4.5.4.10.4 in [2].

4.1.3.6 *Fast-Feedback/CQI Channel Allocation Method*

Table 22. Fast-Feedback/CQI Channel Allocation Method

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Fast-Feedback Allocation Subheader support	6.3.2.2.6	o	N	N	
2	Fast feedback channel allocation using CQICH Allocation IE	8.4.5.4.12	o	Y	Y	
3	Fast feedback channel allocation using CQICH Enhanced Allocation IE	8.4.5.4.16	o	N	N	

4.1.4 Channel Coding

4.1.4.1 *Repetition*

Table 23. Repetition

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Repetition	8.4.9	m	Y	Y	FCH uses repetition coding (8.4.4.4)

4.1.4.2 *Randomization*

Table 24. Randomization

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Randomization	8.4.9.1	m	Y	Y	

4.1.4.3 *Convolutional Code*

Table 25. Convolutional Code

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Tail Biting	8.4.9.2.1	m	Y	Y	
2	Zero Tail	8.4.9.2.4	o	N	N	

4.1.4.4 *Convolutional Turbo Code*

Table 26. Convolutional Turbo Code

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	CTC	8.4.9.2.3 excluding 8.4.9.2.3.5	o	Y	Y	

4.1.4.5 *BTC*

Table 27. Block Turbo Code

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	BTC	8.4.9.2.2	o	N	N	

4.1.4.6 *LDPC*

Table 28. Low Density Parity Check Code

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	LDPC	8.4.9.2.5	o	N	N	

4.1.4.7 *Interleaving*

Table 29. Interleaving

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Interleaving	8.4.9.3	m	Y	Y	The interleaving subject of this section should not be applied to CTC mode.
2	Optional interleaver for CC	8.4.9.3.1 and 11.8.3.7.3	o	N	N	This interleaver mode is only applicable to Convolutional Encoding

4.1.5 H-ARQ Support

4.1.5.1 *Chase Combining*

Table 30. Chase Combining H-ARQ

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Chase w/ CC	8.4.15.1	o	N	N	
2	Chase w/ CTC	8.4.15.1	o	Y	Y	
3	Chase with LDPC	8.4.15.1	o	N	N	

Table 31. HARQ Parameters for Chase with CTC

Item	Parameter Description	Reference	Values	Comment
1	H-ARQ DL Buffer size per channel	11.8.3.7.19	Category 1 = 16,384 (K=20), Category 2 = 8192 (K=16), Category 3 = 16,384 (K=20), Category 4 = 23,170 (K=22)	Status for the four categories is oi, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.
2	H-ARQ UL Buffer size per channel	11.8.3.7.19	Category 1 = 16,384 (K=20), Category 2 = 16,384 (K=20), Category 3 = 16,384 (K=20), Category 4 = 16,384 (K=20)	Status for the four categories is oi, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.
3	DL Aggregate flag for HARQ buffer	11.8.3.7.19	Category 1 = ON or OFF, Category 2 = ON, Category 3 = ON, Category 4 = ON	Status for the four categories is oi, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.
4	UL Aggregate flag for HARQ buffer	11.8.3.7.19	Category 1 = OFF, Category 2 = ON, Category 3 = ON, Category 4 = ON	Status for the four categories is i.o, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.
5	HARQ ACK Delay for DL Burst	6.3.17.1, 11.3.1	1	
6	HARQ ACK Delay for UL Burst	6.3.17.1, 11.4.1	N/A	

Item	Parameter Description	Reference	Values	Comment
7	Number of DL H-ARQ Channels supported by MS	11.8.3.7.2 and 7.3 D5	Category 1 = 4, Category 2 = 16, Category 3 = 16, Category 4 = 16	Status for the four categories is oi, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.
8	Number of UL H-ARQ Channels supported by MS	11.8.3.7.2 and 7.3 D5	Category 1 = 4, Category 2 = 8, Category 3 = 8, Category 4 = 8	Status for the four categories is oi, that is support for values of items 1-4 and 7-8 corresponding to one or more of the categories from the set shall be supported.

Note that the HARQ buffer size shall be interpreted as softbits buffer size, i.e. relating to coded data bits and not un-coded. This means the buffer size refers to both the systematic and parity bits transmitted over the air. It is left to vendor's implementation to determine the amount of memory space for each bit of transmitted information. The buffer size is related to buffer size parameter K according to the following Equation.

$$\text{Buffer size} = floor\left[512 * 2^{(K/4)}\right]$$

4.1.5.2 *Incremental Redundancy*

Table 32. Incremental Redundancy H-ARQ

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	IR w/ CC	8.4.9.2.1.1	o	N	N	
2	IR w/ CTC	8.4.9.2.3.5	o	N	N	

4.1.5.3 *ACK Channel*

Table 33. ACK Channel

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	ACKCH	8.4.5.4.13	m	Y	Y	Conditioned by H-ARQ" support

4.1.6 Control Mechanism

4.1.6.1 *Synchronization*

Table 34. Synchronization

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	BS Synchronization in time /slot	8.4.10.1.1, 6.3.2.3.47	o	Y	N/A	Refer to "Time/Frequency Synchronization Indicator" in Table 108h of the referred section.
2	BS Synchronization in frequency	8.4.10.1.1	o	Y	N/A	
3	BS to Neighbor BS Synchronization in frequency	6.3.2.3.47	o	Y	N/A	Refer to "Time/Frequency Synchronization Indicator" in Table 108h of the referred section.
4	SS Synchronization	8.4.10.1.2	m	N/A	Y	

4.1.6.2 *Closed-loop Power Control*

Table 35. Closed-loop Power Control

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	CL Power Control	8.4.10.3.1	m	Y	Y	

4.1.6.3 *Open-loop Power Control*

Table 36. Open-loop Power Control

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	OL Power Control	8.4.10.3.2	o	Y	Y	
2	Passive Uplink open loop power control	8.4.10.3.2	o	Y	Y	
3	Active Uplink open loop power control	8.4.10.3.2	o	N	N	
4	UL Tx power and Headroom transmission condition using bandwidth request and UL Tx Power Report header	8.4.10.3.2.1 and 6.3.2.1.2.1.2	o	Y	Y	

5	UL Tx power and Headroom transmission condition using PHY channel report header	8.4.10.3.2.1 and 6.3.2.1.2.1.5	o	N	N	
6	UL Tx power and Headroom transmission condition using Tx power report extended subheader	8.4.10.3.2.1 and 6.3.2.2.7.5	o	N	N	

4.1.7 Channel Measurement

4.1.7.1 CINR Measurement

Table 37. CINR Measurement

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Physical CINR measurement from the preamble for frequency reuse==1 (feedback type=0b00 and report type=0 and CINR preamble report type=0)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	Y	Y	
2	Physical CINR measurement from the preamble for frequency reuse==3 (feedback type=0b00 and report type=0 and CINR preamble report type=1)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	Y	Y	
3	Physical CINR measurement for a permutation zone from pilot subcarriers (feedback type=0b00 and report type=1 and CINR zone measurement type=0)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	Y	Y	Also refer [4]
4	Physical CINR measurement for a permutation zone from data subcarriers (feedback type=0b00 and report type=1 and CINR zone measurement type=1)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	N	N	
5	Effective CINR measurement from the preamble for frequency reuse==1 (feedback type=0b01 and report type=0 and CINR preamble report type=0)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	N	N	This option provides capability to the MS to report MCS preference to BS.

Item	Description	Reference	Status	BS Required	MS Required	Comment
6	Effective CINR measurement from the preamble for frequency reuse==3 (feedback type=0b01 and report type=0 and CINR preamble report type=1)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	N	N	This option provides capability to the MS to report MCS preference to BS.
7	Effective CINR measurement for a permutation zone from pilot subcarriers (feedback type=0b01 and report type=1 and CINR zone measurement type=0)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	Y	Y	This option provides capability to the MS to report MCS preference to BS. Also refer [4]
8	Effective CINR measurement for a permutation zone from data subcarriers (feedback type=0b01 and report type=1 and CINR zone measurement type=1)	6.3.18, 8.4.5.4.12, 8.4.11.3 and 11.8.3.7.9	oi	N	N	This option provides capability to the MS to report MCS preference to BS.
9	Support for 2 concurrent CQI channels with effective CINR reports	6.3.18, 8.4.5.4.12 and 11.8.3.7.9	o	N	N	This feature only addresses two concurrent CQI channels reporting Effective CINR measurements.
10	Frequency selectivity characterization report	8.4.5.4.12, 8.4.11.4 and 11.8.3.7.9	o	N	N	
11	Major group indication (applicable to PUSC zone only)	8.4.5.4.12	o	IO-BF	Y	
12	MIMO permutation feedback cycle (applicable to MIMO only)	8.4.5.4.12	o	IO-MIMO	Y	

4.1.7.2 *RSSI Measurement*

Table 38. RSSI Measurement

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	RSSI Measurement	8.4.11.2 and 6.3.2.3.50	m	N/A	Y	Processing of RSSI

						measurements in the BS is specified in Section 6.3.2.3.33.

4.1.8 Modulation

4.1.8.1 *PRBS (Subcarrier Randomization)*

Table 39. PRBS

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	PRBS	8.4.9.4.1	m	Y	Y	

4.1.8.2 *Downlink*

Table 40. Downlink Modulation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	QPSK	8.4.9.4.2	m	Y	Y	
2	16-QAM	8.4.9.4.2	m	Y	Y	
3	64-QAM	8.4.9.4.2	o	Y	Y	

4.1.8.3 *Uplink*

Table 41. Uplink Modulation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	QPSK	8.4.9.4.2	m	Y	Y	
2	16-QAM	8.4.9.4.2	m	Y	Y	
3	64-QAM	8.4.9.4.2	o	N	N	

4.1.8.4 *Pilot Modulation*

Table 42. Pilot Modulation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Pilot Modulation	8.4.9.4.3	m	Y	Y	

4.1.8.5 *Preamble Modulation*

Table 43. Preamble Modulation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Preamble Modulation	8.4.9.4.3.1	m	Y	N/A	MS shall demodulate the preamble

4.1.8.6 *Ranging Modulation*

Table 44. Ranging Modulation

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Ranging Modulation	8.4.7.3	m	N/A	Y	BS shall demodulate the ranging signal.

4.1.9 MAP Support

4.1.9.1 *Normal MAP*

Table 45. Normal MAP

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Normal MAP	6.3.2.3.2 and 6.3.2.3.4	m	Y	Y	

4.1.9.2 *Compressed MAP*

Table 46. Compressed MAP

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Compressed MAP	8.4.5.6	po	Y	Y	

4.1.9.3 *Sub-DL-UL MAP*

Table 47. Sub-DL-UL MAP

Item	Description	Reference	Status	BS Required	MS Required	Comment

1	Sub-DL-UL MAP	6.3.2.3.60	o	Y	Y	See 11.8.3.7.12 OFDMA MAP Capability of [2]. Support for Extended HARQ IE in Normal MAP mandates a support for Sub MAP for first zone. Also refer [4]

4.1.9.4 *H-ARQ MAP Message*

Table 48. H_ARQ MAP Message

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Compact DL-MAP IE	6.3.2.3.43	o	N	N	
2	Compact UL-MAP IE	6.3.2.3.43	o	N	N	

4.1.9.5 *Extended HARQ IE in the Normal MAP*

Table 49. Extended H-ARQ IE in Normal MAP

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Extended HARQ IE in the Normal MAP	8.4.5.3.21 & 8.4.5.3.22 & 8.4.5.4.25 & 8.4.5.4.24	o	Y	Y	

4.1.9.6 *DL Region Definition*

Table 50. DL Region Definition Support

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	DL Region Definition Support	8.4.5.3.21, 8.4.5.3.23, 11.8.3.7.12	o	N	N	

4.1.10 AAS

4.1.10.1 *AAS Zone Support*

Table 51. AAS Zone Support

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	DL AAS Zone	8.4.4.6	o	N	N	
2	UL AAS Zone	8.4.4.6	o	N	N	

4.1.10.2 *Supported Permutation in DL*

Table 52. Supported Permutation in DL

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	PUSC	8.4.4.6.1 and 8.4.6.1.2.1	oi	N	N	Support for all the items in this table is conditional to the support of DL AAS Zone.
2	FUSC	8.4.4.6.1 and 8.4.6.1.2.2	oi	N	N	
3	Optional PUSC	8.4.4.6.1 and 8.4.6.1.2.3	oi	N	N	
4	AMC 2x3	8.4.4.6.1 and 8.4.6.3	oi	N	N	
5	TUSC 1	8.4.4.6.1 and 8.4.6.1.2.4	oi	N	N	
6	TUSC 2	8.4.4.6.1 and 8.4.6.1.2.5	oi	N	N	

4.1.10.3 *Supported Permutation in UL*

Table 53. Supported Permutation in UL

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	PUSC	8.4.4.6.1 and 8.4.6.2.1	oi	N	N	Support for all the items in this table is conditional to the support of AAS Zone.
2	Optional PUSC	8.4.4.6.1 and 8.4.6.2.5	oi	N	N	

3	AMC 2x3	8.4.4.6.1 and 8.4.6.3	oi	N	N	

4.1.10.4 *AAS DL Preamble*

Table 54. AAS DL Preamble

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Frequency shifted	8.4.4.6.4.1	o	N	N	
2	Time shifted	8.4.4.6.4.1	o	N	N	
3	PHY Modifier	8.4.5.3.11	o	N	N	
4	DL AAS Preamble Support	8.4.4.6.4.1	o	N	N	Support for 0-3 symbols

4.1.10.5 *AAS UL Preamble*

Table 55. AAS UL Preamble

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Frequency shifted	8.4.4.6.4.2	o	N	N	
2	Time shifted	8.4.4.6.4.2	o	N	N	
3	Physical Modifier	8.4.5.4.14	o	N	N	
4	UL AAS Preamble Power Control	8.4.4.6.4	o	N	N	
5	UL AAS Preamble Support	8.4.4.6.4.1	o	N	N	Support for 0-3 symbols

4.1.10.6 *Diversity MAP Scan*

Table 56. Diversity MAP Scan

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Diversity-Map Scan	8.4.4.6.2	o	N	N	

4.1.10.7 *DL AAS-SDMA Pilots*

Table 57. DL AAS-SDMA Pilots

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	AMC AAS-SDMA with All SDMA Pilots	8.4.6.3.3	o	N	N	
2	PUSC AAS-SDMA	8.4.8.1.2.1.1	o	N	N	

3	TUSC1 AAS-SDMA	8.4.6.1.2.6	o	N	N	
4	TUSC2 AAS-SDMA	8.4.6.1.2.6	o	N	N	
5	AMC AAS-SDMA with SDMA pilots A&B only	8.4.6.3.3	o	N	N	

4.1.10.8 *UL AAS-SDMA Pilots*

Table 58. UL AAS_SDMA Pilots

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	AMC AAS-SDMA with All SDMA Pilots	8.4.6.3.3	o	N	N	
2	PUSC AAS-SDMA	8.4.8.1.5	o	N	N	
3	Optional PUSC AAS-SDMA	8.4.8.4.1	o	N	N	
4	AMC AAS-SDMA with SDMA pilots A&B only	8.4.6.3.3	o	N	N	

4.1.10.9 *AAS Private MAP*

Table 59. AAS Private MAP

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	AAS Private MAP	8.4.5.6	o	N	N	
2	Reduced Private MAP	8.4.5.8	o	N	N	
3	Reduced Private MAP Chain Support	8.4.5.8	o	N	N	

4.1.10.10 *AAS-FBCK-REQ/RSP support*

Table 60. AAS_FBCK/RSP Support

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	AAS-FBCK-REQ/RSP support	8.4.5.7	o	N	N	

4.1.11 STC/MIMO

4.1.11.1 *Supported Features for DL PUSC*

Table 61. Supported Features for DL PUSC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	FHDC	8.4.8.1.3	o	N	N	
2	2-antenna, matrix A	8.4.8.1.2.1.1 8.4.8.1.4	o	IO-MIMO	Y	
3	2-antenna, matrix B, vertical encoding	8.4.8.1.4, 8.4.8.1.2.1.3	o	IO-MIMO	Y	
4	2-antenna, matrix B, horizontal encoding	8.4.8.1.4, 8.4.8.1.2.1.3	o	N	N	two modulation and coding modules
5	4-antenna enhancement using directivity	8.4.8.1.6	o	N	N	
6	4-antenna, matrix A	8.4.8.2.1 8.4.8.2.3	o	N	N	
7	4-antenna, matrix B, vertical encoding	8.4.8.2.3	o	N	N	
8	4-antenna, matrix B, horizontal encoding	8.4.8.2.3	o	N	N	
9	4-antenna, matrix C, vertical encoding	8.4.8.2.3	o	N	N	
10	4-antenna, matrix C, horizontal encoding	8.4.8.2.3	o	N	N	

4.1.11.2 *Supported Features for DL FUSC*

Table 62. Supported Features for DL FUSC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	FHDC		o	N	N	
2	2-antenna, matrix A	8.4.8.1.2.1.2 8.4.8.1.4	o	N	N	
3	2-antenna, matrix B, vertical encoding	8.4.8.1.4, 8.4.8.1.2.1.3	o	N	N	
4	2-antenna, matrix B, horizontal encoding	8.4.8.1.4, 8.4.8.1.2.1.3	o	N	N	
5	4-antenna enhancement using directivity	8.4.8.1.6	o	N	N	
6	4-antenna, matrix A	8.4.8.2.2	o	N	N	
7	4-antenna, matrix B, vertical encoding	8.4.8.2.3	o	N	N	
8	4-antenna, matrix B, horizontal encoding	8.4.8.2.3	o	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
9	4-antenna, matrix C, vertical encoding	8.4.8.2.3	o	N	N	
10	4-antenna, matrix C, horizontal encoding	8.4.8.2.3	o	N	N	

4.1.11.3 *Supported Features for DL Optional FUSC*

Table 63. Supported Features for DL Optional FUSC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.3	o	N	N	2 consecutive OFDMA symbols
2	2-antenna, matrix B, vertical encoding	8.4.8.3.1.2.2 8.4.8.3.3, 8.4.8.1.2.1.3	o	N	N	
3	2-antenna, matrix B, horizontal encoding	8.4.8.3.1.2.2 8.4.8.3.3, 8.4.8.1.2.1.3	o	N	N	
4	2-antenna, matrix C	8.4.8.3.1.2.2 8.4.8.3.3	o	N	N	
5	3-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.4	o	N	N	2 logical subcarriers over 2 consecutive symbols
6	3-antenna, matrix B	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.4	o	N	N	
7	3-antenna, matrix C	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.4	o	N	N	
8	4-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	2 logical subcarriers over 2 consecutive symbols
9	4-antenna, matrix B, vertical encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	
10	4-antenna, matrix B, horizontal encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
11	4-antenna, matrix C, vertical encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	
12	4-antenna, matrix C, horizontal encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	

4.1.11.4 *Supported Features for DL Optional AMC*

Table 64. Supported Features for DL Optional AMC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.1 8.4.8.3.3	o	N	N	2 bins over 6 OFDMA symbols
2	2-antenna, matrix B, vertical encoding	8.4.8.3.1.2.1 8.4.8.3.3, 8.4.8.1.2.1.3	o	N	N	Figure 251i
3	2-antenna, matrix B, horizontal encoding	8.4.8.3.1.2.1 8.4.8.3.3, 8.4.8.1.2.1.3	o	N	N	Figure 251i
4	2-antenna, matrix C	8.4.8.3.1.2.1 8.4.8.3.3	o	N	N	
5	3-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.1 8.4.8.3.4	o	N	N	2 adjacent subcarriers over 2 consecutive symbols
6	3-antenna, matrix B	8.4.8.3.1.1 8.4.8.3.1.2.1 8.4.8.3.4	o	N	N	
7	3-antenna, matrix C	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.4	o	N	N	
8	4-antenna, matrix A	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	2 adjacent subcarriers over 2 consecutive symbols
9	4-antenna, matrix B, vertical encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	
10	4-antenna, matrix B, horizontal encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
11	4-antenna, matrix C, vertical encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	
12	4-antenna, matrix C, horizontal encoding	8.4.8.3.1.1 8.4.8.3.1.2.2 8.4.8.3.5	o	N	N	

4.1.11.5 *Supported Features for DL PUSC-ASCA*

Table 65. Supported Features for DL PUSC-ASCA

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	STC/MIMO for PUSC-ASCA	8.4.8.3.2	o	N	N	

4.1.11.6 *Supported Features in UL PUSC*

Table 66. Supported Features in UL PUSC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2-antenna, matrix A	8.4.8.1.5	o	N	N	
2	2-antenna, matrix B, vertical encoding	8.4.8.1.5	o	N	N	
3	2-antenna, matrix B, horizontal encoding	8.4.8.1.5	o	N	N	pp. 574 in [2]
4	Collaborative SM for two MS with single transmit antenna	8.4.8.1.5	o	IO-MIMO	Y	
5	Collaborative SM for two MS with two transmit antennas	8.4.8.1.5	o	N	N	Pilot pattern C and D defined in[2]

4.1.11.7 *Supported Features in UL Optional PUSC*

Table 67. Supported Features in UL Optional PUSC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2-antenna, matrix A	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	2 consecutive slots

Item	Description	Reference	Status	BS Required	MS Required	Comment
2	2-antenna, matrix B, vertical encoding	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	
3	2-antenna, matrix B, horizontal encoding	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	
4	Collaborative SM for two MS with single transmit antenna	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	

4.1.11.8 *Supported Features in UL Optional AMC*

Table 68. Supported Features in UL Optional AMC

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2-antenna, matrix A	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	Same AMC pilots as in DL 1x6 format
2	2-antenna, matrix B, vertical encoding	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	
3	2-antenna, matrix B, horizontal encoding	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	
4	Collaborative SM for two MS with single transmit antenna	8.4.8.4.1 8.4.8.4.2 8.4.8.4.3	o	N	N	

4.1.11.9 *Closed-Loop MIMO*

Table 69. Closed-loop MIMO

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Antenna Grouping w/ 3 Tx matrix A	8.4.5.4.10.3 8.4.8.3.4.1	o	N	N	Table 298
2	Antenna Grouping w/ 3 Tx matrix B	8.4.5.4.10.3 8.4.8.3.4.2	o	N	N	
3	Antenna Selection w/ 3 Tx matrix C	8.4.5.4.10.3, 8.4.8.3.4.3	o	N	N	Table 298a Table 317f
4	Antenna Grouping w/ 4 Tx matrix A	8.4.5.4.10.3 8.4.8.3.5.1	o	N	N	Table 298
5	Antenna Grouping w/ 4 Tx matrix B	8.4.5.4.10.3 8.4.8.3.5.2	o	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
6	Antenna Selection w/ 4 Tx matrix C	8.4.5.4.10.3, 8.4.8.3.5.3	o	N	N	Table 298a Table 317g
7	Codebook Based Precoding	8.4.8.3.6, 8.4.5.4.11	o	N	N	
8	Quantized Weight Feedback	8.4.5.4.10.2	o	N	N	4-bit CQICH
9	Quantized Weight Feedback	8.4.5.4.10.6	o	N	N	6-bit CQICH

4.1.11.10 *MIMO Feedback*

Table 70. MIMO Feedback

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Fast MIMO Feedback (complex weights) w/ 4 bits	8.4.5.4.10.2	o	N	N	
2	Mode Selection Feedback w/ 4 bits	8.4.5.4.10.3	o	N	N	
3	3-bit MIMO Fast Feedback	8.4.5.4.10.4	o	N	N	
4	Fast DL measurement feedback w/ more than one Rx antennas	8.4.5.4.10.5 8.4.5.4.10.6 8.4.5.4.10.1	o	IO-MIMO	Y	
5	Fast MIMO Feedback (complex weights) w/ 6 bits	8.4.5.4.10.7	o	N	N	
6	Mode Selection Feedback w/ 6 bits	8.4.5.4.10.8	o	IO-MIMO	Y	

4.1.11.11 *MIMO Midamble*

Table 71. MIMO Midamble

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	2 Tx	8.4.8.5.2.1	o	N	N	
2	3 Tx	8.4.8.5.2.2	o	N	N	
3	4 Tx	8.4.8.5.2.2	o	N	N	

4.1.11.12 *MIMO Soft-Handover Based Macro-diversity*

Table 72. MIMO Soft-Handover Macro-diversity

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Macro MIMO w/	8.4.8.2.4	o	N	N	

	MIMO_in_another_BS_IE()					
2	Macro MIMO w/ Macro_MIMO_DL_Basic_IE()	8.4.8.2.4	o	N	N	

4.1.11.13 *H-ARQ Downlink Support for MIMO*

Table 73. H-ARQ Downlink Support for MIMO

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	MIMO DL Chase	8.4.5.3.21	o	IO-MIMO	Y	MIMO DL Chase is applicable to CC, CTC or LDPC from the perspective of IEEE 802.16. In this document, the feature is only used in CTC mode.
2	MIMO DL IR	8.4.5.3.21 8.4.8.3.1.2.3	o	N	N	w/ CTC
3	MIMO DL IR for Convolutional Code	8.4.5.3.21	o	N	N	
4	MIMO DL STC	8.4.5.3.21.1	o	N	N	

4.1.11.14 *H-ARQ Uplink Support for MIMO*

Table 74. H-ARQ Uplink Support for MIMO

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	MIMO UL Chase	8.4.5.4.24	o	IO-MIMO	Y	MIMO DL Chase is applicable to CC, CTC or LDPC from the perspective of IEEE 802.16. In this document, the feature is only used in CTC mode.
2	MIMO UL IR	8.4.5.4.24	o	N	N	
3	MIMO UL IR for Convolutional Code	8.4.5.4.24	o	N	N	
4	MIMO UL STC	8.4.8.4.24.2	o	N	N	

4.1.12 HO Support in PHY

4.1.12.1 *FBSS*

Table 75. Fast Base Station Switching

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Anchor BS Report for FBSS	8.4.5.4.10.8 and 8.4.5.4.23	o	N	N	Anchor BS CQI and switch indication via CQICH

4.1.12.2 *MIMO Soft-handover based macro-diversity transmission*

Table 76. MIMO Soft-handover based macro-diversity transmission

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	MIMO Soft-handover based macro-diversity transmission	8.4.8.2.4	o	N	N	
2	Support Macro Diversity Handover using DL soft combining	8.4.5.3.6	o	N	N	
3	Support Macro Diversity Handover using DL burst in another segment in PUSC mode	8.4.5.3.13	o	N	N	
4	Support anchor BS indication of DL data burst in active BS	8.4.5.3.14	o	N	N	
5	Support of active BS indication of DL data burst in anchor BS	8.4.5.3. 15	o	N	N	
6	Support of CID translation between Anchor BS and Active BS	8.4.5.3.16	o	N	N	

4.1.12.3 *UL Macro diversity*

Table 77. UL Macro Diversity

Item	Description	Reference	Status	BS Required	MS Required	Comment

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	UL Macro diversity	8.4.5.4.17	o	N	N	To be used with UL PUSC Burst Allocation in Other Segment IE
2	Support of Macro Diversity Handover using UL transmission in another segment in PUSC mode	8.4.5.4.17	o	N	N	
3	Support of anchor BS indication of UL data burst in active BS	8.4.5.4.18	o	N	N	
4	Support of active BS indication of UL data burst in anchor BS	8.4.5.4.19	o	N	N	

4.2 *Performance/Fidelity Requirements*

4.2.1 MS Minimum Performance

4.2.1.1 *SSTTG/SSRTG*

Table 78. SSTTG/SSRTG

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	SSTTG	8.4.4.2	m	Y	50 usec	
2	SSRTG	8.4.4.2	m	Y	50 usec	

4.2.1.2 *Max DL Concurrent Bursts*

Table 79. Maximum DL Concurrent Bursts

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	Max Concurrent Burst	8.4.4.2 and 11.7.8.13	m	Y	10	

4.2.1.3 *Max Bursts in DL Subframe*

Table 80. Max Bursts in DL Subframe

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	Max Burst in Frame	8.4.4.2	m	Y	16	

4.2.1.4 *Max Number of Zones in DL/UL Subframe*

Table 81. Max Number of Zones in DL and UL Subframes

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	Maximum numbers of zones UL			Y	3	The number is the same as the number of Zone Switch IEs plus 1.
2	Maximum numbers of zones DL	8.4.4.2	Max 8	Y	5	The number is the same as the number of Zone Switch IEs plus 1.

4.2.1.5 *Measurement Processes and CQI Channels*

Table 82. Measurement Processes and CQI Channels

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	Maximum numbers of CQI Channels transmitted by an MS per frame			Y	2	
2	Maximum number of concurrent CINR measurement processes			Y	2	Maximum number of CINR measurement processes (for physical or effective CINR) that are active concurrently. A CINR measurement process is active from the frame in which it was allocated by a CQICH_Alloc_IE() until the frame in which the last CQI periodic transmission is sent or in which the CQI was de-allocated by the BS.

4.2.1.6 *Max H-ARQ Bursts in DL/UL Subframe*

Table 83. Max H-ARQ Bursts

Item	Description	Reference	Status	MS Required	MS Values	Comment
1	Max Burst in DL Subframe with H-ARQ	8.4.4.2, 8.4.15.1.3, 11.8.3.7.15	o	Y	Category 1 = 2, Category 2 = 5, Category 3 = 5, Category 4 = 5	Status for the four categories is oi, i.e. support for values corresponding to one or more of the categories from the set shall be supported in correlation to the categories of Section 4.1.5.1.
2	Max Burst in UL Subframe with H-ARQ	8.4.4.2, 8.4.15.1.3, 11.8.3.7.15	o	Y	Category 1 = 2, Category 2 = 2, Category 3 = 2, Category 4 = 2	

4.2.2 Transmit Requirements

Note: unless specified otherwise, requirement applies to both BS and MS.

Table 84. Transmitter Requirements

Item	Requirement	Reference	Values Specified	Values Required
1.	BS Tx dynamic Range	8.4.12.1		10 dB
2.	MS Tx dynamic Range	8.4.12.1		45 dB
3.	MS Tx power level min adjustment step	8.4.12.1	1 dB	1 dB
4.	MS Tx power level min relative step accuracy	8.4.12.1	Single step size m | Required relative accuracy |m| = 1dB | +/- 0.5 dB |m| = 2dB | +/- 1 dB |m| = 3dB | +/- 1.5 dB 4db< |m|< = 10dB | +/- 2 dB Two exception points of at least 10 dB apart are allowed over the 45 dB range, where in these two points an accuracy of up to +/- 2 dB is allowed for any size step.	Single step size m | Required relative accuracy |m| = 1dB | +/- 0.5 dB |m| = 2dB | +/- 1 dB |m| = 3dB | +/- 1.5 dB 4db< |m|< = 10dB | +/- 2 dB Two exception points of at least 10 dB apart are allowed over the 45 dB range, where in these two points an accuracy of up to +/- 2 dB is allowed for any size step.
5.	Spectral flatness	8.4.12.2	≤ ±2 dB for spectral lines from $-N_{used}/4$ to –1 and +1 to	≤ ±2 dB for spectral lines from $-N_{used}/4$ to –1 and +1 to

Item	Requirement	Reference	Values Specified		Values Required
			$N_{used}/4$ Within +2/-4 dB for spectral lines from $-N_{used}/2$ to $-N_{used}/4$ and $+N_{used}/4$ to $N_{used}/2$		$N_{used}/4$ Within +2/-4 dB for spectral lines from $-N_{used}/2$ to $-N_{used}/4$ and $+N_{used}/4$ to $N_{used}/2$
6.	Power difference between adjacent subcarriers	8.4.12.2	≤ 0.4 dB		≤ 0.4 dB
7.	BS Tx reference timing accuracy	8.4.12.4, 8.4.10.1.1	Tx downlink radio frame shall be time-aligned with the 1pps timing pulse		1 usec
8.	Tx relative constellation error	8.4.12.3.1 for BS and 8.4.12.3.2 for MS	QPSK 1/2	≤ -15.0 dB	≤ -15.0 dB
			QPSK 3/4	≤ −18.0 dB	≤ −18.0 dB
			16-QAM 1/2	≤ -20.5 dB	≤ -20.5 dB
			16-QAM 3/4	≤ -24.0 dB	≤ -24.0 dB
			64-QAM 1/2 (if 64-QAM supported)	≤ -26.0 dB	≤ -26.0 dB
			64-QAM 2/3 (if 64-QAM supported)	≤ -28.0 dB	≤ -28.0 dB
			64-QAM 3/4 (if 64-QAM supported)	≤ -30.0 dB	≤ -30.0 dB

4.2.3 Receiver Requirements

Table 85. Receiver Requirements

Item	Requirement	Reference	Values Specified	Values Required

Item	Requirement	Reference	Values Specified		Values Required
1.	Min SNR requirements for BER=10^{-6} with CTC in AWGN channel (The Min SNR requirements are used along with Eq. 149b to define sensitivity specifications for CTC.)	8.4.13.1	QPSK 1/2 with 60 bytes block size QPSK 3/4 with 54 bytes block size 16-QAM 1/2 with 60 bytes block size 16-QAM 3/4 with 54 bytes block size 64-QAM 1/2 with 54 bytes block size (if 64-QAM supported) 64-QAM 2/3 with 48 bytes block size (if 64-QAM supported) 64-QAM 3/4 with 54 bytes block size (if 64-QAM supported) 64-QAM 5/6 with 60 bytes block size (if 64-QAM supported)		2.9 dB 6.3 dB 8.6 dB 12.7 dB 13.8 dB 16.9 dB 18 dB 19.9 dB
2.	MS Rx max input level on-channel reception tolerance	8.4.13.3.1	-30 dB		-30 dB
3.	BS Rx Max input level on-channel reception tolerance	8.4.13.3.2	-45 dBm		-45 dBm
4.	MS Rx max input level on-channel damage tolerance	8.4.13.4.1	0 dB		0 dB
5.	BS Rx Max input level on-channel damage tolerance	8.4.13.4.2	-10 dBm		-10 dBm
6.	Min adjacent channel rejection at BER=10^{-6} for 3 dB degradation C/I	8.4.13.2	16-QAM 3/4 64-QAM 3/4 (if 64-QAM supported)	10 dB 4 dB	10 dB 4 dB
7.	Min alternate channel rejection at BER=10^{-6} for 3 dB degradation C/I	8.4.13.2	16-QAM 3/4 64-QAM 3/4 (if 64-QAM supported)	29 dB 23 dB	29 dB 23 dB

Item	Requirement	Reference	Values Specified	Values Required
8.	"Implementation loss plus Noise Figure" (dB) value assumed for MS for deriving receiver minimum sensitivity (equation 149b)	8.4.13.1	The min requirement for Implementation Loss and Noise Figure in [2] are 5 and 8 dB respectively.	13 dB Note: Eq. 149b of [2] shall be used for calculation of Rx sensitivity requirements where min SNR values for CC are given in Table 338 of [2] and the min SNR values for CTC mode are specified in the item 1 of this table.
9.	"Implementation loss plus Noise Figure" (dB) value assumed for BS for deriving receiver minimum sensitivity (equation 149b)	8.4.13.1	The min requirement for Implementation Loss and Noise Figure in [2] are 5 and 8 dB respectively.	13 dB Note: Eq. 149b of [2] shall be used for calculation of Rx sensitivity requirements where min SNR values for CC are given in Table 338 of [2] and the min SNR values for CTC mode are specified in the item 1 of this table.
Comments: [Editor's Note: The Accepted CR #653 calls for above requirements of Items 6 and 7 to be applicable to CC FEC. Considering the fact that TWG members believed that the numbers should be revisited for CTC FEC, it is recommended to consider the same requirements for CTC until an agreement by group is developed for possible update. In the case of CTC, the requirements shall be applied to the most sensitive MCS level for each Modulation order. This means for MS equipments and CTC mode, 64-QAM requirements shall be applied to 64-QAM 5/6 and not to 64-QAM 3/4.]				

4.2.4 Frequency and Time Synchronization Requirements

Table 86. Frequency and Time Synchronization Requirements

Item	Requirement	Reference	Values Specified	Values Required	Comment
1.	MS UL symbol timing accuracy	8.4.10.1.2	≤ ± (Tb/8)/4	≤ ± (Tb/32)/4	This requirement includes only the timing error due to MS component and not the effect of inaccuracy of the BS ranging feedback.

2.	BS reference frequency accuracy	8.4.14.1	$\leq \pm 2*10^{-6}$	$\leq \pm 2*10^{-6}$	
3.	BS to BS frequency synchronization accuracy for Hand Over	6.3.2.3.47	1% of OFDMA subcarrier spacing	1% of OFDMA subcarrier spacing	
4.	MS to BS frequency synchronization tolerance	8.4.14.1	≤ 2% of the subcarrier spacing	≤ 2% of the subcarrier spacing	

5. MAC Profile

5.1 *Profiles of BS and MS*

5.1.1 PHS

Table 87. PHS

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	PHS	5.2.3 5.2.3.1 5.2.3.2	o	Y	Y	

5.1.2 CS Options

Table 88. Convergence Sublayer Options

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Packet, IPv4	5.2.6, 11.13.19	oi	Y	Y	
2.	Packet, IPv6	5.2.6, 11.13.19	oi	Y	Y	
3.	Packet, 802.3/Ethernet	5.2.4, 11.13.19	oi	IO-ETH1	N*	* For MS, not required for WiMAX certified label, only optionally certified
4.	Packet, 802.1Q VLAN	5.2.5, 11.13.19	oi	N	N	
5.	Packet, IPv4 over 802.3/Ethernet	5.2.6, 11.13.19	oi	IO-ETH2	N*	* For MS, not required for WiMAX certified label, only optionally certified
6.	Packet, IPv6 over 802.3/Ethernet	5.2.6, 11.13.19	oi	IO-ETH3	N*	* For MS, not required for WiMAX certified label, only optionally certified
7.	Packet, IPv4 over 802.1Q VLAN	5.2.6, 11.13.19	oi	N	N	
8.	Packet, IPv6 over 802.1Q VLAN	5.2.6, 11.13.19	oi	N	N	
9.	ATM	5.2.6, 11.13.19	oi	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
10.	Packet, IPv4 with Header Compression (ROHC)	5.2.6, 11.13.19	oi	Y	Y	
11.	Packet, IPv4 with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	
12.	Packet, IPv6 with Header Compression (ROHC)	5.2.6, 11.13.19	oi	Y	Y	
13.	Packet, IPv6 with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	
14.	Packet, IPv4 over 802.3/Ethernet with Header Compression (ROHC)	5.2.6, 11.13.19	oi	N	N	
15.	Packet, IPv4 over 802.3/Ethernet with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	
16.	Packet, IPv6 over 802.3/Ethernet with Header Compression (ROHC)	5.2.6, 11.13.19	oi	N	N	
17.	Packet, IPv6 over 802.3/Ethernet with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	
18.	Packet, IPv4 over 802.1Q VLAN with Header Compression (ROHC)	5.2.6, 11.13.19	oi	N	N	
19.	Packet, IPv4 over 802.1Q VLAN with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
20.	Packet, IPv6 over 802.1Q VLAN with Header Compression (ROHC)	5.2.6, 11.13.19	oi	N	N	
21.	Packet, IPv6 over 802.1Q VLAN with Header Compression (ECRTP)	5.2.6, 11.13.19	oi	N	N	

Note: At least one of options shall be implemented.

5.1.3 MAC PDU formats

Table 89. MAC PDU Formats

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Reassembly at Rx	6.3.2.2.1, 6.3.3.3.2	m	Y	Y	
2	Fragmentation at Tx	6.3.2.2.1, 6.3.3.3.2	m	Y	Y	Capability is mandatory.
3	Packing of fixed-length MAC SDUs	6.3.2.2.3, 6.3.3.4	o	N	N	
4	Packing of variable-length MAC SDUs at MS	6.3.2.2.3, 6.3.3.4	o	N/A	Y	Unpacking is mandatory. Refer 6.3.3.4.
5	Packing ARQ Feedback Payload	6.3.3.4.3	o	Y	Y	"ARQ Feedback Payload is treated like any other payload" (Refer to 6.3.3.4.3 of [1]) Unpacking of ARQ Feedback Payload is mandatory if ARQ implemented/enabled at the connection
6	Extended subheader support	6.3.2.2.7, 11.7.5	o	Y	Y	Extended subheader support is negotiated

Item	Description	Reference	Status	BS Required	MS Required	Comment
7	Capability of receiving bandwidth requests using Grant management Subheader	6.3.2.2.2	o	Y	N/A	
8	3-bit FSN support		o	N	N	See [2] negotiated during SBC, 11 bits is default

5.1.4 MAC Support of PHY layer

5.1.4.1 *Feedback Mechanism*

Table 90. Feedback Mechanism

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Feedback Header	6.3.2.1.2.2.1	o	Y	Y	
2.	FAST-FEEDBACK allocation subheader	6.3.2.2.6	o	N	N	
3.	MIMO mode feedback extended subheader	8.4.5.4.10.3, 6.3.2.2.7.4	o	N	N	
4.	Feedback request extended subheader	6.3.2.2.7.3	o	N	N	
5.	Mini-Feedback extended subheader	6.3.2.2.7.6	o	N	N	
6.	Feedback Polling IE	8.4.5.4.28	o	Y	Y	
7.	PHY channel report header	6.3.2.1.2.1.5	o	N	N	
8.	UL Tx Power Report extended subheader	6.3.2.2.7.5	o	N	N	

5.1.5 Multicast connection

Table 91. Multicast Connection

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Multicast traffic connection	6.3.13	o	Y	Y	

5.1.6 Network Entry

Table 92. Network Entry

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	SS management support	6.3.9.9.1, 6.3.9.10-12, 6.3.2.3.28-29, 11.7.2	o	N	N	
2	IP management mode	11.7.3	o	N	N	Conditional based on item 1

5.1.7 ARQ

Table 93. ARQ

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	ARQ implementation	6.3.4	o	Y	Y	All items below are conditional dependently on ARQ implementation
2	ARQ ACK type 0 - Selective ACK entry	6.3.4.2, 11.7.23	o	N	N	Negotiable over REG-REQ/RSP (11.7.23 ARQ-ACK Type)
3	ARQ ACK type 1 - Cumulative ACK entry	6.3.4.2, 11.7.23	o	Y	Y	Negotiable over REG-REQ/RSP (11.7.23 ARQ-ACK Type)
4	ARQ ACK type 2 - Cumulative with Selective ACK entry	6.3.4.2, 11.7.23	o	Y	Y	Negotiable over REG-REQ/RSP (11.7.23 ARQ-ACK Type)
5	ARQ ACK type 3 - Cumulative ACK with Block Sequence ACK	6.3.4.2, 11.7.23	o	Y	Y	Negotiable over REG-REQ/RSP (11.7.23 ARQ-ACK Type)

5.1.8 MAC support for H-ARQ

Table 94. MAC Support for HARQ

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	HARQ Support	6.3.17	o	Y	Y	All items below are conditional dependently on HARQ support.

Ite m	Description	Reference	Status	BS Required	MS Required	Comment
2.	HARQ Buffer Negotiation Capability	11.8.3.7.19	o	Y	Y	
3.	HARQ Channel mapping	6.3.17, 11.13.32	o	Y	Y	Determined by BS
4.	Capability of DL HARQ channels Number negotiation	11.8.3.7.2	o	Y	Y	
5.	Capability of UL HARQ channels Number negotiation	11.8.3.7.3	o	Y	Y	
6.	Capability of HARQ ACK delay negotiation in DL transmission	11.4.1	o	Y	Y	
7.	Capability of HARQ ACK delay negotiation in UL transmission	11.3.1	o	Y	Y	
8.	PDU SN extended subheader for HARQ reordering	11.13.33	o	Y	Y	

5.1.9 QoS

Table 95. QoS

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Dynamic service flow creation - BS-initiated	6.3.14.7.1.2	m	Y	Y	
2	Dynamic service flow creation -SS-initiated	6.3.14.7.1.1	o	Y	Y	
3	Dynamic service flow change - BS-initiated	6.3.14.9.4.2	m	Y	Y	
4	Dynamic service flow change -SS-initiated	6.3.14.9.4.1	o	Y	Y	
5	Dynamic service flow deletion -BS-initiated	6.3.14.9.5.2	m	Y	Y	
6	Dynamic service flow deletion – SS-initiated	6.3.14.9.5.1	o	Y	Y	

5.1.10 Data delivery services for mobile network

Table 96. Data Delivery Services for Mobile Network

Item	Description	Reference	Status	BS Required	MS Required	Comment
1	Unsolicited Grant service (UGS)	6.3.20.1.1, 6.3.5.2.1	o	Y	Y	
2	Real-Time Variable Rate (RT-VR) Service	6.3.20.1.2, 6.3.5.2.2	o	Y	Y	
3	Non-Real-Time Variable Rate (NRT-VR) Service	6.3.20.1.3, 6.3.5.2.3	o	Y	Y	
4	Best Effort (BE) Service	6.3.20.1.4, 6.3.5.2.4	o	Y	Y	
5	Extended Real-Time Variable Rate (ERT-VR) service	6.3.20.1.5, 6.3.5.2.2.1	o	Y	Y	

5.1.11 Request-Grant mechanism

Table 97. Request-Grant Mechanism

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Incremental bandwidth request using BW request header	6.3.6.1	o	Y	Y	
2.	Aggregate bandwidth request using BW request header	6.3.6.1	pm	Y	Y	[2] mistakenly does not request periodically to transmit aggregate bandwidth requests
3.	Bandwidth request using Grant Management Subheader	6.3.2.2.2	o	Y	Y	
4.	Multicast Polling Assignment Request / response	6.3.2.3.18-19	o	N	N	
5.	Request-Grant mechanism combined with CINR report	6.3.2.1.2.1.3	o	N	N	
6.	Request-Grant mechanism combined with UL Tx power report	6.3.2.1.2.1.2	o	Y	Y	

7.	CQICH allocation request using CQICH allocation request header	6.3.2.1.2.1.4	o	Y	Y	

5.1.12 Neighbor Advertisement

Table 98. Neighbor Advertisement

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Neighbor Advertisement	6.3.2.3.47	o	Y	Y	All items below are conditional dependently on Neighbor Advertisement implementation
2.	Support BS index at the BS (Use BS index instead of BSID) in Scan/HO related messages, as numbered in MOB_NBR-ADV	6.3.2.3.48-51, 6.3.2.3.53	o	Y	N/A	Applicable to MOB_SCN-REQ/RSP, MOB_SCAN-REPORT, MOB_xxHO-REQ/RSP BS may decide not to use the index
3.	Support BS index at the MS (Use BS index instead of BSID) in Scan/HO related messages, as numbered in MOB_NBR-ADV	6.3.2.3.48-51, 6.3.2.3.53	pm	N/A	Y	Applicable to MOB_SCN-REQ/RSP, MOB_SCAN-REPORT, MOB_xxHO-REQ/RSPas BS may decide to use the index while MS has to support it.

5.1.13 Scanning and Association

5.1.13.1 *Scanning*

Table 99. Scanning

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Scanning for cell selection (HO)	6.3.2.3.48-49	o	Y	Y	

2.	MS Requests Scanning Interval Allocations from BS	6.3.2.3.48-49 6.3.21.1.2	o	Y	Y	BS shall respond to MOB_SCN-REQ message from mobile.
3.	Unsolicited Scanning Interval Allocation by BS	6.3.2.3.48-49, 6.3.21.1.2	o	Y	Y	
4.	Event Triggered Scanning based on serving BS metrics	6.3.21.1.2	o	Y	Y	
5.	MS autonomous neighbor cell scanning	8.4.13.1.3	o	N/A	Y	

5.1.13.2 *Scan Reporting Type Support*

Table 100. Scan Reporting Type Support

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Periodic reporting as indicated in MOB_SCN-RSP message	6.3.2.3.49, 11.4.1	o	Y	Y	
2.	Event triggered reporting based on metric conditions	6.3.2.3.49, 11.4.1	o	Y	Y	

5.1.13.3 *Association*

Table 101. Association

Item	Description	Reference	Status	BS Required	MS Required	Comment

1.	Support for association during scanning	6.3.21.1.3, 6.3.2.3.51	o	N	N	It is recommended to implement the following capabilities for MS: When switching to a different Frequency Assignment, the MS should be capable of independently (without ranging) perform timing, power, and frequency adjustments based on both downlink reception quality ("open loop ranging") and information in the DCD/UCD of the target BS.
2.	Support "Ranging Parameters Validity Time" Indication (by MS)	11.20	o	N	N	

5.1.13.4 *Association Type Support*

Table 102. Association Type Support

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Uncoordinated Association (Level 0)	6.3.21.1.3.1 and 11.8.8	o	N	N	Conditioned on the support of association
2.	Coordinated Association (level 1)	6.3.21.1.3.2 and 11.8.8	o	N	N	Conditioned on the support of association
3.	NW Assisted Association Reporting (level 2)	6.3.21.1.3.3 and 11.8.8	o	N	N	Conditioned on the support of association This feature includes Reporting of Association Result.

4.	Directed Association	6.3.21.1.3, 11.8.8	o	N	N	Conditioned on the support of association

5.1.13.5 *HO/Scan/Report Trigger Metrics*

Table 103. HO/Scan/Report Trigger Metrics

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Mean BS CINR	6.3.2.3.53, 11.8.7	o	Y	Y	Conditioned by HO and Scanning support.
2.	Mean BS RSSI	6.3.2.3.53, 11.8.7	o	Y	Y	Conditioned by HO and Scanning support
3.	Relative Rx Delay	6.3.2.3.53, 11.8.7	o	N	N	Conditioned by HO and Scanning support .
4.	BS Round Trip Delay	6.3.2.3.53, 11.8.7	o	Y	Y	Conditioned by HO and Scanning support

5.1.14 MAC layer HO procedures

Table 104. MAC Layer HO Procedures

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	General HO Support	6.3.21.2, 6.3.2.3.55	o	Y	Y	Following items are conditioned by this item
2.	HO initiated by MS support at MS side		oi	N/A	Y	
3.	HO initiated by MS support at BS side		pm	Y	N/A	
4.	HO initiated by BS support at MS side ,		oi	N/A	Y	
5.	HO initiated by BS support at BS side	6.3.21.2.2	o	Y	N/A	
6.	HO Indication	6.3.21.2.5	o	Y	Y	
7.	Cancellation of HO	6.3.21.2.3	o	Y	Y	Conditioned by support of HO Indication
8.	Metric Triggered HO Requests	11.1.7 (Table 348g)	o	Y	Y	

9.	Resource Retention Support	6.3.2.3.52, 6.3.2.3.54	o	Y	Y	
10.	CDMA HO Ranging	6.3.10.3.3	o	Y	Y	
11.	HO_ID support	6.3.2.3.52, 6.3.2.3.54	o	Y	Y	
12.	Support negotiating of "HO authorization policy" during HO (i.e. between BSs)	6.3.2.3.52, 6.3.2.3.54	o	Y	Y	Using MOB_BSHO-REQ/RSP Does not request support of specific policy, just capability of negotiating.

5.1.15 HO Optimization

Table 105. HO Optimization

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	HO Optimization Support	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	1. HO Optimization requires network support 2. All further features are conditioned by this item
2.	Support Omission of SBC-REQ management messages	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
3.	Support Omission of PKM Authentication phase except TEK Phase	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
4.	Support Omission of PKM TEK creation phase during re-entry processing	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
5.	Support of Network Address Acquisition at secondary management connection	6.3.2.3.6, 6.3.21.2.7, 11.6	o	N	N	Meaningful only for managed MS.
6.	Support of Time of Day Acquisition at secondary management connection	6.3.2.3.6, 6.3.21.2.7, 11.6	o	N	N	Meaningful only for managed MS.

Item	Description	Reference	Status	BS Required	MS Required	Comment
7.	Support of TFTP Phase at secondary management connection	6.3.2.3.6, 6.3.21.2.7, 11.6	o	N	N	Meaningful only for managed MS.
8.	Support "Full State Sharing" – No exchange of network re-entry messages after ranging before resuming normal operations	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
9.	Notifying MS of DL data Pending	6.3.2.3.6, 6.3.21.2.7, 11.6	o	N	N	
10.	Unsolicited SBC-RSP management message with updated capabilities information	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
11.	Unsolicited SBC- RSP message in same frame as RNG-RSP	6.3.2.3.6, 6.3.21.2.7	o	N	N	
12.	Support SBC- RSP TLVs as part of RNG-RSP message	11.6	o	Y	Y	
13.	Support Omission of REG-REQ during NW reentry	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
14.	Unsolicited REG-RSP with updated capabilities information	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	
15.	Unsolicited REG-RSP in same frame as RNG-RSP message	6.3.2.3.6, 6.3.21.2.7	o	N	N	
16.	Support REG-RSP TLV as part of RNG-RSP message	11.6	o	Y	Y	
17.	Support of ARQ continuation using SN report header after NW re-entry	6.3.2.3.6, 6.3.21.2.7, 11.6	o	Y	Y	Requires support of SDU SN extended subheader and SN_REPORT header

Item	Description	Reference	Status	BS Required	MS Required	Comment
18.	Support continuation of non-ARQ connection using SDU SN extended sub-header before handover and using SN report header after NW re-entry			Y	Y	
19.	OFDMA Fast Ranging IE	8.4.5.4.21 6.3.21.2.4	o	Y	Y	
20.	Support sending Bandwidth Request header with zero BR as a notification of MS's successful re-entry registration	6.3.21.2.7, 11.6	o	Y	Y	
21.	Support sending at BS and receiving at MS traffic IP address refresh bit	11.6	o	Y	Y	

5.1.16 CID and SAID Update

CID update encodings (11.7.9) and SAID update encodings (11.7.18) may be used in RNG-RSP for reestablishment of connections.

Table 106. CID and SAID Update

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	CID update from BS by RNG-RSP	11.7.9, 11.6	o	Y	N/A	
2.	CID update in MS by RNG-RSP	11.7.9	pm	N/A	Y	
3.	CID update from BS by REG-RSP	11.7.9	o	Y	N/A	
4.	CID update in MS by REG-RSP	11.7.9	pm	N/A	Y	
5.	Compressed CID update from BS by RNG-RSP	11.7.9.1	o	Y	N/A	
6.	Compressed CID update in MS by RNG-RSP	11.7.9.1	pm	N/A	Y	

7.	Compressed CID update from BS by REG-RSP	11.7.9.1	o	Y	N/A	
8.	Compressed CID update in MS by REG-RSP	11.7.9.1	pm	N/A	Y	
9.	SAID update from BS by RNG-RSP	11.7.17, 11.6	o	Y	N/A	
10.	SAID update in MS by RNG-RSP	11.7.17, 11.6	pm	N/A	Y	
11.	SAID update from BS by REG-RSP	11.7.17, 11.6	o	N	N/A	
12.	SAID update in MS by REG-RSP	11.7.17, 11.6	pm	N/A	N	
13.	SAID update from BS by SA-TEK-RSP	11.7.20	o	Y	N/A	
14.	SAID update in MS by SA-TEK_RSP	11.7.20	o	N/A	Y	

5.1.17 Fast BS Switching

Table 107. Fast Base Station Switching

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	General FBSS capability	6.3.21.3.2-4	o	N	N	All further features in the table are conditioned by this item
2.	Diversity set Update initiated by MS	6.3.21.3.3	oi	N	N	If FBSS supported, Diversity set update is mandatory
3.	Diversity set Update initiated by BS	6.3.21.3.3	oi	N	N	
4.	Anchor BS Update using HO messages	6.3.21.3.4	oi	N	N	MS and BS supporting MDHO or FBSS shall implement at least one of the two mechanisms to perform Anchor BS update.
5.	Anchor BS Update using fast feedback channel	6.3.21.3.4	oi	N	N	
6.	MS implementation of Fast feedback channel pre-allocated by MOB_BSHO-RSP or MOB_BSHO-REQ	6.3.21.3.4.2	pm	N	N	Fast-feedback channel shall be allocated by one of the following three methods, if fast-feedback channel is supported.

Item	Description	Reference	Status	BS Required	MS Required	Comment
7.	BS implementation of Fast feedback channel pre-allocated by MOB_BSHO-RSP or MOB_BSHO-REQ	6.3.21.3.4.2	oi	N	N	
8.	MS implementation of Fast feedback channel allocation by Anchor_Switch_IE	6.3.21.3.4.2	pm	N	N	
9.	BS implementation of Fast feedback channel allocation by Anchor_Switch_IE	6.3.21.3.4.2	oi	N	N	
10.	MS implementation of Fast feedback channel allocation by UL_MAP of new Anchor BS	6.3.21.3.4.2	pm	N	N	
11.	BS implementation of Fast feedback channel allocation by UL_MAP of new Anchor BS	6.3.21.3.4.2	oi	N	N	
12.	Monitoring of multiple MAPs from active BSs	11.7.11	o	N	N	
13.	MS assisted coordination of DL transmission using SN report	6.3.21.3.5	o	N	N	
14.	Cancellation of Diversity set update by MOB_HO-IND	6.3.21.3.3	o	N	N	
15.	Rejection of Diversity set update by MOB_HO-IND	6.3.21.3.3	o	N	N	
16.	SN report header	6.3.2.1.6	o	N	N	Conditional, dependent on SN feedback support
17.	SDU SN extended subheader	6.3.2.2.7.1	o	N	N	Conditional, dependent on SN feedback support

Item	Description	Reference	Status	BS Required	MS Required	Comment
18.	SN request extended subheader	6.3.2.2.7.7	o	N	N	
19.	SN feedback support	11.13.28	o	N	N	No text on optionality in standard, but it is negotiated on a per-connection basis in DS(A/C)-REQ and disabled by default. So it is effectively optional.
20.	MS autonomous neighbor cell scanning	8.4.13.1.3	m	N	N	This feature is conditioned by implementation of FBSS or MDHO.

5.1.18 Macro Diversity Handover

Table 108. Macro Diversity Handover

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	General MDHO capability	6.3.21.3.1, 6.3.21.3.3-4	o	N	N	Status for all following features is conditional, based on implementation of MDHO capability. Network support may be required to support this feature.
2.	Diversity set Update initiated by MS	6.3.21.3.3	oi	N	N	If MDHO supported, Diversity set update is mandatory.
3.	Diversity set Update initiated by BS	6.3.21.3.3	oi	N	N	If MDHO supported, Diversity set update is mandatory.
4.	Anchor BS Update using HO messages	6.3.21.3.4	oi	N	N	If MDHO supported, at least one of the items 4 and 5 shall be implemented.
5.	Anchor BS Update using fast feedback channel	6.3.21.3.4.2	oi	N	N	If MDHO supported, at least one of the items 4 and 5 shall be implemented.

Item	Description	Reference	Status	BS Required	MS Required	Comment
6.	MOB_BSHO-RSP for acknowledgement for Diversity set update request from MS	6.3.21.3.1	m	N	N	
7.	MDHO DL soft Combining supported with monitoring single MAP from anchor BS	8.4.5.3.14 8.4.5.3.15 8.4.5.4.18 8.4.5.4.19 11.7.11	o	N	N	
8.	MDHO DL RF Combining supported with monitoring MAPs from all active BS	8.4.5.3.14 8.4.5.3.15 8.4.5.4.18 8.4.5.4.19 11.7.11	o	N	N	
9.	MDHO DL soft combining supported with monitoring MAPs from all active BS	8.4.5.3.14 8.4.5.3.15 8.4.5.4.18 8.4.5.4.19 11.7.11	o	N	N	
10.	Recommended BS list in MOB_MSHO-REQ	6.3.21.3.3	po	N	N	MS may provide a list, but BS is not obligated to follow the list.
11.	Recommended BS list in MOB_BSHO-RSP	6.3.21.3.3	po	N	N	BS may provide a list ("the BSs may provide a recommended list of BSs to be included in the MS' Diversity set."), but MS is not obligated to follow the list.
12.	MS implementation of Fast feedback channel pre-allocated at the new Anchor BS by MOB_BSHO-RSP or MOB_BSHO-REQ when a BS is added to the Diversity set	6.3.21.3.4.2	pm	N	N	At least one of the following three methods of fast-feedback channel allocation shall be implemented, if fast-feedback channel is supported.

Item	Description	Reference	Status	BS Required	MS Required	Comment
13.	BS implementation of Fast feedback channel pre-allocated at the new Anchor BS by MOB_BSHO-RSP or MOB_BSHO-REQ when a BS is added to the Diversity set	6.3.21.3.4.2	oi	N	N	
14.	MS implementation of Fast feedback channel allocation by Anchor_Switch_IE	6.3.21.3.4.2	pm	N	N	
15.	BS implementation of Fast feedback channel allocation by Anchor_Switch_IE	6.3.21.3.4.2	oi	N	N	
16.	MS implementation of Fast feedback channel allocation by UL_MAP of new Anchor BS	6.3.21.3.4.2	pm	N	N	
17.	BS implementation of Fast feedback channel allocation by UL_MAP of new Anchor BS	6.3.21.3.4.2	oi	N	N	
18.	UL transmission to multiple BS	11.7.11	o	N	N	
19.	MS autonomous neighbor cell scanning	8.4.13.1.3	m	N	N	This feature is conditioned by implementation of FBSS or MDHO.

5.1.19 Sleep Mode

Table 109. Sleep Mode

Item	Description	Reference	Status	BS Required	MS Required	Comment

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Sleep Mode Implementation in MS	6.3.20.2	o	N/A	Y	For MS, all items below are conditional based on Sleep Mode implementation
2.	Power Saving Class type 1 support	6.3.20.2	o	Y	Y	
3.	Support of Traffic Indication Message for Power Saving Class type 1	6.3.20.2	o	Y	Y	Status of following items related to SLPID is conditional, depends on support of TRF-IND. Three alternative ways to wake an MS are 1) to use SLP-RSP message, and 2) to use downlink sleep control extended sub-header.
4.	Indicating DL traffic by SLPID bit map in TRF-IND	6.3.20.1	oi	Y	Y	One of the items 4 or 5 shall be implemented. BS may just not use SLPID. BS must support either this or Short Basic CID
5.	Indicating DL traffic by SLPID in TRF-IND	6.3.20.1	oi	Y	Y	BS must support either this or SLPID
6.	Support of SLPID at the MS including SLPID_Update TLV in TRF-IND	6.3.20.1	pm	N/A	Y	MS has no way to signal it does not support SLPID
7.	Support of SLPID_Update TLV at BS in TRF-IND	6.3.20.1	o	Y	N/A	
8.	Traffic triggered wakening flag	6.3.2.3.44-45, 6.3.20.2	m (MS) and o (BS)	Y	Y	
9.	Power Saving Class type 2 support	6.3.20.3	o	N	N	
10.	Power Saving Class type 3 support	6.3.20.4	o	N	N	
11.	Activation of Power Saving Class by unsolicited SLP-RSP message from BS	6.3.20.1	o	Y	Y	

Item	Description	Reference	Status	BS Required	MS Required	Comment
12.	Activation of Power Saving Class by RNG-RSP message (type 3 only)	6.3.20.4	o	N	N	
13.	Activation of Power Saving Class by RNG-REQ message with Power_Saving_Class_Parameters TLV	6.3.2.3.5	o	N	N	
14.	DL sleep control extended subheader	6.3.2.2.7.2	o	Y	Y	
15.	Bandwidth request and uplink sleep control header	6.3.2.1.5	o	Y	Y	
16.	Support of periodic ranging in sleep mode	6.3.20.5	pm	Y	Y	
17.	DL Traffic indication by RNG-RSP message	6.3.20.5	o	N	N	
18.	MDHO/FBSS diversity set maintenance during sleep mode at MS	6.3.20.6	m	N/A	N	Conditioned by support of MDHO/FBSS
19.	MDHO/FBSS diversity set maintenance during sleep mode at BS	6.3.20.6	m	N	N/A	Conditioned by support of FBSS/MDHO.
20.	Sleep mode multicast CID support at MS	10.4	m	N/A	Y	MS has to support it as BS can use it.
21.	Sleep mode multicast CID support at BS	10.4	o	Y	N/A	
22.	MS Support of triggered action indicated by Enabled-Action-Triggered TLV	6.3.20.1, 11.5, 11.6, 11.7.3	o	N/A	Y	
23.	BS Support of triggered action indicated by Enabled-Action-Triggered TLV	6.3.20.1, 11.5, 11.6, 11.7.3	o	Y	N/A	If MS transmits the TLV, BS has to respond to it.

5.1.20 Idle Mode

Table 110. Idle Mode

Item	Description	Reference	Status	BS Required	MS Required	Comment

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	General Idle Mode functionality	6.3.24	o	Y	Y	All items below are conditional based on Idle Mode implementation
2.	Idle mode initiation by DREG-REQ message from MS	6.3.24.1	oi	Y	Y	One of two Idle mode initiation methods is mandatory.
3.	Idle Mode initiation by unsolicited DREG-CMD from BS	6.3.24.1	oi	Y	Y	
4.	Maintain connection information at BS during Idle Mode initiation process	6.3.24.1	m	Y	Y	
5.	Request for MS to retain service and operational information by DREG-CMD message	6.3.24.1	m	Y	Y	
6.	Request from MS to BS to retain service and operational information by DREG-REQ message	6.3.24.1	m	Y	Y	Mandatory feature see 6.3.2.3.42;
7.	Implementation in MS of the reception of periodic transmission of MS MAC address hash in Paging message	6.3.24.1	m	N/A	N	See 6.3.2.3.5-6. The MS may request BS inclusion of MS MAC Address Hash in MOB_PAG-ADV message at regular intervals, regardless of need for notification
8.	Implementation in BS of Periodic transmission of MS MAC address hash in Paging message for a idle MS	6.3.24.1	o	N	N/A	
9.	BS capability of transmitting Broadcast Control Pointer IE	6.3.24.5	o	Y	N/A	
10.	MS capability of receiving Broadcast Control Pointer IE	6.3.24.5	m	N/A	Y	

Item	Description	Reference	Status	BS Required	MS Required	Comment
11.	BS Capability of providing dedicated ranging region and ranging code allocation for location update or network entry of MS in Idle Mode 6.3.22.8.1	6.3.24.8.1	o	N	N/A	
12.	MS Capability of using dedicated ranging region and ranging code allocation for location update or network entry of MS in Idle Mode	6.3.24.8.1	m	N/A	Y	
13.	Paging Group Update at MS	6.3.24.9.1.1	m	Y	Y	
14.	Timer Location Update at MS	6.3.24.9.1.2	m	Y	Y	
15.	Power Down Location Update at MS	6.3.24.9.1.3	m	Y	Y	
16.	MAC Hash Skip Threshold Location Update at MS	6.3.24.9.1.4	m	N/A	N	This is mandatory under the condition that MAC Hash Skip Threshold option is implemented in the MS. This item is conditioned by Item 7 of this table.
17.	Secure Location Update	6.3.24.9.2.1	o	Y	Y	
18.	Un-secure Location Update	6.3.24.9.2.2	m	Y	Y	
19.	Paging Preference	11.13.27	pm	Y	Y	
20.	Idle mode multicast CID support at MS	10.4	m	N/A	Y	MS has to support it as BS can use it.
21.	Idle mode multicast CID support at BS	10.4	o	Y	N/A	

5.1.21 Expedited Network Re-entry from Idle Mode

Table 111. Expedited Network Re-entry from Idle Mode

Item	Description	Reference	Status	BS Required	MS Required	Comment

Item	Description	Reference	Status	BS Required	MS Required	Comment
1.	Expedited network re-entry from Idle Mode support	6.3.23.9	o	Y	Y	
2.	Support Omission of SBC-REQ management messages	11.6	o	Y	Y	
3.	Support Omission of PKM Authentication phase except TEK phase	11.6	o	Y	Y	
4.	Support Omission of PKM TEK creation phase during re-entry processing	11.6	o	Y	Y	
5.	Support of Network Address Acquisition at secondary management connection	11.6	o	N	N	
6.	Support of Time of Day Acquisition at secondary management connection	11.6	o	N	N	
7.	Support TFTP Phase at secondary management connection	11.6	o	N	N	
8.	Support "Full State Sharing" - No exchange of network re-entry messages after ranging before resuming normal operations	11.6	o	Y	Y	
9.	Notifying MS of DL data pending	11.6	o	N	N	Not relevant to idle mode.
10.	Unsolicited SBC-RSP management message with updated capabilities information	11.6	o	Y	Y	
11.	Unsolicited SBC-RSP message in same frame as RNG-RSP	11.6	o	N	N	

Item	Description	Reference	Status	BS Required	MS Required	Comment
12.	Support SBC-RSP TLVs as part of RNG-RSP message	11.6	o	Y	Y	
13.	Support Omission of REG-REQ during NW re-entry	11.6	o	Y	Y	
14.	Unsolicited REG-RSP with updated capabilities information	11.6	o	Y	Y	
15.	Unsolicited REG-RSP in same frame as RNG-RSP message	11.6	o	N	N	
16.	Support REG-RSP TLV as part of RNG-RSP message	11.6	o	Y	Y	
17.	MS send Bandwidth Request header with zero BR as a notification of MS's successful re-entry registration.	11.6	o	Y	Y	
18.	MS trigger a higher layer protocol required to refresh its traffic IP address (e.g. DHCP Discover [IETF RFC 2131] or Mobile IPv4 re-registration [IETF RFC 3344]).	11.6	o	Y	Y	

5.1.22 Security

5.1.22.1 *Authorization Policy Support*

Table 112. Authorization Policy Support

Item	Feature	Reference	Status	BS Required	MS Required	Comments
1	802.16 Authorization policy support	11.7.8.7	o	Y	Y	

5.1.22.2 *PKM Version Support*

Table 113. PKM Version Support

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	PKMv1 Support	11.8.4.1	o	N	N	
2.	PKMv2 Support	11.8.4.1	o	Y	Y	

5.1.22.3 *PKMv2 Authorization policy support – initial network entry*

Table 114. PKMv2 Authorization Policy Support-Initial Network Entry

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No Authorization	11.8.4.2	o	Y	Y	
2.	EAP-based authorization	11.8.4.2	o	Y	Y	
3.	EAP-based authorization and Authenticated (EIK) EAP-based authorization	11.8.4.2	o	N	N	
4.	RSA-based authorization	11.8.4.2	o	N	N	
5.	RSA-based authorization and Authenticated (EIK) EAP-based authorization	11.8.4.2	o	N	N	
6.	RSA-based authorization and EAP-based authorization	11.8.4.2	o	N	N	

5.1.22.4 *PKMv2 Authorization policy support – network re-entry*

Table 115. PKMv2 Authorization Policy Support-Network Re-entry

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No Authorization	11.8.4.2	o	Y	Y	
2.	EAP-based authorization	11.8.4.2	o	Y	Y	

3.	EAP-based authorization and Authenticated (EIK) EAP-based authorization	11.8.4.2	o	N/A	N/A	
4.	RSA-based authorization	11.8.4.2	o	N/A	N/A	
5.	RSA-based authorization and Authenticated (EIK) EAP-based authorization	11.8.4.2	o	N/A	N/A	
6.	RSA-based authorization and EAP-based authorization	11.8.4.2	o	N/A	N/A	

5.1.22.5 *Supported cryptographic suites*

"Cryptographic suites" includes Data encryption, Data authentication, TEK encryption algorithm.

Table 116. Supported Cryptographic Suites

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No data encryption, no data authentication & 3-DES, 128	11.9.14	o	Y	Y	This cryptographic suite means no encryption and no TEK exchange.
2.	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128	11.9.14	o	N	N	
3.	No data encryption, no data authentication & RSA, 1024	11.9.14	o	N	N	
4.	CBC-Mode 56-bit DES, no data authentication & RSA, 1024	11.9.14	o	N	N	
5.	CCM-Mode 128-bit AES, CCM-Mode, 128-bit, ECB mode AES with 128-bit key	11.9.14	o	N	N	
6.	CCM-Mode 128-bit AES, CCM-Mode, AES Key Wrap with 128-bit key	11.9.14	o	Y	Y	

Item	Description	Reference	Status	BS Required	MS Required	Comments
7.	CBC-Mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key	11.9.14	o	N	N	
8.	MBS CTR Mode 128 bits AES, no data authentication, AES ECB mode with 128-bit key	11.9.14	o	N	N	
9.	MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key	11.9.14	o	N	N	

5.1.22.6 *Message Authentication Code Mode*

Table 117. Message Authentication Code Mode

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No message authentication	11.8.4.3	o	Y	Y	
2.	HMAC	11.8.4.3	o	N	N	
3.	CMAC	11.8.4.3	o	Y	Y	
4.	64-bit short-HMAC	11.8.4.3	o	N	N	
5.	80-bit short-HMAC	11.8.4.3	o	N	N	
6.	96-bit short-HMAC	11.8.4.3	o	N	N	

5.1.22.7 *Security Association*

Table 118. Security Association

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	Support of Static SA	7.2.1.1	o	Y	Y	
2.	Support of Dynamic SA	7.2.1.1	o	Y	Y	
3.	Support of Primary SA	7.2.1.1	m	Y	Y	

5.1.22.8 *SA Service Type*

Table 119. SA Service Type

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	Unicast	11.9.35	o	Y	Y	
2.	Group multicast service	11.9.35	o	N	N	
3.	MBS Services	11.9.35	po	N	N	Conditioned by MBS support

5.1.22.9 *EAP Authentication methods*

Table 120. EAP Authentication Methods

Item	Description	Reference	BS Required	MS Required	Comments
1.					

5.1.22.10 *Certificate profile*

Table 121. Certificate Profile

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	X.509 MS certificate for device authorization	7.6	pm	N	N	Conditioned by usage of PKM v1 or PKM v2 with RSA authentication
2.	X.509 Manufacturer certificate	7.6	pm	N	N	Conditioned by usage of PKM v1 or PKM v2 with RSA authentication
3.	X.509 BS Cert Profile	7.6	pm	N	N	Conditioned by usage of PKM v1 or PKM v2 with RSA authentication

5.1.22.11 *Multicast Broadcast Re-keying Algorithm (MBRA)*

Table 122. Service Type

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	MBRA for Group multicast service	7.9	o	N	N	
2.	MBRA for MBS	7.9	o	N	N	

	service					

5.1.23 MBS

Table 123. MBS

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	Single-BS-MBS	6.3.13	o	N	N	
2.	Multi-BS-MBS	6.3.13	o	IO-MBS	Y	Synchronization between BSs of mapping of MBS service flow IDs to CIDs throughout MBS_ZONE.
3.	Time diversity scheme in Multi-BS-MBS	6.3.2.3.57	o	N	N	Conditioned by item 2
4.	Logical channel ID scheme in Multi-BS-MBS	6.3.2.3.57	o	N	N	Conditioned by item 2
5.	Support for MBS_MAP-IE	6.3.13.2.3	pm	IO-MBS	Y	This item depends on multi-BS MBS implementation.
6.	MS initiated MBS request using DSA-REQ	11.13.20	oi	IO-MBS	Y	At least one is required. Dependent on MBS implementation (either item 1 or item 2).
7.	BS initiated MBS request using DSA-REQ	11.13.20	oi	IO-MBS	Y	Dependent on MBS implementation (either item 1 or item 2).

5.1.24 AAS

Table 124. AAS

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	General AAS functionality	6.3.7.6	o	N	N	

5.1.25 MS's Network Entry issued by BS restart

Table 125. MS's Network Entry issued by BS restart

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	MS's Network Entry triggered by BS restart counter change	6.3.9.11, 11.4.1	o	Y	Y	

5.1.26 NSP Selection

Table 126. NSP Selection

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	General NSP Selection TLV Support	802.16g-D6:: 11.1.8.1-2, 11.8.9, 6.3.2.3, 6.3.2.3.63	o	Y	Y	

5.2 *Parameters*

A default, maximum and minimum should be provided for all parameters.

Table 127. Parameters

Item	Description	Reference	Status	Min	Def	Max	Comments
1.	Number of concurrent outstanding PKM exchanges SS is capable of handling at one time.			2			
2.	Number of transport security associations that SS is capable of supporting simultaneously.			2			
3.	PN window size in PNs	11.8.4.4	pm	128			Conditional, depends on support of AES in CCM mode

Item	Description	Reference	Status	Min	Def	Max	Comments
4.	UCD Transition		BS	50msec			The time the BS shall wait after transmitting a UCD message with an incremented Configuration Change Count before issuing a UL-MAP message referring to Uplink_Burst_Profiles defined in that UCD message
5.	DCD Transition		BS	50msec			The time the BS shall wait after transmitting a DCD message with an incremented Configuration Change Count before issuing a DL-MAP message referring to Downlink_Burst_Profiles defined in that DCD message
6.	Tproc		BS	Tf = Frame length			Time provided between arrival of the last bit of a UL-MAP at an SS and effectiveness of that map
7.	RNG-RSP processing time		MS			2.5 msec from the start of the frame (n+1) were frame n is the frame containing the RNG_RSP. If there is an UL allocation to the SS before the 2.5 msec in frame n+1 then the power change shall be applied before the end of the frame n+1.	Time allowed for an SS following receipt of a RNG-RSP before it is expected to apply the corrections instructed by the BS Minimum value

Item	Description	Reference	Status	Min	Def	Max	Comments
8.	Initial Ranging Interval		BS			250m	Time between Initial Ranging regions allocated by the BS
9.	Lost DL-MAP Interval		MS			600m	Time since last received DL-MAP message before downlink synchronization is considered lost
10.	Lost UL-MAP Interval		MS			600m	Time since last received UL-MAP message before uplink synchronization is considered lost
11.	T1		MS			min (20 secs , 5x DCD Interval maximum value)	Wait for DCD timeout
12.	T3		MS			60 ms: RNG-RSP after CDMA ranging or RNG-REQ during initial or periodic ranging 50 ms: RNG-RSP after RNG-REQ during HO to negotiated target BS 200 ms: RNG-RSP after RNG-REQ during HO to non-negotiated target BS 200 ms: RNG-RSP after RNG-REQ during location update or re-entry from idle mode	Ranging Response reception timeout following the transmission of a Ranging Request
13.	T4		MS	5sec		35sec	Wait for unicast ranging opportunity. If the pending-until-complete field was used earlier by this SS, then the value of that field shall be added to this interval (copied from [1])

Item	Description	Reference	Status	Min	Def	Max	Comments
14.	T6		MS			1sec	Wait for registration response (copied from [1])
15.	T7		MS/BS			1s	Wait for DSA/DSC/DSD Response timeout (copied from [1])
16.	T8		MS/BS			100 msec	Wait for DSA/DSC Acknowledge timeout (copied from [1])
17.	T12		MS			min (20 sec , 5x UCD Interval maximum value)	Wait for UCD descriptor
18.	T14		MS			100msec	Wait for DSX-RVD Timeout
19.	T17		BS	5min	5min		Time allowed for SS to complete SS Authorization and Key Exchange
20.	T18		MS	50ms	50 ms	90 ms	Wait for SBC-RSP timeout
21.	T22		MS/BS			0.5 s	Wait for ARQ-Reset
22.	Idle Mode Timer		MS	128 s	4096 s	65536 s	
23.	T43		MS			100 ms	Time the MS waits for MOB_SLP-RSP
24.	T44		MS			100 ms	Time the MS waits for MOB_SCN-RSP
25.	T46		BS	50 ms		100 ms	Time the BS waits for DREG REQ in case of unsolicited Idle Mode initiation from BS
26.	T47			8 frames	64 frames	128 frames	PMC_RSP Timer: BS shall send the PMC_RSP before T47 + 1 frames after BS receives PMC_REQ (confirmation = 0) correctly.
27.	Paging Interval Length		MS/BS	1 frames	2 frames	5 frames	time duration of Paging Interval of the BS
28.	Max Dir Scan Time		MS			2 sec	Maximum scanning time of neighbor BSs by MS before reporting any results

Item	Description	Reference	Status	Min	Def	Max	Comments
29.	Maximum SDU size			1522 Bytes			Recommended value to derive Maximum Transmission Unit (MTU) from
30.	Number of transport connections in UL			4			Minimum number of concurrent transport CIDs MS is capable to support in UL.
31.	Number of transport connections in DL			4			Minimum number of concurrent transport CIDs MS is capable to support in DL.
32.	Total number of power save class instances supported from class types 1 & 2	11.8.5		1			Number of power saving class instances supported by the MS sufficient for the conformance with the profile.
33.	ARQ_RESET_MAX_RETRIES	6.3.4.6.2, Figures 34, 35			2		The default value must be supported
34.	Min required CS Types per MS		MS		1		Minimum number of simultaneously supported CS options, which is required for MS certification
35.	ARQ_RETRY_TIMEOUT on non H-ARQ connections	11.13.18.3	BS/MS	20ms		1.3s	Used in DSA-REQ and DSA-RSP to indicate the ARQ_Retry_Timeout value. 5msec granularity.
36.	ARQ_RETRY_TIMEOUT on H-ARQ connections	11.13.18.3	BS/MS			1.3s	Used in DSA-REQ and DSA-RSP to indicate the ARQ_Retry_Timeout value. 5msec granularity.
37.	ARQ_SYNC_LOSS_TIMEOUT for non H-ARQ connections	11.13.18.5	BS/MS	100ms			Used in DSA-REQ and DSA-RSP to indicate timeout for ARQ. 5msec granularity.
38.	ARQ_RX_PURGE_TIMEOUT for non H-ARQ connections	11.13.18.7	BS/MS	100ms			Used in DSA-REQ and DSA-RSP to indicate timeout for ARQ. 5msec granularity.
39.	ARQ_RX_PURGE_TIMEOUT for H-ARQ connections	11.13.18.7					Used in DSA-REQ and DSA-RSP to indicate timeout for ARQ. 5msec granularity.
40.	ARQ_BLOCK_LIFETIME granularity	11.13.18.4					5msec granularity.
41.	AI_SN value upon init and after HO (HARQ reset)	6.3.2.3.43.4	BS/MS		0		AI_SN is used in HARQ to indicate the sequence number of the ACID. Initial value at the network entry and after HO.

Item	Description	Reference	Status	Min	Def	Max	Comments
42.	Power_control_IE::Power measurement frame relevance		BS/MS			4 MS Transmission	

Table 128. Minimum Performance Requirements

Item	Description	Reference	Status	Min	Def	Max	Comments
1.	HO Parameters Processing Time	11.7.24				3 frame	Time in msec the MS needs to process information on connections provided in RNGRSP or REG-RSP message during HO

5.3 *Recommended Configuration*

Table 129. Recommended Configurations

Parameter	Value	Reference
PN window size		MS PN window size for HARQ CID
SAID supported - DL		Maximum number of SAID supported - Downlink
SAID supported - UL		Maximum number of SAID supported - Uplink
Max SDU size for IP CS		
Maximum number of power save class instances supported from class 1 & 2		
Maximum number of power save class instances supported from class 3		

6. Radio Profile

Table 130 defines the RF channels to be calculated using the following formula:

$$RFChannel_n = F_{start} + n \cdot \Delta F_c, \forall n \in N_{range}$$

Where:

F_{start} is the start frequency for the specific band,

ΔF_c is the center frequency step,

N_{range} is the range values for the n parameter

Table 130. RF Profiles List

	RF Profile Name	Channel BW (MHz)	Center Frequency Step (KHz)	F_{start} (MHz)	N_{range}	Comment
1.	Prof1.A_2.3	8.75	250	2304.5	{0, …, 364)	
2.	Prof1.B_2.3-5	5	250	2302.5	{0, …, 380)	
	Prof1.B_2.3-10	10		2305	{0, …, 360)	
3.	Prof2.A_2.305	3.5	250	2306.75 and 2346.75	{0, …, 46}	
4.	Prof2.B_2.305	5	250	2307.5 and 2347.5	{0, …, 40}	
5.	Prof2.C_2.305	10	250	2310 and 2350	{0, …, 20}	
6.	Prof3.A_2.496 – 5	5	250	2498.5	{0, …, 756}	200 KHz Frequency step is considered for Europe 2.5 GHz extension.
	Prof3.A_2.496 – 10	10		2501	{0, …, 736}	200 KHz Frequency step is considered for Europe 2.5 GHz extension.
7.	Prof4.A_3.3	5	250	3302.5	{0, …, 380)	
8.	Prof4.B_3.3	7	250	3303.5	{0, …, 372)	
9.	Prof4.C_3.3	10	250	3305	{0, …, 360)	
10.	Prof5.A_3.4	5	250	3402.5	{0, …, 1580)	
	Prof5L.A_3.4				{0, …, 780)	
	Prof5H.A_3.4				{800, …, 1580)	
11.	Prof5.B_3.4	7	250	3403.5	{0, …, 1572)	
	Prof5L.B_3.4				{0, …, 772)	
	Prof5H.B_3.4				{800, …, 1572)	
12.	Prof5.C_3.4	10	250	3405	{0, …, 1560)	
	Prof5L.C_3.4				{0, …, 860)	
	Prof5H.C_3.4				{800, …, 1560)	

Note that comprehensive RF raster of Table Table 130 is only for interoperability purposes and not a basis for any performance testing on RF channel scanning and synchronization to network. RF preferred sets are needed to be developed to be considered as basis for scanning time performance requirements.

7. Power Class Profile

The Power Classes listed in following table is developed to cover the complete target range of power levels while different interpretation of applicable modulation levels is addressed through a dual range requirement for QPSK and 16-QAM per Power Class.

Table 131. Power Classes

Class Identifier	Transmit Power (dBm) for 16-QAM	Transmit Power (dBm) for QPSK	MS Required
Power Class 1	18 <= PTx,max < 21	20 <= PTx,max < 23	oi
Power Class 2	21 <= PTx,max < 25	23 <= PTx,max < 27	oi
Power Class 3	25 <= PTx,max < 30	27 <= PTx,max < 30	oi
Power Class 4	30 <= PTx,max	30 <= PTx,max	oi

Attachment 4-1

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[Stage 2 and Stage 3 Abbreviations]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Stage 2 and Stage 3 Abbreviations]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

1. Abbreviations/Acronyms, Definitions, and Conventions

1.1 Abbreviations/Acronyms

The following table lists several abbreviations and acronyms used throughout NWG Stage 2 and Stage 3 documents.

Abbreviation	Expansion of Abbreviation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AA	Anchor Authenticator also called Network Authenticator Server (NAS)
AAA	Authentication, Authorization, and Accounting
AAA Proxy	An intermediary for transparently routing and/or processing AAA messages sent between a AAA client and a AAA server
AAA Server	Computer system performing AAA services (authentication, authorization, accounting)
AAA-V	AAA proxy server located within the visited network
AASN	Anchor ASN. Refers to the ASN that holds the Anchor Data Path Functions for a given MS
AC	Admission Control
ADPF	Anchor Data Path Function
AF	Application Function
AK	Authorization Key
AKA	Authentiction and Key Agreement
AK SN	- Derivation from PMK and PMK2 SN
AM	Authorization Module
APC	Anchor paging Controller
APCF	Anchor paging controller function
API	Application Program Interface
AR	Access Router
ARQ	Automatic Retransmission Request
AS	Authentication Server
ASN	Access Service Network
ASP	Application Service Provider
BCE	Binding Cache Entry
BE	Best Effort
BRAS	Broadband Remote Access Server
BS	Base Station
BSID	Base Station Identifier
BU	Binding Update
CAC	Connection Admission Control
CCoA	Collocated Care of Address
CDMA2000	3rd Generation Code Division Multiple Access Radio Technology
CID	Connection IDentifier
CMAC	Cipher-based Message Authentication Code
CMIP	Client Mobile IP

Abbreviation	Expansion of Abbreviation
COA	Change of Authority
CoA	Care of Address
COS	Class of Service
CS	Convergence Sublayer
CSN	Connectivity Service Network
CUI	Chargeable User Identity
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DL	Down Link
diffserv	Differentiated services
DNS	Domain Name Service
DoS	Denial of Service
DP	Decision Point Data Path
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Link Access Multiplexer
E2E	End-to-End
E911	US Emergency Services
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement to be used with USIM
EAP-MD5	Extensible Authentication Protocol - Message Digest 5
EAP-MSCHAPv2	EAP Microsoft Challenge Handshake Authentication Protocol version 2
EAP-PSK	Extensible Authentication Protocol - Pre Shared Key
EAP-SIM	EAP Subscriber Identity Module to be used with SIM
EAP-TLS	EAP with TLS
EMSK	Extended Master Session Key
ertPS	Extended Real-Time Polling Service
EUI-64	Extended Unique Identifier (64-bit)
FA	Foreign Agent
FBSS	Fast Base Station Switching
FCAPS	Fault Configuration Accounting Performance and Security
FQDN	Fully Qualified Domain Name
FRD	Fast Router Discovery
FWA	fixed wireless access
GPRS	General Packet Radio Services
GRE	Generic Routing Encapsulation
GSA	Group Security Association
GSM	Global System for Mobile communication
GW	Gateway
HA	Home Agent
HLA	Hot-Line Application

Abbreviation	Expansion of Abbreviation
	Hot-Lining Application
HLD	Hot-Line Device Hot-lining Device
HMAC	Keyed-Hashing for Message Authentication Code
HO	Handoff
HO ID	Handoff Identifier
HoA	MS Home Address
Hotspot	Public location such as an airport or hotel where WLAN services have been deployed
HSDPA	High Speed Downlink Packet Access
HTTP	HyperText Transfer Protocol
I-WLAN	Interworking with Wireless LANs
IANA	Internet Assigned Numbers Authority
IBS	Integrated Base Stations. Refers to a BS that can instantiate all the ASN functions for a given MS. Such an Integrated BS can also be labeled a Profile B ASN
ICMPv6	Internet Control Message Protocol for (IPv6) Specification [RFC 2463]
IE	information elements
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.3	IEEE standard specification for Ethernet
IETF	Internet Engineering Task Force
IID	Interface Identifier
IK	Integrity Key
IKEv2	Internet Key Exchange protocol version 2
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISF	Initial Service flow
IWF	Internetworking Function
IWG	Inter-working Gateway
IWU	Internetworking Unit
LBS	Location Based Services
LE	License-Exempt deployments
LPF	Local Policy Function
LR	Location Register MSID, BSID
LSB	Least Significant Byte
MAC	Medium Access Control
MBMS	Multimedia Broadcast/Multicast Service
MCC	Mobile Country Code
MDHO	Macro Diversity handoff
MIP	Mobile IP (Refers to both Mobile IPv4 and Mobile IPv6)

Abbreviation	Expansion of Abbreviation
MIP6	Mobile IP version 6
MM	Mobility Management
MMS	Multimedia Messaging Service
MNC	Mobile Network operator Code
MN_HOA	Allow-MN-HA=Assignment
MPLS	Multi Protocol Label Switching
MS	Mobile Station
MSID	Mobile Station Identifier
MSK	Master Session Key
NA	Neighbor Advertisements
NAI	Network Access Identifier
NAP	Network Access Provider
NAPT	Network Address Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NMS	Network Management System
NRM	Network Reference Model
nrtPS	Non-real-time Polling Service
NS	Neighbor Solicitation
NSP	Network Service Provider
NUD	Neighbor Unreachability Detection
OAM	Operations and Maintenance
OTA	Over-The-Air
OUI	Organization Unique Identifier
P-CSCF	Proxy-Call Session Control Function
PA	Paging Agent
PC	Paging Controller
PDFID	packet data flow ID
PDG	Packet Data Gateway
PDU	Packet Data Unit
PEAP	Protected EAP
PF	Policy Function
PG	Paging Group
PG ID	Paging Group Identifier
PHS	Packet header suppression (PHS)
PKM	Privacy Key Management
PMIP	Proxy-Mobile IP
PMK	Pairwise Master Key
PMK2	Pairwise Master Key
PMN	Proxy Mobile Node
PoA	Point of Attachment
PPAC	prepaid accounting capability

Abbreviation	Expansion of Abbreviation
PPC	Prepaid Client
PPS	Prepaid Server
Proxy-ARP	Proxy Address Resolution Protocol
PSK	PreShared Key
PSTN	Public Switched Telephone Network
PtP	Peer to Peer
QoS	Quality of Service
RADIUS	Remote Access Dial In User Service
RA	Router Advertisement
RO	route optimization
RR	Resource-Reservation
RP	Reference Point
RRA	Radio Resource Agent
RRC	Radio Resource Controller
RRM	Radio Resource Management
RS	Router Solicitation
RSVP	Resource Reservation Protocol
rtPS	Real-time Polling Service
RUIM	Removable User Identity Module
SA	Security Association
SAE	system architecture evolution
SCI	Spare capacity indicator
S-CSCF	Serving-Call Session Control Function
SDFID	service data flow ID
SDU	Service Data Unit
SFA	Service Flow Authorization
SFID	Service Flow ID
SFM	Service Flow Management
SHO	Soft Hand Off
SI	Subscriber Identity
SII	System Information Identity or Service Identity Information
SIM	Subscriber Identity Module. Smart cards used by GSM operators.
SLA	Service Level Agreement
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SS7	Signaling System 7
SSL	Secure Sockets Layer
SS	Subscriber Station
SUBC	Subscriber Credentials
TBS	Target BS
TCP	Transmission Control Protocol
TE	Terminal Equipment

Abbreviation	Expansion of Abbreviation
TLS	Transport Layer Security, a variant of SSL
TLV	Type Length Value
TTLS	Tunneled TLS
UDP	User Datagram Protocol
UDR	Usage Data Record
UE	User Equipment
UGS	Unsollicited Grant Service
UICC	Universal Integrated Circuit Card
UID	user-identity
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module. Smart cards used by UMTS operators
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VSA	Vendor Specific Attributes
WAG	WLAN Access Gatewa
WATSP	WiMAX ASN Transport Signaling Protocols
WCDMA	Wideband Code-Division Multiple Access
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
Wi-Fi	Wireless Fidelity, refers to 802.11 standards, including 802.11b, 802.11a, and 802.11g
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless local area network based on IEEE 802.11 and related standards
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network
X.509	ITU standard for digital public-key certificate issued by a CA

Attachment 4-2

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[Part 0]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 0]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Document Structure

Note: See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

This document is the first part of *WiMAX Forum Network Architecture*, which includes the following parts:

Part 0	• **Document Structure** • **Revision History**
Part 1	• **Section 1 - Document Scope** • **Section 3 - References** used in the document • **Section 4 - Tenets for WiMAX Network System Architecture** • **Section 5 - Identifiers: List of identifiers used in a WiMAX network** • **Section 6 - Network Reference Model**, a logical representation of the network architecture.
Part 2	• **Section 7 - Functional Design and Decomposition** • **Section 8 - ASN Profile Introduction**
Part 3	**Informative Annexes for Stage 2** • **Annex A:** WiMAX NWG Reference Architecture Deployment Scenarios • **Annex B:** MS Movement with FA change, no PC change • **Annex C:** ASN-GW Selection Protocol • **Annex D:** 'RRM': Spare Capacity Report per QoS Profiles • **Annex E:** Ethernet Operational Behavior • **Annex F:** TECHNICAL ANNEX: SUPPORT OF REAL TIME SERVICES
Stage 2 Abbreviations	• **Section 1**- Abbreviations, Acronyms, Definitions and Conventions used in the document
3GPP	• **WiMAX Interworking**
3GPP2	• **WiMAX Interworking**
WiMAX Interworking with DSL	• **WiMAX Interworking with DSL**

Revision History

Date	Revision
February 18, 2005	Accepted contributions/changes from F2F meeting in NJ. File name changed from "050130_NWG_BaselineSubmission_01r1_TenetsRef_Model" to "050218_NWG_STAGE2.doc" (Using web site revision management)
March 14, 2005	Incorporated changes from 050309_NWG_03_AAA.doc, Section 2 Updates, Stage 2 Tenets update, and Basic IP address management – 01r3
April 20, 2005	Added RRM changes from file "050418_RRM_1r6.doc" Approved at the Malaga Spain meeting

Date	Revision
June 17, 2005	Added the following contributions (file names): • 050602_NWG_05_Client_MIP_Architechture-accepted; • 050605_NWG_07_EAP_Arch_Accepted; • 050607_NWG_01r8_PMIP-Inter-ASN-mobility-accepted; • 050607_NWG_NRM-Accepted; • 050609_NWG_01-Intra-ASN-mobility_R6_v03_accepted; • 050609_NWG_Intra-ASN_R4_03_accepted; • 050610_NWG-QoS_accepted
June 22, 2005	Added the table of figures and the following contribution (file name): 050606_NWG_R3MM_PMIP-Security
July 5, 2005	Added contribution 050629_NWG_RRM-Stage2-updates-accepted
July 6, 2005	RRM corrections and missing text from previous RRM contribution
August 8, 2005	Added the following contributions (file names): • 050609_NDS-r2 Huawei edits meeting edits • 050627_NWG_FranceTelecom_02_3GPPInterworking • 050701_NWG_Sprint_01_IPv6_Address_Management_Section_632-Revision 1 • 050701_NWG_Sprint_02_Ipv6_Address_Management_Section_7 3 2 • 050703_NWG_02_EAP_Arch_modif_proposal(sm)2accepted • 050706_NWG_Sprint_02_3GPP2_Interworking-Revision_2 • 050706_NWG_Sprint_03_Mobile_Ipv6_Architecture • 050707_NWG_Huawei_Comments_(Intra_ASN_R4_03_accepted)_v1 • 050707_NWG_Huawei_Comments_(Intra_ASN_R4_R6_v03)_v1_accepted • 050707-NWG-QoS-Framework-Accepted • 050708_NWG_Stage2_rev4c PMN-AAA Key(Lucent) • 050712_NWG_siem_STAGE2-6-10(RRM)corr-accepted • 050714_NWG_DLS_Interworking-v14 • 050714_NWG_Emergency_Service_v1 • 070805-eth-cs-specification_stage2r2 • 050714_NWG_Inter-NAP-Mobility-harmonized • 050223_NWG_IP Address Management-1r6 • 050805_NWG_Functional_Decomposition_Paging-1r5
September 5, 2005	Added the following contributions (file names): • 050824_NWG_Huawei_Comments_Intra_ASN_ Data path modify proposal.doc • 050822_NWG_Huawei_Intra_ASN_R4_HO_flow_proposal.doc • 08-16-05_NWG_WiMAX Stage 2 – Text for NRM functional

Date	Revision
	decomposition • 08-16-05_NWG_Sprint Nextel_New Section 4_v05 • 050823_NWG_Sprint_01_MIPv6 Section 7.22 Updates • 050812_NWG_Sprint_01_ Additional MIPv6 Changes to Section 6 of Stage-2 Text – R02 • 05-08-16_NWG_Changes_to_section_6.18.2 • 050822_NWG_Huawei_Inter-NAP-Mobility_Multiple IP address comments.doc • 050827_NWG_Siemens_10_STAGE2-DSL-Interworking.doc • 050830 R1-NWG-AAA-RADIUS-Stage-2.doc • 08-16-05_NWG_Sprint Nextel_New Section 4_v05 • 050826_NWG_VoIP_v2.doc • 050826-NWG-IMS_WiMAX_integration.doc • 050826-NWG-QoS Messages r3.doc • 082505 WiMAX Key Transfer Correction – LU.doc • 08-16-05_NWG_Sprint Nextel_New Section 4_v05 • 050831_NWG-Fn-Decomp_Ch6.doc • 050825_NWG_SuggestedTextForIntraASNmobilitySec7_v01 • 050825_NWG_Siemens_Identifiers-List_r1.doc • 050826_NWG_Motorola_10_PMN_Migration_r3.doc • 050826_NWG_Motorola_PMIPKey_r1.doc
September 9, 2005	• 050818_NWG_Huawei_Comments for Secure Location Update of Paging-r4.doc • 050905_NWG_Siemens_channelbinding_r1.doc • 050826-NWG-ND&S-Revised-Huawei.doc • 050822_NWG_Huawei_Inter-NAP-Mobility_PMIP connection setup comment.doc • Added Table List
September 11, 2005	• 050826-NWG-ND&S-Revised-Huawei_r1.doc • 050825_NWG_Siemens_Identifiers-List_r2.doc
September 12, 2005	Reformatted As Agreed in 050906_NWG_02_STAGE2-document-structure
September 13, 2005	Re-applied contribution 050816_NWG_WiMAX Stage 2 – Text for NRM functional decomposition_v3 • 050826_NWG_Sprint_01_MIPv6 Inter-NAP Mobility-R02 • 050912 wimax accounting stage 2 • 050912_NWG_STAGE2 – Navini Siemens Ethernet edits • 050908_NWG_Huawei_EAP_Arch_modify proposal-r4_sanjay • 050907_NWG-R3MM-function-5

Date	Revision
September 14, 2005	Removed duplicate text on CMIP per Surest email showing the duplications Provided missed edits per Bala email Cleaned up figure 7-55 per Peretz email Corrected figures and edits per Achim's email Cleaned up formatting in the Accounting Section (7.13) Cleaned up formatting in the Hot-lining Section (7.14) **Note:** Was not able to Identify DSL Updates per Max's email This still needs addressing.
September 15, 2005	Corrected Figures 7-35, 7-105, A-8, and A-8 Accepted all changes First Ballot Version
November 29, 2005	Updated to address all initial round ballot comments as documented in 051122_Stage2_Comment_Tracking.xls
December 12, 2005	Updated to address all the quality review comments as defined in 051211_Stage2_QR_Comment_Tracking.xls. EXCEPT 9 – 11 14 23 28 33 – 34 36 – 38 41 – 43 46 – 47 49 – 68 73 – 75 77 80 – 81 84 – 85 87 – 88 91 104-105 These are all deferred for various reasons and need more input based on this version of the Stage-2
December 14, 2005	Corrected section numbering addressed additional Quality Review Comments. Open Comments to be addressed are: 9, 10, 11, 14, 36, 52, 53, 54, 55, 56, 58, 59, 60, 62, 63, 64, and 65 Note that comment 36 has a resolution, but the file cannot be located at this time.
December 15, 2005	Address comment QR36 and cleaned up some minor formatting issues. There are still 3 open issue that need resolving

Date	Revision
	1. Section 4.1.2 the NAI Identifier has an un-resolved [ref] needs resolving 2. Section 7.2.1.4 there is a large "Editors Note" that I am not sure I should remove or not. 3. QR9 regarding the 3GPP2 reference of the MIPv6 text needs to be addressed. Sprint is leading an effort to get reuse permission from 3GPP2 which should not be an issue since they have done this in the past.
February 6, 2006	No technical changes to document This version simply broke the December 15, 2005 version into 4 separate parts to reduce the size of the document to keep it more manageable. The sections are as follows: Part 0 – This document – It contains to overall cover sheet, revision history, and document definitions Part 1 – Contains sections 1 through 6 and associated Table of Contents Part 2 – Contains section 7 and associated Table of Contents Part 3 – Contains all the Annexes and associated Table of Contents
March 3, 2006	Incorporated the following agreed contributions. • 060106_NWG_Huawei_Requirements for Supporting MIPv6 Proxy DAD on the MS's CoA-r2.doc • 051104_NWG_Huawei_Change Stage2 HO Function Primitives_r2.doc • 051104_NWG_Huawei_CATR_Add Accounting Trigger_r2.doc • 051104_NWG_Huawei_CATR_Add New Action for Charging_accepted.doc • 051104_NWG_Huawei_CATR_Clarify In Prepaid of Charging_r2.doc • 051106_NWG_Huawei_CATR_Accounting proposal for Volume Count Stage 2-r2.doc • 051104_NWG_Huawei_Stage2 CMIP session termination-r1.doc • 051104_NWG_Huawei_CATR_Change Stage2 Data Path Primitives_r1.doc • 060118_NWG_Siemens&Alcatel_QoS-ArchModifProposal.doc • 060131_NWG_stage2_paging_modifications_final.doc • ASN Profiles Text Proposed Baseline v2.doc • 051205_NWG_Intel_stage2pagingchanges_tosupport_stage3r2.doc
April 14, 2006	Incorporated the following agreed contributions. • 060125_NWG_stage2_paging_modifications.doc • 060224_NWG_Siemens_stage2_annexA_update_r1.doc • 060321_NWG_Samsung_RefSec_r1.doc
April 20, 2006	Incorporated the following agreed contributions. • 060321_NWG_Siemens_stage2_AAA_update_r1.doc
August 08, 2006	Incorporate comments resolution from V&V readiness ballot' in Stage 2 Part 0 and Stage 3
August 9th, 2006	- Final V&V readiness draft

Date	Revision
February 24th, 2007	All accepted contributions from V&V implemented
July 11, 2007	Implemented all Stage 2 accepted contributions from 00000_r016_NWG-Rel-1[1].0.0-CR-Tracking-Spreadsheet.xls

Attachment 4-3

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[Part 1]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 1]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

1. Introduction and Scope

This document describes the architecture reference model, reference points and protocols and procedures for different end-to-end architecture aspects of WiMAX NWG. The framework is in response to the Stage 1 requirements document.

2. Definitions, and Conventions

2.1 Definitions

2.1.1 AAA

AAA refers to a framework, based on IETF protocols (RADIUS or Diameter), that specifies the protocols and procedures for authentication, authorization, and accounting associated with the user, MS, and subscribed services across different access technologies. For example, AAA includes mechanisms for secure exchange and distribution of authentication credentials and session keys for data encryption.

Location: ASN and CSN

2.1.2 Access Service Network (ASN)

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
- Transfer of AAA messages to WiMAX subscriber's Home Network Service Provider (H-NSP) for authentication, authorization and session accounting for subscriber sessions
- Network discovery and selection of the WiMAX subscriber's preferred NSP
- Relay functionality for establishing Layer-3 (L3) connectivity with a WiMAX MS (i.e. IP address allocation)
- Radio Resource Management

In addition to the above mandatory functions, for a portable and mobile environment, an ASN SHALL support the following functions:

- ASN anchored mobility
- CSN anchored mobility
- Paging
- ASN-CSN tunneling

ASN comprises network elements such as one or more Base Station(s), and one or more ASN Gateway(s). An ASN MAY be shared by more than one Connectivity Service Networks (CSN)

2.1.3 Accounting Agent

The Account Agent is defined as the functional entity which collects the related accounting information, such as the unsent downlink volume information to the MS and the airlink record information, etc.

Location: ASN

2.1.4 Admission Control

Admission Control is the ability to admit or ability to control admission of a user to a network based on user's service profile and network performance parameters (for example, load and average delay). If a user requests access to network services but the incremental resources required to provide the grade of service specified in the user's service profile are not available, the Admission Control function rejects the user's access request. Note that Admission Control is implemented to ensure service quality and is different from authentication and authorization, which are also used to admit or deny network access.

Location: ASN and CSN

2.1.5 Application Service Provider (ASP)

Application Service Provider (ASP) is a business entity that provides applications or services via V-NSP or H-NSP.

2.1.6 ASN Anchored Mobility

ASN Anchored mobility refers to the set of procedures associated with the movement (handover) of an MS between two Base Stations (referred to in the IEEE 802.16 literature as Serving and Target BS), where the Target BS may belong to the same ASN or a different one, without changing the traffic anchor point for the MS in the serving (anchor) ASN. The associated procedures involve transferring the context of all service flows together with other context from the previous BS to the new BS while attempting to ensure minimal delay and data loss during the transition. ASN Anchored Mobility is mobility within the area of one or more ASNs without FA relocation, i.e. without R3 Mobility. This includes intra-ASN and inter-ASN MM as long as the “ASN R3 reference anchor point” in the NAP, and hence the FA, does not change.

Entities: MS and ASN

2.1.7 ASN Mobility

Same as ASN Anchored Mobility.

2.1.8 Authenticator

Authenticator functionality is defined as per standard EAP 3-party model. An authenticator is an entity at one end of a point-to-point link that facilitates authentication of supplicant (MS) attached to the other end of that link. It enforces authentication before allowing access to services that are accessible to the supplicant. The Authenticator also incorporates AAA client functionality that enables it to communicate with the AAA backend infrastructure (AAA-based Authentication Server) which provides the Authenticator with authentication services over AAA protocols. The Authenticator is always collocated with the Key Distributor and MAY be collocated with the Authentication Relay and Key Receiver functions as defined in Part 2 Section 7.4 – ASN Security Architecture.

2.1.9 Base Station

See Section 6.3.3

2.1.10 Connectivity Service Network (CSN)

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

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

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.

2.1.11 CSN Anchored Mobility

CSN Anchored mobility refers to a set of procedures for changing the traffic anchor point for the MS from one anchor point to another one in the ASN without changing the CSN anchor. CSN anchored mobility is independent to the .16e handover.

Entities: MS, ASN, CSN

2.1.12 Ethernet Support

Ethernet support refers to a transport that carries encapsulated IPv4 or IPv6 addressing or other payload and encapsulation of end-user data sessions. Ethernet support includes IEEE802.3, IEEE802.1D and IEEE802.1Q. Ethernet MAY be tunneled using MPLS, IPsec, GRE or other tunneling protocols. Ethernet support in WiMAX network MAY operate in two variations:

- End-to-End Ethernet connectivity from the WiMAX SS/MS across WiMAX network (e.g. for connectivity to DSL networks with PPPoE). This option does not support Macro Mobility.
- Ethernet support within the ASN segment only. This support allows Ethernet transport between WiMAX SS/MS and ASN.

Location: MS, ASN, and CSN

2.1.13 Firewall

A firewall provides protection to network elements by enforcing access and filter policies used to monitor and control traffic to and from a network. It can be viewed as a set of rules and policies that determine which traffic should be permitted to go through or blocked. One of its main purposes is to detect and prevent Denial of Service (DoS) attacks on a network.

Location: ASN, CSN, and possibly the ASP Network's infrastructure

2.1.14 Home Network Service Provider (H-NSP)

A home NSP is the operator or business entity that has Service Level Agreements with WiMAX subscribers, authenticates and authorizes subscriber sessions (in-network or roaming scenarios) and services the subscriber's account (charging and billing). To support roaming services, a Home NSP MAY have roaming relationships with other NSPs.

2.1.15 Internet Access

Internet access refers to a gateway that resides at the edge of NAP or NSP network connecting it to Internet. Apart from the IP routing functionality, such gateways MAY include functions such as VPN, Firewall, NAT, layer-4 forwarding, and mobile IPv4 home agent. Alternatively, these functions MAY be implemented in network elements that are either in front of or behind the gateway. Certain deployments MAY also implement functions such as metering and policing as part of Internet Access.

2.1.16 Internetworking Function

An Internetworking Function (IWF) or an Internetworking Unit (IWU) is a network entity that translates one or more communication protocols (data and/or control) from one form to another. An IWU enables integration or interoperability between different types or generations of networks and/or services. For example, an IWU terminating a WiMAX NWG-specified reference point MAY facilitate interoperability between a Greenfield WiMAX network and an incumbent 3G network.

Location: This function resides in the CSN.

2.1.17 IP Header Compression

Header compression is a function to reduce the size of the headers of the packets and increase the overall communication performance between a pair of communication nodes.

Location: MS and ASN

2.1.18 IP Support

IP Support refers to the capability of the WiMAX network to transport IPv4 and IPv6 datagrams as end to end managed session between the WiMAX SS/MS and any IP peer across WiMAX network. IP support does not require any additional L2 encapsulation over the air except for 802.16e and MAY be tunneled in WiMAX network using GRE, MPLS, VLAN or other tunneling protocols.

2.1.19 IPv4 Support

IPv4 support refers to a set of capabilities that enable IPv4 addressing and encapsulation of end-user data sessions. The IPv4 encapsulation MAY directly encapsulate an IPv4-compatible application protocol running over IP transports, such as FTP, SIP, SMTP or HTTP. Alternatively, it MAY encapsulate tunneled end-user data as in the cases of Mobile IP, IPsec or GRE. The end-user IPv4 session MAY in turn be encapsulated within the NAP and NSP networks in an IPv6 tunnel, so long as the IPv6 cladding is removed prior to the delivery of its IPv4 contents. IPv4 Support does not guarantee performance of any particular end-user IPv4 flow, only that the flow will be conveyed between any two nodes in the NAP or NSP networks in a manner logically consistent with IPv4.

Location: MS, ASN, CSN and ASP Network infrastructure

2.1.20 IPv6 Access Router (AR)

The IPv6 AR is the first hop router for an IPv6 MS in the ASN. The IPv6 link exists between the MS and the IPv6 AR and is established via a combination of the transport connection over the air interface (R1) and the GRE tunnel between the BS and ASN-GW functions when implemented in separate physical entities.

2.1.21 IPv6 Support

IPv6 support is a set of capabilities enabling IPv6 addressing and encapsulation of end-user data sessions. The IPv6 encapsulation MAY directly encapsulate an IPv6-compatible application protocol running over IP transports, such as FTP, SIP, SMTP or HTTP. Alternatively, it MAY encapsulate tunneled end-user data as in the case of GRE. The end-user IPv6 session MAY in turn be encapsulated within the NAP and NSP networks in an IPv4 tunnel, so long as the IPv4 cladding is removed prior to the delivery of its IPv6 contents. IPv6 support does not guarantee the performance of any particular end-user IPv6 flow, only that the flow will be conveyed between any two nodes in the NAP or NSP networks in a manner logically consistent with IPv6.

Location: MS, ASN, CSN and ASP Network infrastructure

2.1.22 Location-Based Service (LBS)

A location-based service (or LBS) is a service provided to a subscriber based on the current geographic location of the WiMAX client MS.

Location: CSN or ASP Network and MS

2.1.23 Media Gateway

A media gateway is an entity that converts media formats in order to provide compatibility between two networks. . For example, a media gateway could terminate bearer channels from a switched circuit network (e.g., DS0s) and media streams from a packet network (e.g., RTP streams in an IP network). A media gateway MAY be capable of processing audio, video and T.120 alone or in any combination, and MAY be capable of full duplex media translations. Additionally, a media gateway MAY also play audio/video messages and support interactive voice response features, or MAY perform media conferencing.

Location: CSN or existing core network in an Interworking scenario

2.1.24 Mobile Station (MS)

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..

2.1.25 NAS

The term NAS refers to the grouping of the following functions in the ASN:

* EAP Authenticator

* The Prepaid Client

* Hot-line Device

* AAA client

* Accounting Client

In addition to the above, the NAS maintains and distributes keys received from the AAA infrastructure to various other functions in the ASN and for that reason may also be labeled Anchor Authenticator.

2.1.26 Network Access Provider (NAP)

Network Access Provider (NAP) is a business entity that provides WiMAX radio access infrastructure to one or more WiMAX Network Service Providers (NSPs). A NAP implements this infrastructure using one or more ASNs.

2.1.27 Network Discovery and (Re)selection

Network Discovery and (Re)selection refers to protocols and procedures where the MS detects the existence of one or more NAPs owned by or affiliated with the subscriber's home NSP (directly or through a roaming partner) and selects a NAP based on its local policy to gain access to IP data services.

Location: MS and ASN

2.1.28 Network Management

Network management refers to a variety of tools, applications, and MSs that assist human network managers in monitoring and maintaining networks. The fundamental classes of management operations are typically described as Fault, Configuration, Accounting, Performance and Security (FCAPS).

Most network management architectures use the same basic structure and set of relationships. Managed MSs, such as computer systems and other network MSs, run software (typically referred to as an agent) that enables network managers to query information from agents or be notified when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.

Location: The ASN, CSN and ASP infrastructure will nominally have independent network management functions. Mechanisms to query and process the management information bases MAY be centralized or distributed.

2.1.29 Network Service Provider (NSP)

Network Service Provider (NSP) is a business entity that provides IP connectivity and WiMAX services to WiMAX subscribers compliant with the Service Level Agreement it establishes with WiMAX subscribers. To provide these services, an NSP establishes contractual agreements with one or more NAPs. Additionally, an NSP MAY also establish roaming agreements with other NSPs and contractual agreements with third-party application providers (e.g., ASP or ISPs) for providing WiMAX services to subscribers.

From a WiMAX subscriber standpoint, an NSP MAY be classified as Home NSP (H-NSP) or Visited NSP (V-NSP).

2.1.30 Paging

Paging refers to procedures used by the network to seek an MS in idle mode in the coverage area of a predefined set of Base Station(s) identified by a Paging Group (as per IEEE 802.16e specification). In addition, Paging Update refers to procedures to obtain location update or network entry from an MS in idle mode. Paging procedures are implemented using Paging MAC message exchanges between MS and BS, under the control of a higher-layer paging management functions.

Location: ASN and MS

2.1.31 Payload Compression

Payload compression is a function to reduce the size of datagram payloads and increase the overall communication performance between a pair of communication nodes. Examples of payload compression protocols include the use of [37] over IP transport.

Location: The payload compression function and its protocol SHALL be running between two communicating peers.

2.1.32 Peer-to-Peer Service

Peer-to-peer or point-to-point services are IP services delivered to MS using a point-to-point IP-connectivity bearer channel. The correspondent node to MS for such services MAY be another MS or a network server. Examples of such services include peer-to-peer file-sharing, VoIP, gaming, etc.

Location: MS, CSN, or ASP Network

2.1.33 Point of Attachment Address (PoA)

A Point of Attachment (PoA) address refers to the IP address, routable in CSN domain that is allocated to MS for the purpose of data connectivity. For fixed, nomadic and PMIP-based access, the PoA address is delivered to MS using DHCP. For CMIPv4-based mobile SS/MSs, the PoA address is delivered using MIP-based procedures. For MIPv4-based access, a PoA address refers to Home Address. For MIPv6 based access, a PoA may refer to the CoA or HoA

2.1.34 Power Management

There are two aspects of power management:

- **MS platform power management** – This refers to efficient allocation of Sleep and Idle modes to an MS with the intention of maximizing battery life while minimizing disruption to communication flows between an MS and the network. Sleep and Idle modes are described in the 802.16e specification.
- **MS transmit power management** – This refers to the management of MS transmit power based on one or more factors with the intent to conserve battery resources while not impacting communication flows between an MS and the network.

Location: MS and ASN

2.1.35 QoS Enforcement and Admission Control

QoS enforcement and admission control refers to procedures that ensure QoS in the ASN infrastructure comprising infrastructure provided by more than one Service Provider or third-party carrier. These functions include QoS profile authorization, QoS admission control, Policy Enforcement Point (PEP), Policy Decision Functions (PDF), policing and monitoring, QoS parameter mapping across different QoS domains, etc. These procedures MAY reside within a network or distributed across networks.

Location: MS, ASN, CSN, and ASP Network

2.1.36 Radio Resource Management (RRM)

Radio Resource Management refers to *measurement*, *exchange*, and *control* of radio resource-related indicators (e.g., current subchannel allocations to service flows) in a wireless network.

Measurement refers to determining values of standardized radio resource indicators that measure or assist in estimation of available radio resources.

Exchange refers to procedures and primitives between functional entities used for requesting and reporting such measurements or estimations. The resulting information from exchange MAY be made available within the measuring station (using proprietary procedures and primitives), or, to a remote functional entity (using standardized procedures and primitives).

Control refers to decisions made by the measuring station or remote entity to adjust (i.e., allocate, reallocate or deallocate) radio resources based on the reported measurements, other information, or using proprietary algorithms, and communicating such adjustments to network entities using standardized primitives. Such control MAY be local and remote from the measuring station.

Location: MS and ASN

2.1.37 Reference Point

A reference point (RP) is a conceptual link that connects two groups of functions that reside in different functional entities of an ASN, CSN, or MS. It is not necessarily a physical interface. A reference point only becomes a physical interface when the functional entities on either side of it are contained in different physical MSs.

2.1.38 Roaming

Roaming is the capability of wireless networks via which a wireless subscriber obtains network services using a "visited network" operator's coverage area. At the most basic level, roaming typically requires the ability to reuse authentication credentials provided/provisioned by the home operator in visited networks, successful user/MS authentication by the home operator, and a mechanism for billing reconciliation and optionally access to services available over the Internet services. A key benefit of roaming is to provide a wider coverage and access to subscribers of an operator with consolidated/common billing.

Location: MS, ASN, and CSN

2.1.39 Service Level Agreement (SLA)

A Service Level Agreement (SLA), as defined in [8] is "a contract between a network's provider and user or between network providers that defines the service level which a user will see or an operator can obtain and the cost associate with that level of service".

2.1.40 Session Management

At a fundamental level, a session refers to link-layer, IP-layer, or, higher layer connectivity established between one or more MS and a network element in order to exchange link-level frames or packets. Additionally, a session MAY have certain well-defined properties associated with it such as traffic characteristics (e.g., traffic type, policy, encryption), mobility support (e.g., re-authentication, re-keying, routing), and robustness (e.g., state management, persistence). Session management generically refers to the set of procedures implemented in MS and the network that support all such properties associated with an active session.

Location: MS and ASN or CSN or ASP Network

2.1.41 SLA Management

SLA management refers to procedures that translate a Service Level Agreement into a set of QoS parameters and their values, which together define the service offered.

Location: This function MAY be located between ASN and CSN, CSN and ASP's infrastructure, or between CSNs of two NSPs.

2.1.42 MS IP Address Management

IP address assignment is typically done after the MS is authenticated and authorized to the network. The IP address allocated to an MS may be public or private, and may either be a point-of-attachment IP address or an inner-tunnel IP address. For the basic-connectivity IP service, the IP address is assigned by the CSN (incumbent or reference). For IP services accessible over an inner-tunnel, the network that terminates the tunnel allocates the IP address.

Location: MS and CSN

2.1.43 Subscriber Station

Generalized stationary equipment set providing connectivity between subscriber equipment and a base station (BS). The Subscriber Station may be a host or support multiple hosts.

2.1.44 Tunneling

Tunneling refers to the capability that enables two packet networks to exchange data or packets via intermediate networks, while hiding the protocol details from the intermediate networks. Tunneling is generically implemented by encapsulating an end-to-end network protocol within packets that are natively carried over the intermediate networks. For example, Point-to-Point Tunneling Protocol (PPTP) is a technology that enables organizations to use the Internet to transmit private data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. Tunneling is alternately referred to as encapsulation.

Location: MS and CSN and/or ASP's infrastructure.

2.1.45 Visited Network Service Provider (V-NSP)

A visited NSP is defined from a roaming WiMAX subscriber standpoint. A roaming subscriber uses the visited NSP's coverage area for access to WiMAX services. A visited NSP may have roaming relationship with subscriber's home NSP. The visited NSP provides AAA traffic routing to home NSP. Depending on WiMAX services requested and the roaming agreement between home NSP and visited NSP, the visited NSP MAY provide some/all WiMAX services to roaming WiMAX subscriber or provide data/control traffic routing to home NSP.

2.2 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [10].

3. References

[1] IEEE 802.16-2004 October 2004, Air Interface for Fixed and Mobile Broadband Wireless Access Systems — Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, August 2004.

[2] IEEE 802.16-2005 and IEEE 802.16-2004/Cor 1-2005, Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, February 2006

[3] Public EtherType Field Listings, http://www.iana.org/assignments/ethernet-numbers

[4] RFC792 - Internet Control Message Protocol (ICMP), J. Postel, September 1981,

[5] RFC826 - An Ethernet Address Resolution Protocol (ARP), David C. Plummer, November 1982.

[6] RFC1027 - Using ARP to Implement Transparent Subnet Gateways, Smoot Carl-Mitchell and John S. Quarterman, October 1987

[7] RFC1349 – Type of Service in the Internet Protocol Suite, P. Almquist, July 1992.

[8] RFC1678 - IPng Requirements of Large Corporate Networks, E. Britton and J. Tavs, August 1994, Informational

[9] RFC1701 - Generic Routing Encapsulation (GRE), S. Hanks, et al., October 1994, Informational

[10] RFC2119 – Key words for use in RFCs to Indicate Requirement Levels, S. Bradley, March 1997, Best Current Practice

[11] RFC2131 – Dynamic Host Configuration Protocol (DHCP), R. Droms, March 1997, Standards Track

[12] RFC2132 – DHCP Options and BOOTP Vendor Extensions, S. Alexander and R. Droms, March 1997, Standards track

[13] RFC2205 – Resource ReSerVation Protocol (RSVP), R. Braden, et al., September 1997, Standards track

[14] RFC2327 – SDP: Session Description Protocol, M. Handley and V. Jacobson, April 1998, Standards Track

[15] RFC2461 – Simpson, Neighbor Discovery for IP Version 6 (IPv6), Narten and Nordmark, December 1998, Standards Track

[16] RFC2462 – IPv6 Stateless Address Auto-configuration, Thomson and Narten, December 1998, Standards Track

[17] RFC2474 – Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers, K. Nichols, et al., December 1998, Standards Track

[18] RFC2475 – Architecture for Differentiated Services, S. Blake, et al., December 1998, informational

[19] RFC2597 – Assured Forwarding PHB Group, J. Heinanen, et al., June 1999, Standards Track

[20] RFC2598 – Expedited Forwarding PHB Group, V. Jacobson, et al., June 1999, Standards Track

[21] RFC2748 – The COPS (Common Open Policy Service) Protocol, D. Durham, et al., January 2000, Standards Track

[22] RFC2794 – Mobile IP Network Access Identifier Extension for IPv4, P. Calhoun and C. Perkins, March 2000, Standards Track

[23] RFC2865 – Remote Authentication Dial In User Service (RADIUS), C. Rigney, et al., June 2000, Standards Track

[24] RFC2866 – RADIUS Accounting, C Rigney and Livingston, June 2000, Informational

[25] RFC2904 – AAA Authorization Framework, J. Vollbrecht, et al., August 2000, Informational

[26] RFC2905 – AAA Authorization Application Examples, J. Vollbrecht, et al., August 2000, Informational

[27] RFC2906 – AAA Authorization Requirements, S. Farrell, et al., August 2000, Informational

[28] RFC3012 – Mobile IPv4 Challenge/Response Extensions, C. Perkins and P. Calhoun, November 2000, Standards Track

[29] RFC 3024 – Reverse Tunneling for Mobile IP, revised, G. Montenegro, January 2001, Standards track

[30] RFC3041 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6, Narten, Draves, January 2001, Standards Track

[31] RFC3046 – DHCP Relay Agent Information Option, M. Patrick, January 2001, Standards Track

[32] RFC3084 – COPS Usage for Policy Provisioning (COPS-PR), K. Chan, et al., March 2001, Standards Track

[33] RFC3115 – Mobile IP Vendor/Organization-specific extensions, G. Dommety and K. Leung, April 2001, Standards Track

[34] RFC3118 – Authentication for DHCP Messages, R. Droms and W. Arbaugh, June 2001, Standards Track

[35] RFC3159 – Structure of Policy Provisioning Information (SPPI) K. McCloghrie, et al., August 2001, Standards Track

[36] RFC3162 - RADIUS and IPv6, B. Aboba, et al., August 2001, Standards Track

[37] RFC3173 - IP Payload Compression Protocol (IPComp), A. Shacham, et al., September 2001, Standards Track

[38] RFC3203 – DHCP Reconfigure Extension, Y. T'Joens, et al., December 2001, Standards Track

[39] RFC3264 – An Offer/Answer Model with the Session Description Protocol (SDP), J. Rosenberg and H. Schulzrinne, June 2002, Standards Track

[40] RFC3312 – Integration of Resource Management and Session Initiated Protocol, G. Camarillo, et al., October 2002, Standards Track

[41] RFC3313 – Private Session Initiation Protocol (SIP) Extensions for Media Authorization, W. Marshall, January 2003, Informational

[42] RFC3315 – Dynamic Host Configuration Protocol for IPv6 (DHCPv6, R. Droms, et al., July 2003, Standards Track

[43] RFC3344 – Mobile IP support for IPv4, C. Perkins, August 2002, Standards Track

[44] RFC3520 – Session Authorization Policy Element, L-N. Hamer, et al., April 2003, Standards Track

[45] RFC3543 - Registration Revocation in Mobile IPv4, S. Glass and M. Chandra, August 2003, Standards Track

[46] RFC3556 – Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth, S. Casner, July 2003, Standards Track

[47] RFC3565 - Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), J. Schaad, July 2003, Standards Track

[48] RFC3576 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), M. Chiba, et al., July 2003, Informational

[49] RFC3579 – RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), B. Aboba and P. Calhoun, September 2003, Informational

[50] RFC3588 – Diameter Base Protocol, P. Calhoun, et al., September 2003, Standards Track

[51] RFC3736 – Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6, R. Droms, April 2004, Standards Track

[52] RFC3748 – Extensible Authentication Protocol, B. Aboba, et al., June 2004, Standards Track

[53] RFC3775 – Mobility Support in IPv6, D. Johnson, C. Perkins, J. Arkko, June 2004, Standards Track

[54] RFC3776 – Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, J. Arkko, V. Devarapalli, F. Dupont, June 2004, Standards Track

[55] RFC3957 – Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, C. Perkins and P. Calhoun, March 2005, Standards Track

[56] RFCaaaa – draft-adrangi-eap-network-discovery-14.txt, Network Discovery and Selection within the EAP Framework, F. Adrangi, et al., August 2005, Informational (RFC Editor's Queue)

[57] draft-ietf-eap-netsel-problem-05.txt

[58] RFC4285 –Authentication Protocol for Mobile IPv6, A. Patel, et al., January 2006, Informational

[59] RFC4283 –Mobile Node Identifier Option for MIPv6, A. Patel, et al., November 2005, Standards Track

[60] RFC4282 –The Network Access Identifier, B. Aboba, et al., December 2005, Standards Track

[61] draft-ohba-eap-aaakey-binding-01.txt

[62] TR-025 – DSL Forum, “Core Network Architecture for Access to Legacy Data Network over ADSL”, Nov-1999

[63] TR-044 – DSL Forum , “Auto-Config for Basic Internet (IP-based) Services, “ Nov-2001

[64] TR-059 – DSL Forum, “DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services,” Sept-2003

[65] 3GPP TR 22.934 V6.2.0 (2003-09) “Feasibility Study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)”

[66] 3GPP TR 23.981 V6.3.0 (2005-03) “Interworking aspects and migration scenarios for IPv4 based IMS Implementations”

[67] 3GPP TS 23.002 V6.9.0 (2005-10) “Technical Specification Group Services and Systems Aspects; Network architecture (Release 6)”

[68] 3GPP TS 23.234 V6.5.0 (2005-06) “3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)”

[69] 3GPP TS 23.207 V6.6.0 (2005-10) “End-to-end Quality of Service (QoS) concept and architecture (Release 6)”

[70] 3GPP TS 23.228 V6.10.0 (2005-06) “IP Multimedia Subsystem (IMS); Stage 2, (Release 6)”

[71] 3GPP TS 24.229 V6.8.0 (2005-10) “Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 6)”

[72] 3GPP TS 24.234 V6.3.0 (2005-06) “3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (Release 6)”

[73] 3GPP TS 29.234 V6.4.0 (2005-10) “3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3”

[74] 3GPP TS 33.234 V6.5.1 (2005-06) “Wireless Local Area Network (WLAN) interworking security (Release 6)”

[75] TR-101 - DSL Forum, "Migration to Ethernet-Based DSL Aggregation", Apr-2006

[76] 3GPP2 X.S0013-000-0 v2.0 “All-IP Core Network Multimedia Domain – Overview,” Aug-2005

[77] 3GPP2 X.S0013.00200 v1.0 “All-IP Core Network Multimedia Domain: IP Multimedia Subsystem Stage 2,” Feb-2004

[78] 3GPP2 X.S0013-004-0 v1.0 “All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3,” Feb-2004

[79] WiMAX Service Provider Working Group Requirements Document, “SPWG_Requirements_10182005,” Most Current Version

[80] IEEE 802.16g /D9, April 2007.

[81] RFC 4017 – EAP Method Requirements for Wireless LAN, D. Stanley, J. Walker, B. Aboba, March 2005, Informational.

4. Identifiers

4.1 Identifiers Used in Stage-2 document

4.1.1 Introduction

This section provides at one place a list of various identifiers used in a WiMAX network. The following table is an exhaustive list of those identifiers. Each identifier is accompanied with a few key attributes (like scope, size, etc.) and a short description on its usage.

4.1.2 List of Identifiers

Identifier	Type	Size	Definition (Stage-2 section or reference to external source)	Scope (area of validity)
MS ID	binary	48 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	Global
	Each WiMAX subscriber station is provisioned with a unique 48-bit MAC address by the manufacturer. It is used in 802.16 management messages to address the MS prior to allocation of CIDs. It is transferred as part of context during handover.			
NAI	character	variable up to 253 bytes	RFC 4282 [60]	Global
	NAI is allocated to a WiMAX subscriber by its home operator and serves as primary ID for AAA purposes. WiMAX networks use NAI as defined in [60] instead of RFC2486 because the draft allows for decorated NAIs which are necessary for roaming. Although actually separate name space, NAIs are administered together with FQDNs.			
HoA	binary	4 octets / 16 octets	Section 2.1.33	Global / NSP
	HoA belongs to the address range allocated to the NSP. It is either a globally valid IPv4 or IPv6 address or allocated from the private address space range. In the second case its scope is CSN. HoA's primary use is to route MS's IP packets from internet to home or visited CSN. The CSN uses tunneling to deliver packets to ASN. HoA is also used for classifications to determine the tunnel tag.			
Flow ID	binary	variable	Part 2 Section 7.4	MS
	Used by the accounting framework to identify IP flows in primitives between CSN and ASN. Packet Data Flow ID always identifies a single unidirectional or bidirectional flow. A unidirectional Packet Data Flow ID maps to a single SFID while bidirectional Packet Data Flow ID maps to exactly two SFIDs. Packet Data Flow ID is always allocated by AAA server.			
Service flow ID (SFID)	binary	32 bit	IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]	MS
	Each service flow represents a single unidirectional WiMAX radio interface connection with guaranteed QoS parameters. Service flows could be pre-provisioned or dynamically created. SFID doesn't change during Intra-NAP handover. Note that Service Flows according 802.16 should not be confused with Service Flows as used in QoS Framework of IETF.			

<table>
<tr><th>Identifier</th><th>Type</th><th>Size</th><th>Definition (Stage-2 section or reference to external source)</th><th>Scope (area of validity)</th></tr>
<tr><td rowspan="2">Connection ID (CID)</td><td>binary</td><td>16 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>BS</td></tr>
<tr><td colspan="4">CID represents a unidirectional connection between BS and MS and it is used to address the MS when it is attached to a BS.</td></tr>
<tr><td rowspan="2">Data Path ID</td><td>binary</td><td>variable</td><td>7.7</td><td>NAP</td></tr>
<tr><td colspan="4">Data Path ID is used to identify the tunnel carrying MS traffic between ASN gateways or between the ASN gateway and base station. This specification allows only for GRE key to be used as data path ID.</td></tr>
<tr><td rowspan="2">HO ID</td><td>binary</td><td>8 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>Target BS</td></tr>
<tr><td colspan="4">Allocated by target BS and used instead of MS MAC to send the RNG_REQ during network re-entry for non-contention based ranging. Used for R6/R8 and R4 MM.</td></tr>
<tr><td rowspan="2">Paging Controller ID</td><td>binary</td><td>48 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>NAP</td></tr>
<tr><td colspan="4">Paging controller ID is a unique identity of a network entity which retains the MS state and operational parameters while MS is in idle mode. The Paging Controller ID parameter is signaled by MS during network re-entry and location update procedures.</td></tr>
<tr><td rowspan="2">PG ID</td><td>binary</td><td>16 bits</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>NAP</td></tr>
<tr><td colspan="4">Base stations are organized into paging groups, and each group is assigned a paging group ID. When the subscriber is paged, it is paged in all base stations belonging to its current paging group.</td></tr>
<tr><td rowspan="2">BS ID</td><td>binary</td><td>48 bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>Global</td></tr>
<tr><td colspan="4">BS ID is a global unique identifier for a WiMAX base station, as defined in the IEEE 802.16-2004 and IEEE 802.16-2005 standard represents one logical instance of a PHY and MAC function providing 802.16 radio connectivity services to an SS/MS (equivalent to a single frequency sector of a physical base station). The upper 24 bits contain unique identifier of a NAP (NAP ID), while lower 24 bits are used to differentiate between NAP's base stations. BS ID is programmable and is regularly broadcasted by the PHY/MAC in the DL-MAP message. Note that a physical multi-sector cell site implementation SHALL include multiple BS IDs.</td></tr>
<tr><td rowspan="2">Operator ID</td><td>binary</td><td>24-bit</td><td>IEEE 802.16-2004 and IEEE 802.16e-2005 [1] and [2]</td><td>Global</td></tr>
<tr><td colspan="4">Operator ID is a globally unique identifier of WiMAX network access provider, and is alternatively termed NAP ID. The upper 24 bits of BS ID always contain operator ID of the NAP.</td></tr>
</table>

Identifier	Type	Size	Definition (Stage-2 section or reference to external source)	Scope (area of validity)
NSP ID	binary	24 bit	Part 2 Section 7.1.4.2	Global
	NSP ID is a globally unique identifier of a WiMAX network service provider. NSP ID(s) is broadcasted on a regular basis by a base station, and it can be also solicited by the MS.			
Anchor Data Path FunctionID	binary	4 /6 / 16 octets	7.7	NAP
	Uniquely identifies the ASN GW to which the CSN sends the downlink user plane traffic.			
Authenticator ID	binary	4 /6 / 16 octets	Delivered in Intra ASN primitives (e.g. micro mobility, paging)	NAP/NSP
	IP address or other ID for the Authenticator.			

4.2 Network Addressable Identifiers for Inter-ASN Communications

When several ASNs are engaged in communication, they may use the following four Identifiers in order to address the network entities located within the communicating ASNs:

1. Base Station ID
2. Authenticator ID
3. Anchor Data Path Function ID (Anchor ASN GW ID in profiles A&C and ASN ID in profile B)
4. Paging Controller ID

These Identifiers are referred to as Network Addressable Identifiers. Network Addressable Identifier is a generic term. It can take form of 6-octet IEEE 802.16e Identifier (e.g. BS ID, PC ID), IPv4 Address or IPv6 Address.

5. Tenets for WiMAX Network Systems Architecture

The tenets presented in this section are independent of particular releases of the WiMAX Network Systems Architecture.

5.1 General

a. The architecture framework and Network Reference Model (NRM) SHALL accommodate all WiMAX-based usage models as defined in the Stage 1 requirements specification [79].

b. The WiMAX architecture, based on a packet-switched framework, SHALL be based on the IEEE 802.16 standard and its amendments and use appropriate IETF RFCs and IEEE Ethernet standards. In the event that currently defined IETF protocols do not satisfy a solution requirement, extensions (some possibly unique to WiMAX) MAY be specified.

c. The architecture framework SHALL permit decoupling of access architecture (and supported topologies) from connectivity IP services and consider network elements of the connectivity serving network (CSN) agnostic to the IEEE 802.16 radio specifics.

d. The WiMAX network architecture framework SHALL be based on functional decomposition principles (i.e. decomposition of features into functional entities across interoperability reference points, without specific implementation assumptions including the notion of network entities and interfaces). Such a framework SHALL be modular and flexible enough to accommodate a broad range of deployment options such as:

   - Small-scale to large-scale (sparse to dense radio coverage and capacity) WiMAX networks
   - Urban, suburban and rural radio propagation environments
   - Licensed and/or licensed exempt frequency bands
   - Hierarchical, flat, or mesh topologies, and their variants
   - Co-existence of fixed, nomadic, portable and mobile usage models

e. The WiMAX architecture SHALL employ use of native IEEE 802.16 procedures and logical separation between such procedures and IP addressing, routing and connectivity management procedures and protocols to enable use of the access architecture primitives in standalone and interworking deployment scenarios.

f. The architecture SHALL support sharing of a NAP's ASN(s) by multiple NSPs.

g. The architecture SHALL support a single NSP providing service over multiple ASN(s) – managed by one or more NAPs.

h. The architecture SHALL support the discovery and selection of accessible NSPs by an MS.

i. The architecture SHALL support NAPs that employ one or more ASN topologies.

j. The architecture SHALL support access to incumbent operator services through internetworking functions as needed.

k. The architecture SHALL specify open, published and accepted standards based and well-defined reference points between various groups of network functional entities (within an ASN, between ASNs, between an ASN and a CSN, and between CSNs), and in particular between an MS, ASN and CSN to enable multi-vendor interoperability.

l. The architecture SHOULD be flexible so it is likely that it accommodates future enhancements to the IEEE802.16 suite of standards

m. The architecture SHOULD be able to accommodate documented geo-specific constraints.

n. The architecture SHOULD support evolution paths between the various usage models subject to reasonable technical assumptions and constraints.

o. The architecture SHALL not preclude different vendor implementations based on different combinations of functional entities on physical network entities, as long as these implementations comply with the normative protocols and procedures across applicable reference points, as defined in this specification.

p. The architecture SHALL support the most trivial scenario of a single operator deploying an ASN together with a limited set of CSN functions, so that the operator can offer basic Internet access service without consideration for roaming or interworking.

5.2 Services and Applications

a. The architecture SHALL be capable of supporting voice, multimedia services and other mandated regulatory services such as emergency services and lawful interception.

b. The architecture SHALL be agnostic to and support access to a variety of independent Application Service Provider (ASP) networks.

c. The architecture SHALL support mobile telephony communications using VoIP and, in applicable roaming scenarios, SHALL support inter-operator policy definition, distribution and enforcement as needed for voice communications. The following capabilities SHALL apply (subject to specific services offered and provisioned):

- The architecture SHALL support SLA-based resource management for subscribers
- The architecture SHALL support more than one voice session (when applicable) to the particular subscriber
- The architecture SHALL support simultaneous voice and data sessions.
- The architecture SHALL support prioritization (including pre-emption) for emergency voice calls and high priority data sessions

d. The architecture SHALL support interfacing with various interworking and media gateways permitting delivery of incumbent/legacy services translated over IP (for example, SMS over IP, MMS, WAP) to WiMAX access networks.

e. The architecture SHALL support delivery of IP Broadcast and Multicast services over WiMAX access networks.

5.3 Security

a. The WiMAX security framework SHALL be agnostic to the operator type and ASN topology and apply consistently across Greenfield and internetworking deployment models and usage scenarios (where possible).

b. The architecture SHALL accommodate support for strong mutual MS authentication between an MS and the WiMAX network, based on the IEEE 802.16 security frameworks.

c. An MS SHOULD be able to support all commonly deployed authentication mechanisms and authentication in home and visited operator network scenarios based on a consistent and extensible authentication framework. An MS SHOULD be able to select between various authentication method(s) based on NSP type.

d. The architecture SHALL support data integrity, replay protection, confidentiality and non-repudiation using applicable key lengths within the WiMAX Access Network.

e. The architecture SHALL accommodate the use of MS initiated/terminated security mechanisms such as Virtual Private Networks (VPNs) [ref].

f. The architecture SHALL accommodate standard secure IP address management mechanisms between the MS and its home or visited NSP [ref].

g. Unless explicitly permitted, the architecture SHOULD ensure MS and host's specific states such as – authentication state, IP Host configuration, service provisioning and service authorization are not inadvertently shared with other users/SS/MSs.

h. As required and specified in IEEE 802.16 and applicable IETF IP protocol specifications [ref], group communications SHALL be restricted to authorized group membership.

5.4 Mobility and Handovers

a. The architecture SHALL NOT preclude inter-technology handovers— e.g., to Wi-Fi, 3GPP, 3GPP2, DSL/MSO – when such capability is enabled in multi-mode MS.

b. The architecture SHALL accommodate IPv4 or IPv6 based mobility management. Within this framework, and as applicable, the architecture SHALL accommodate MS with multiple IP addresses and simultaneous IPv4 and IPv6 connections.

c. The architecture SHALL NOT preclude roaming between NSPs. The architecture SHOULD allow a single NAP to serve multiple MSs using different private and public IP domains owned by different NSPs (except where solutions become technically infeasible). The NSP MAY be one operator or a group of operators (e.g., Visited Operator MAY be different from the Home Operator and the Home Operator MAY delegate mobility unrelated service aspects to third party ISPs).

d. The architecture SHALL support mechanisms to support seamless handovers at up to vehicular speeds— satisfying bounds of service disruption as specified in Stage 1.

e. The architecture SHALL support dynamic and static home address configurations.

f. The architecture SHALL allow for dynamic assignment of the Home Agent in the service provider network as a form of route optimization, as well as in the home IP network as a form of load balancing.

g. The architecture SHALL allow for dynamic assignment of the Home Agent in H-CSN or V-CSN based on policies

5.5 Quality of Service

a. To flexibly support simultaneous use of a diverse set of IP services, the architecture framework SHALL support:

- Differentiated levels of QoS – coarse-grained (per user/SS/MS) and/or fine-grained (per service flow per user/SS/MS)
- Admission control
- Bandwidth management

b. The architecture SHALL support the means to implement policies as defined by various operators for QoS based on their SLAs, which MAY require policy enforcement per user and user group as well as factors such as location, time of day, etc. QoS policies MAY be synchronized between operators depending on subscriber SLAs, accommodating for the fact that not all operators MAY implement the same policies.

c. The architecture SHALL use standard IETF mechanisms for managing policy definition and policy enforcement between operators.

5.6 Scalability, Extensibility, Coverage and Operator Selection

a. The WiMAX Access Service Network (ASN) architecture SHALL enable a user to manually or automatically select from available NAPs and NSPs.

b. The architecture SHALL enable ASN and CSN system designs that easily scale upward and downward – in terms of coverage, range or capacity.

c. The architecture SHALL accommodate a variety of ASN topologies— including hub-and-spoke, hierarchical, flat, and/or multi-hop interconnects.

d. The architecture SHALL accommodate a variety of backhaul links, both wireline and wireless with different latency and throughput characteristics.

e. The architecture SHALL support incremental infrastructure deployment.

f. The architecture SHALL support phased introduction of IP services that in turn scale with increasing number of active users and concurrent IP services per user.

g. The architecture SHALL support the integration of base stations of varying coverage and capacity— for example, pico, micro, and macro base stations.

h. The architecture SHALL support flexible decomposition and integration of ASN functions in ASN network deployments in order to enable use of load balancing schemes for efficient use of radio spectrum and network resources.

5.7 Interworking and Roaming

a. The architecture SHALL support loosely-coupled interworking with existing wireless networks (for example, 3GPP, 3GPP2) or wireline networks (for example DSL). In all such interworking instances, the interworking interface(s) SHALL be based on standard IETF and IEEE suite of protocols.

b. The architecture SHALL support global roaming across WiMAX operator networks, including support for credential reuse, consistent use of AAA for accounting and charging, and consolidated/common billing and settlement.

c. The architecture SHALL support a variety of user authentication credential formats such as username/password, digital certificates, Subscriber Identity Module (SIM), Universal SIM (USIM), and Removable User Identify Module (RUIM).

5.8 Manageability

a. The architecture SHALL accommodate a variety of online and offline client provisioning, enrollment, and management schemes based on open, broadly deployable, industry standards.

b. The architecture SHALL accommodate Over-The-Air (OTA) services for MS SS/MS provisioning and software upgrades.

5.9 Performance

a. The architecture SHALL accommodate use of header compression/suppression and/or payload compression for efficient use of the WiMAX radio resources.

b. The architecture SHALL support mechanisms that enable maximum possible enforcement and fast re-establishment of established QoS SLAs due to handover impairments.

5.10 Multi-vendor Interoperability

a. The architecture SHOULD support interoperability between equipment from different manufacturers within an ASN and across ASNs. Such interoperability SHALL include:

- Interoperability between BS and backhaul equipment within an ASN.
- Interoperability between various ASN elements (possibly from different vendors) and CSN, with minimal or no degradation in functionality or capability of the ASN.

5.11 Convergence Sublayers (CS)

a. The IEEE 802.16 standard defines multiple convergence sub layers. The network architecture framework SHALL support the following CS types:

- Ethernet CS and IPv4/IPv6 over Ethernet CS
- IPv4 CS

- IPv6 CS

6. Network Reference Model

6.1 Overview

The Network Reference Model (NRM) is a logical representation of the network architecture. The NRM identifies functional entities and reference points over which interoperability is achieved between functional entities. Figure 6-1 illustrates the NRM, consisting of the following logical entities: MS, ASN, and CSN, whose definitions were given in Section 2.1. The figure depicts the normative reference points R1-R5.

Each of the entities, MS, ASN and CSN represent a grouping of functional entities. Each of these functions MAY be realized in a single physical functional entity or MAY be distributed over multiple physical functional entities. While the grouping and distribution of functions into physical devices within the ASN is an implementation choice, the NWG Release 1.0.0 specification defines three ASN interoperability profiles - Profiles A, B and C (see chapter 8). Infrastructure manufacturers MAY choose one or more of these ASN profiles in their physical implementations of the ASN to satisfy network interoperability requirements as detailed in other parts of the specification**.**

The intent of the NRM is to allow multiple implementation options for a given functional entity, and yet achieve interoperability among different realizations of functional entities. Interoperability is based on the definition of communication protocols and data plane treatment between functional entities to achieve an overall end-to-end function, for example, security or mobility management. Thus, the functional entities on either side of RP represent a collection of control and Bearer Plane end-points. In this setting, interoperability will be verified based only on protocols exposed across an RP, which would depend on the end-to-end function or capability realized (based on the usage scenarios supported by the overall network).

This document specifies the normative use of protocols over an RP for such a supported capability. If an implementation claims support for the capability and exposes the RP, then the implementation SHALL comply with this specification. This avoids the situation where a protocol entity can reside on either side of an RP or the replication of identical procedures across multiple RPs for a given capability.

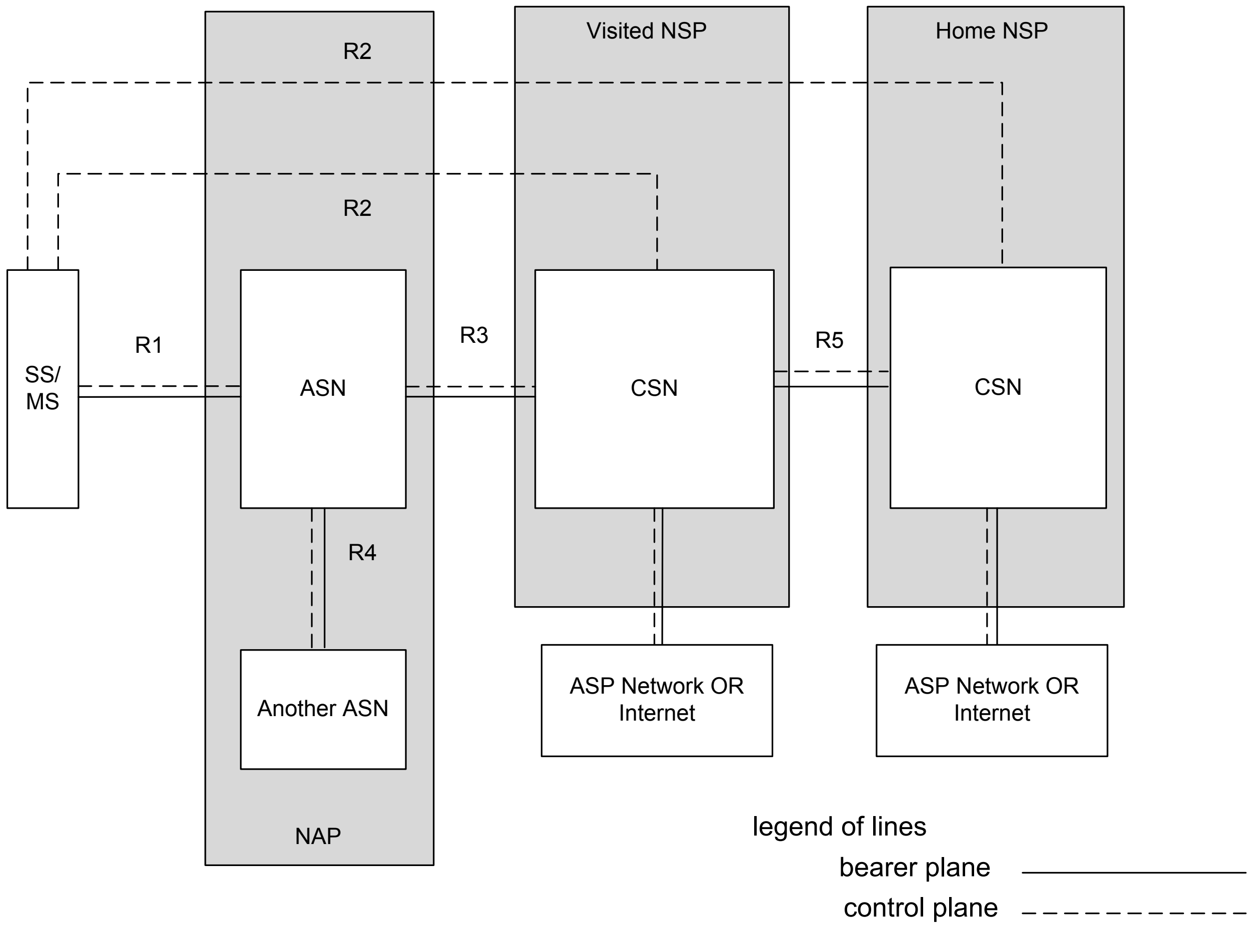


Figure 6-1—Network Reference Model[1]

6.2 Reference Points

Figure 6-1 introduces several interoperability reference points. A reference point is a conceptual point between two groups of functions that resides in different functional entities on either side of it. These functions expose various protocols associated with an RP. All protocols associated with a RP MAY not always terminate in the same functional entity i.e., two protocols associated with a RP SHALL be able to originate and terminate in different functional entities. The normative reference points between the major functional entities are in the following subsections.

6.2.1 Reference Point R1

Reference Point R1 consists of the protocols and procedures between MS and ASN as per the air interface (PHY and MAC) specifications (IEEE P802.16e-2005 [2], IEEE P802.16-2004 [1] and IEEE 802.16g). Reference point R1 MAY include additional protocols related to the management plane.

6.2.2 Reference Point R2

Reference Point R2 consists of protocols and procedures between the MS and CSN associated with Authentication, Services Authorization and IP Host Configuration management.

This reference point is logical in that it does not reflect a direct protocol interface between MS and CSN. The authentication part of reference point R2 runs between the MS and the CSN operated by the home NSP, however the

[1] Dashed/Dotted line represents the Control Plane, Normal line represents Bearer Plane

ASN and CSN operated by the visited NSP MAY partially process the aforementioned procedures and mechanisms. Reference Point R2 might support IP Host Configuration Management running between the MS and the CSN (operated by either the home NSP or the visited NSP).

6.2.3 Reference Point R3

Reference Point R3 consists of the set of Control Plane protocols between the ASN and the CSN to support AAA, policy enforcement and mobility management capabilities. It also encompasses the Bearer Plane methods (e.g., tunneling) to transfer user data between the ASN and the CSN.

6.2.4 Reference Point R4

Reference Point R4 consists of the set of Control and Bearer Plane protocols originating/terminating in various functional entities of an ASN that coordinate MS mobility between ASNs and ASN-GWs. R4 is the only interoperable RP between similar or heterogeneous ASNs.

6.2.5 Reference Point R5

Reference Point R5 consists of the set of Control Plane and Bearer Plane protocols for internetworking between the CSN operated by the home NSP and that operated by a visited NSP.

6.3 ASN Reference Model

6.3.1 ASN Definition

The ASN defines a logical boundary and represents a convenient way to describe aggregation of functional entities and corresponding message flows associated with the access services. The ASN represents a boundary for functional interoperability with WiMAX clients, WiMAX connectivity service functions and aggregation of functions embodied by different vendors. Mapping of functional entities to logical entities within ASNs as depicted in the NRM is informational.

6.3.2 ASN Decomposition

The ASN reference model is illustrated in Figure 6-2 and Figure 6-3.

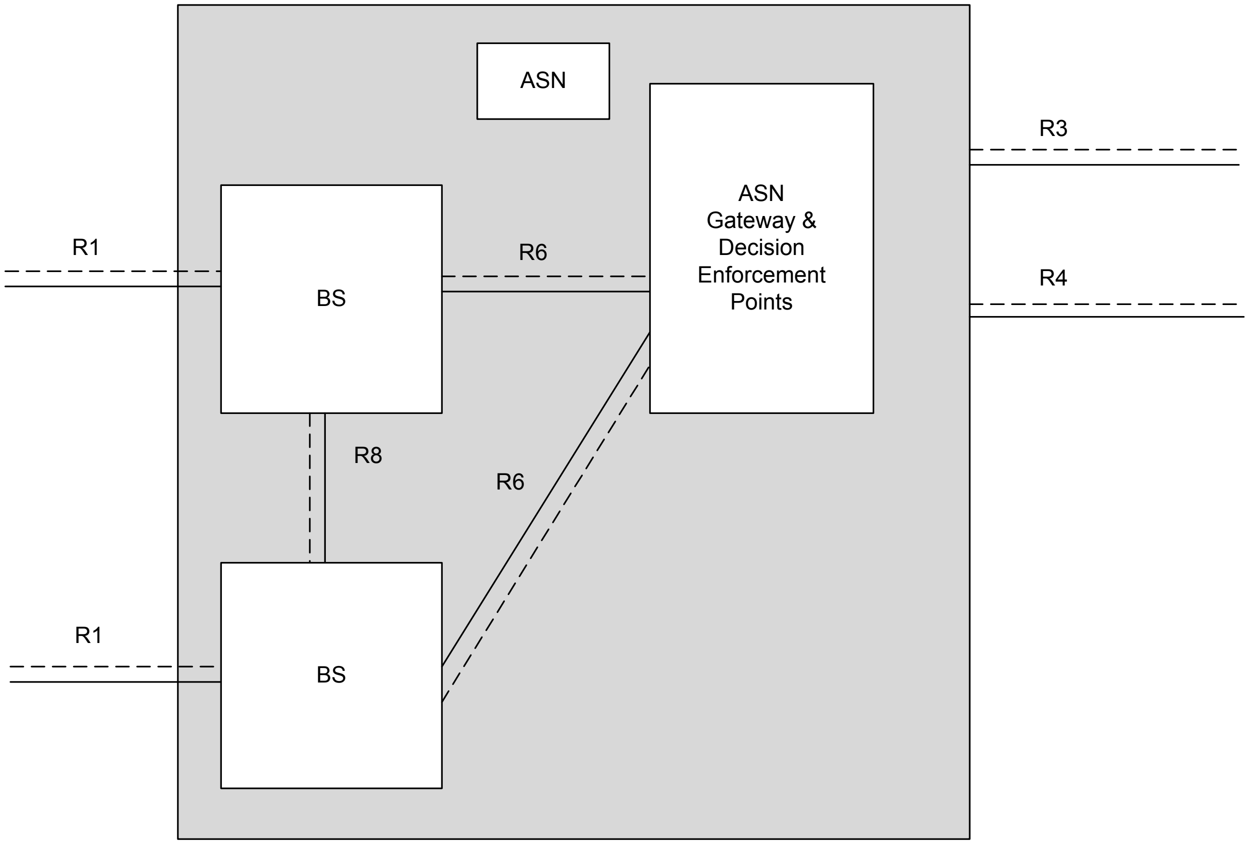


Figure 6-2—ASN Reference Model containing a single ASN-GW

An ASN shares R1 reference point (RP) with an MS, R3 RP with a CSN and R4 RP with another ASN. The ASN consists of at least one instance of a Base Stations (BS) and at least one instance of an ASN Gateway (ASN-GW). A BS is logically connected to one or more ASN Gateways (Figure 6-3)

The R4 reference point is the only RP for Control and Bearer Planes for interoperability between similar or heterogeneous ASNs. Interoperability between any types of ASNs is feasible with the specified protocols and primitives exposed across R1, R3 and R4 Reference Points.

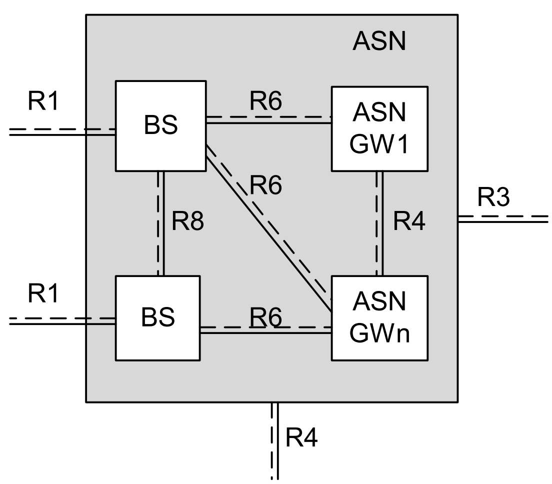


Figure 6-3—ASN Reference Model containing multiple ASN-GW

When ASN is composed of *n* ASN-GWs (where *n* > 1), Intra ASN mobility MAY involve R4 control messages and Bearer Plane establishment. For all applicable protocols and procedures, the Intra-ASN reference point R4 SHALL be fully compatible with the Inter-ASN equivalent.

6.3.3 BS Definition

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 and MAY host one or more access functions. A BS instance represents one sector with one frequency assignment. It incorporates scheduler functions for uplink and downlink resources, which will be left for vendor implementation and is outside the scope of this document. Connectivity (i.e. reachability) 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.

6.3.4 ASN Gateway Definition

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.

ASN-GW implementation MAY include redundancy and load-balancing among several ASN-GWs. The implementation details are out of scope for this document.

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).

6.3.5 ASN-GW Decomposition

The ASN functions hosted in an ASN-GW MAY optionally be viewed as consisting of two groups of functions, namely, the Decision Point (DP) and the Enforcement Point (EP). The EP includes bearer-plane functions and the DP includes non-bearer-plane functions. For implementation purposes, the decomposition of ASN functions into these two groups is optional.

If decomposed as DP and EP, the EP includes bearer-plane and the DP MAY include non-bearer-plane function – for example, Radio Resource Management Controller.

As indicated above, the aggregated ASN-GW MAY optionally be decomposed into the DP and the EP, separated by Reference Point R7, as shown in Figure 6-4 below. In an aggregated ASN-GW, the R7 RP will not be exposed. An ASN-GW DP MAY be associated with one or more ASN-GW.

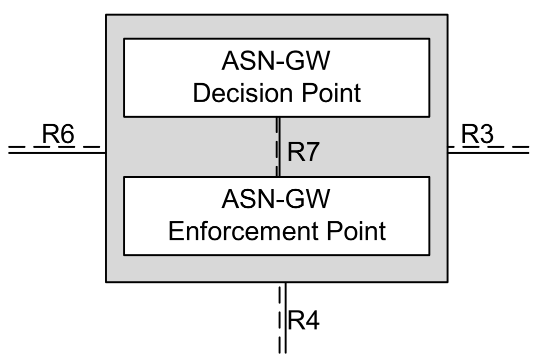


Figure 6-4—ASN-GW Decomposition Reference Diagram

ASN-GW decomposition is associated with ASN-GW reference points decomposing (e.g., R3, R4, R6) as shown in Figure 6-4..

Further decomposition of R6, R4 and R3 are out of scope for this document.

6.3.6 ASN Reference Points

In addition to the normative Reference Points R1, R2, R3, R4 and R5, the following intra-ASN informative Reference Points are identified:

6.3.6.1 Reference Point R6

Reference point R6 consists of the set of control and Bearer Plane protocols for communication between the BS and the ASN-GW. The Bearer Plane consists of intra-ASN datapath between the BS and ASN gateway. The Control Plane includes protocols for datapath establishment, modification, and release control in accordance with the MS mobility events. However, when protocols and primitives over R8 are defined, MAC states will not be exchanged over R6.

6.3.6.2 Reference Point R7

Reference Point R7 consists of the optional set of Control Plane protocols e.g., for AAA and Policy coordination in the ASN gateway as well as other protocols for co-ordination between the two groups of functions identified in R6. The decomposition of the ASN functions using the R7 protocols is optional.

6.3.6.3 Reference Point R8

Reference Point R8 consists of the set of Control Plane message flows and optionally Bearer Plane data flows between the base stations to ensure fast and seamless handover. The Bearer Plane consists of protocols that allow the data transfer between Base Stations involved in handover of a certain MS. The Control Plane consists of the inter-BS communication protocol in line with IEEE 802.16e-2005, March 2006 [2] and 802.16g [80] (802.16g is under development in the IEEE.) and additional set of protocols that allow controlling the data transfer between the Base Stations involved in handover of a certain MS. Messages and protocols shall be informatively specified for applicable ASN profiles in Release 1.0.0.

6.4 Core to Access Network Internetworking Relationships

The following figures show a couple of particular internetworking relationships between ASN and CSN for

- sharing an ASN by multiple CSN,
- providing service to roaming MS with mobility anchor in the visited CSN
- providing service to roaming MS with mobility anchor in the home CSN,
- providing a stationary service without inter-ASN mobility and
- enabling service access in the client MIPv6 case over the CoA as well as over the HoA and enabling services in the client MIPv4 case over HoA.

ASN decomposition is only shown as example for illustrative purposes.

6.4.1 NAP Sharing

Several ASNs might be connected to a single CSN and vice-versa i.e., several CSNs might share the same ASN. Figure 6-5 depicts an instance of ASN-CSN inter-connection wherein multiple CSNs share the same group of ASNs. In this scenario, ASN and MS will exchange information so that the ASN can determine which CSN an MS SHOULD be connected to. ASN and CSN may be owned by the same operator or may belong to different operators.

The case where multiple operators share the same ASN constitutes an example of unbundled access networking.

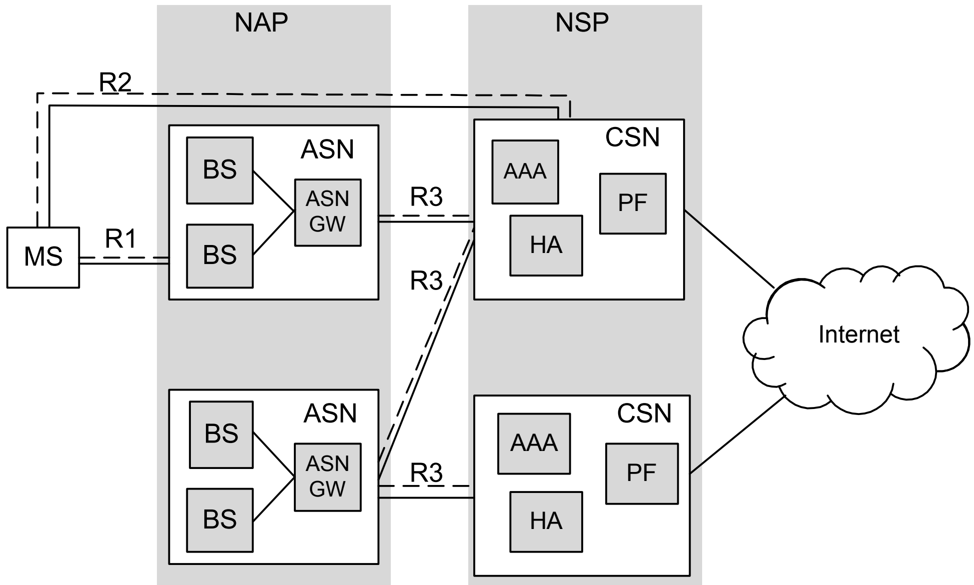


Figure 6-5: Multiple ASN to Multiple CSN Connectivity

6.4.2 Roaming with HA located in the visited NSP

The Figure 6-6 shows the reference architecture for providing service to roaming MS with usage of the HA in the visited CSN. Authentication, authorization as well as policy information is provided from the home CSN to the visited CSN over the reference point R5. Accounting information is forwarded from the visited CSN to the home CSN over R5, and access to services in the home CSN may also provided over R5 whereas Internet access is usually established directly out of the visited CSN.

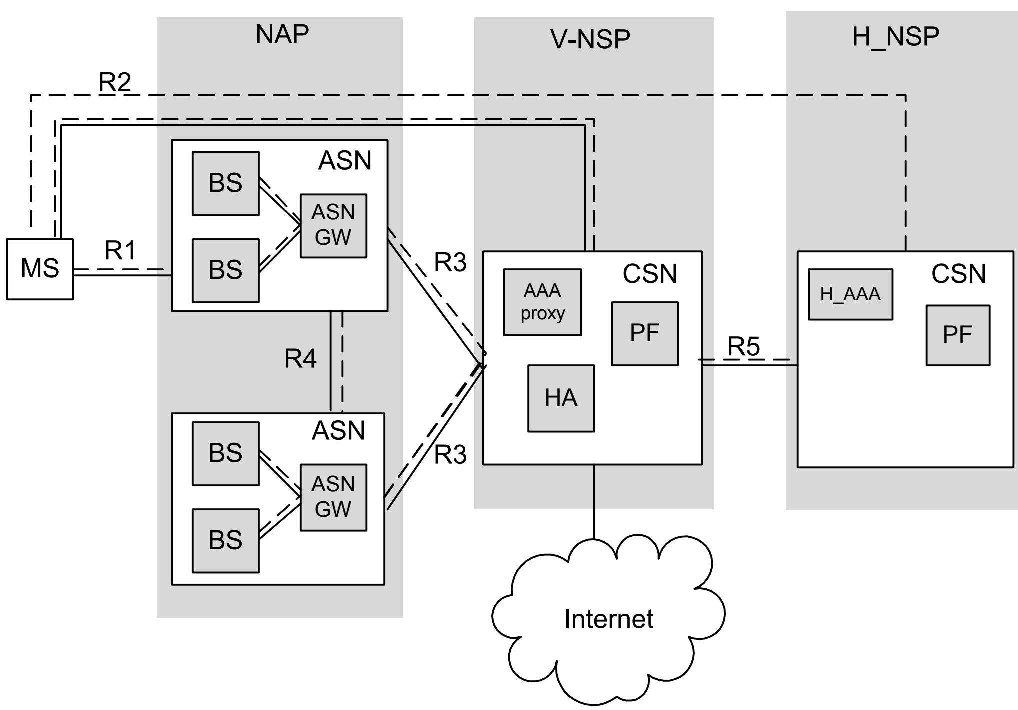


Figure 6–6: Roaming model with HA in visited NSP

6.4.3 Roaming with HA located in the home NSP

The Figure 6-7 shows the reference architecture for providing service to roaming MS with usage of the HA in the home CSN. In this case the visited CSN becomes a kind of proxy for R3. The home CSN is connected to the visited CSN over an R3 reference point with Mobile IP passing through the visited CSN and terminating in the HA in the home CSN.

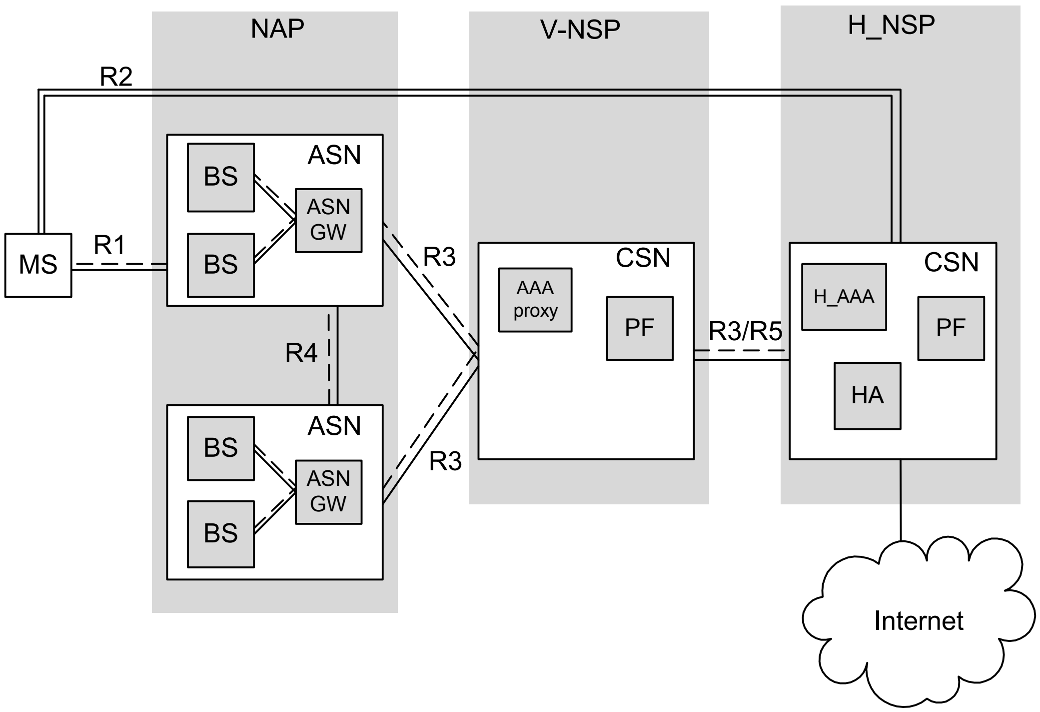


Figure 6-7: Roaming model with HA in home NSP

6.4.4 Stationary Network

When CSN-anchored mobility management is not required and a single ASN is connected with a single CSN the reference point R3 may not to be exposed. In this case it is possible to attach directly the CSN to the ASN and remove in the combined ASN/CSN all the functions not being visible on any of the remaining reference points. When serving only PMIP terminals, even the FA and the HA can be removed in the model, as these entities do not have any impact on any of the remaining reference points.

Such a simplified model is well suitable for stationary applications, as there is no need for Mobile IP based mobility management. Figure 6-8 shows the derived stationary network reference model with support for roaming MS. For roaming MS the authentication, authorization, accounting and policy control are provided by the home NSP over the reference point R5.

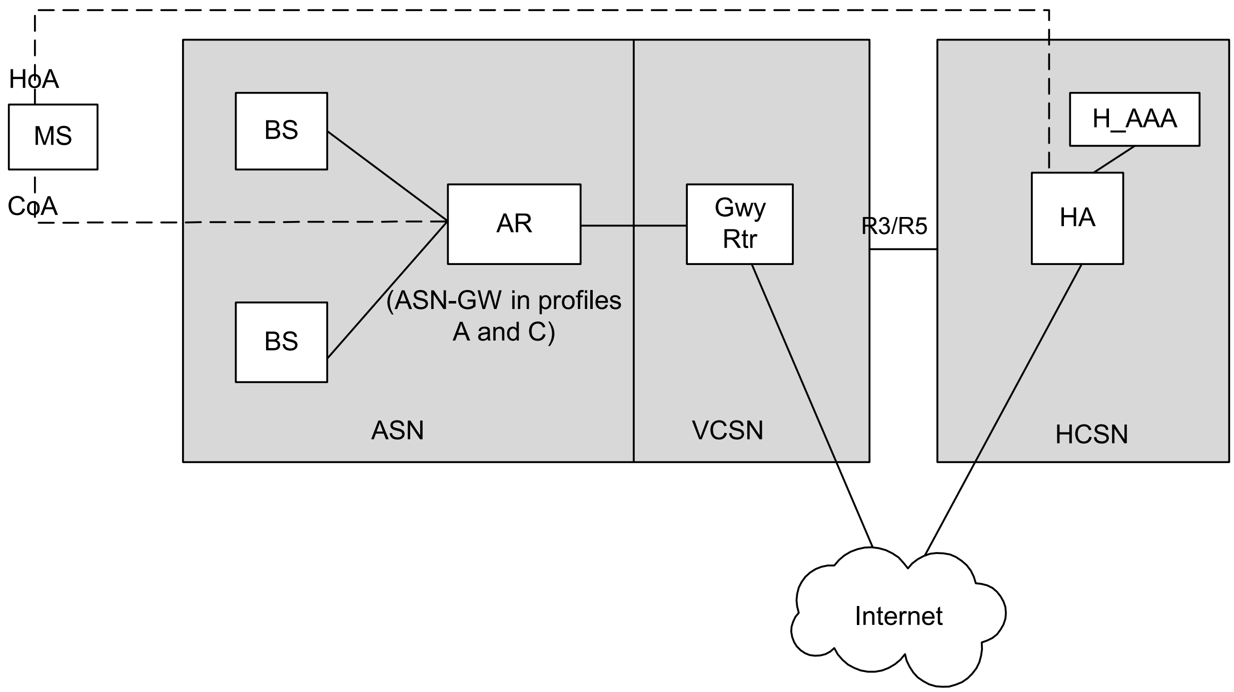


Figure 6-8 Stationary network model

6.4.5 Client MIPv6 network with service connectivity on the CoA as well as on the HoA

Terminals with client MIPv6 have been assigned two addresses: the Care-of-Address (CoA) for establishing the transport connection to the HA, and the Home Address (HoA) for providing mobile service connectivity by the HA in the home CSN. In addition to the mobile services over the HoA, the CoA can be used for stationary access to services and for route optimization between mobile terminals. Making use of the CoA for access to services requires the extension of the ASN to stationary network by directly attaching a CSN to the ASN to provide all the necessary control for service access. While route optimization and stationary services are provided by the directly attached CSN, mobile IPv6 runs over R2 from the MS to the HA in the home NSP. Authentication, authorization and accounting information as well as policy control are handled by the home NSP over an R5 reference point.

Figure 6-9 shows the network reference model for client Mobile IPv6 with support of route optimization and stationary services on the CoA.

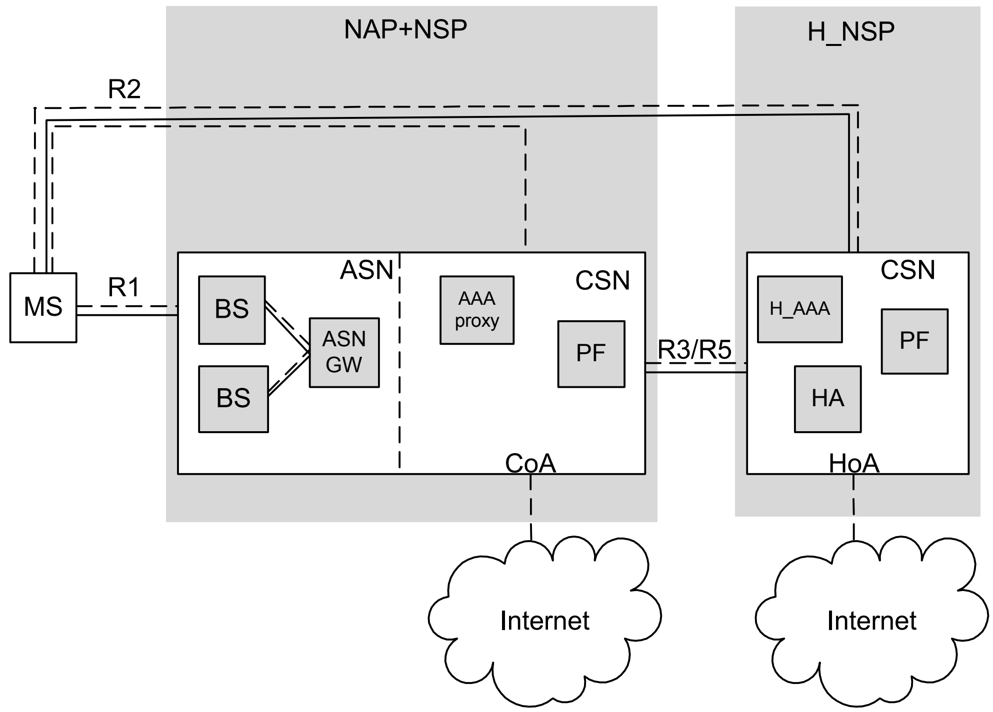


Figure 6-9 Mobile IPv6 with service over CoA and HoA

.

6.5 Release 1.0.0 Interoperability Scope

6.5.1 Reference Points

Supported capabilities across reference points R1–R5 (based on usage scenarios), and the normative definition of interoperable protocols/procedures for each supported capability is within the scope of Release 1.0.0 specification. Control Plane definition message flows and Bearer Plane data flows for interoperable R6 reference points are within the normative scope of the Release 1.0.0 specification and R7-R8 is informative for particular ASN profiles exposing the reference points.

6.5.2 ASN Functions

The normative definition of protocols, messages, and procedures to support ASN functions and capabilities, independent of specific grouping of these capabilities into physical realizations, is within the scope of Release 1.0.0 specification. The functional decomposition is the preferred methodology of Release 1.0.0 without specific reference to any logical or physical network entities. Additionally, 3 ASN Profiles (Profile A, B and C) have been defined in scope of Release 1.0.0.

6.6 CSN Reference Model

CSN internal reference points are out of scope of this specification.

Attachment 4-4

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[Part 2]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 2]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Table of Contents

TABLE OF FIGURES

LIST OF TABLES

7. Functional Design and Decomposition

Unless specified otherwise, call flows and messages defined in this section are superseded by corresponding definitions in Stage 3.

Note: See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

7.1 Network Entry Discovery and Selection/Re-selection

7.1.1 Functional Requirements

a) The solution architecture SHALL accommodate Nomadic, Portable, and fully mobile deployment scenarios.

b) The solution architecture SHALL accommodate "NAP sharing" and "NAP+NSP" deployment models.

c) The solution architecture SHOULD support Licensed and License-Exempt (LE) deployments.

d) The solution architecture SHOULD support both manual [1] and automatic [2] NSP selection.

7.1.2 Use Case Scenarios

NSP discovery and selection procedures are typically executed on a first time use, initial network entry, network re-entry, or when an MS transitions across NAP coverage areas. This subsection describes all four use case scenarios.

7.1.2.1 Use-case Scenario 1—First-Time Use without NAP/NSP Configuration Information Stored on MS

a) MS detects one or more available WiMAX NAPs.

b) MS discovers available NSPs associated with one or more NAPs.

c) MS identifies all accessible NSPs and selects an NAP and an NSP based on some preference criteria.

d) MS performs more concrete processes procedure with a NAP.

e) MS becomes authorized on the selected NSP for service subscription purposes only to create a business relationship with the selected NSP.

f) MS creates a business relationship enabling access via the selected NSP.

g) MS acquires and stores the configuration information.

7.1.2.2 Use-case Scenario 2—Initial Network Entry or First-Time Use with NAP/NSP Configuration Information

a) MS detects, using the stored configuration information, one or more available WiMAX NAPs.

b) MS discovers available NSPs associated with one or more NAPs.

c) MS identifies all accessible NSPs and, using the stored configuration information, selects or allows a subscriber to select an NSP based on some preference criteria.

---

[1] In manual selection, the user must be able to receive the information about all available NSPs, and indicate its NSP preference to the network manually.

[2] In automatic selection, the MS will automatically make the NSP selection decision based on the detected wireless environment and configuration file information without the user's intervention.

d) MS performs initial network entry procedure with a NAP that has a business relationship enabling access via the selected NSP.

In case of failure, MS reverts to Use Case Scenario 1.

7.1.2.3 Use-case Scenario 3—Network Re-entry

Network re-entry is equivalent to establishing connection with the same or another BS in a previously discovered WiMAX NAP. Scenario 3 mechanics assumes that NAP and NSP geographic coverage are synonymous in this context.

In case of failure, MS reverts to scenario 2.

7.1.2.4 Use-case Scenario 4—MS Transitions Across NAP Coverage Areas

a) MS has previously completed network entry and is in normal operation with its NSP on a WiMAX NAP.

b) MS discovers, using the stored configuration information, one or more available neighboring WiMAX NAP(s)[3].

c) MS discovers NSPs associated with one or more NAPs, which MAY include its currently authorized NSP [3].

d) Due to user movement or other confounding factor, MS elects to transition to another NAP.

e) MS identifies all accessible NSPs and, using the stored configuration information, selects an NSP based on some preference criteria.

f) MS performs network re-entry with a NAP that has a business relationship enabling access via the selected NSP. This network re-entry will involve a full authentication. Optimized handover on all other network re-entry steps is not possible.

In case of failure, MS reverts to scenario 2.

7.1.3 NAP, NSP Domains

The adopted NWG reference model enables deployments wherein an MS may encounter one or more of the following situations:

a) An Access Service Network (ASN) managed/owned by a single NSP administrative domain (also referred to as "NAP+NSP" deployment case).

b) An ASN managed by a NAP but shared by two or more NSPs (also referred to as "NAP sharing" deployment case).

c) A physical geographic region covered by two or more ASNs, representing either a "NAP+NSP" or "NAP sharing" scenario.

NOTE: "NAP sharing" is referred to the ASN deployment scenario when it has the management plane, control plane and data plane connectivity shared directly with more than one NSP; i.e. this is not the same as the roaming scenario, where multiple NSPs may be accessible via the ASN, but are accessible indirectly through one (or more) of the NSPs attached to that specific ASN.

The requirement is to enable the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN. The actual NSP selection mechanism employed by the MS may be based on various preference criteria, possibly depending on the presence on the MS of configuration information. Configuration information SHALL include:

a) information useful in MS discovery of NAP including channel, center frequency, and PHY profile,

[3] Steps b and c of Scenario 4 may occur either before or after step 4 without affecting performance.

b) information useful in MS decision mechanism to discriminate and prioritize NSPs for service selection including a list of authorized NAP(s) and a list of authorized NSP(s) with a method of prioritization for the purpose of automatic selection,

c) a list of authorized ‘share’ or ‘roaming’ affiliation relationships between authorized NAP(s) and NSP(s) and partner NAP(s) and NSP(s), with a method of prioritization for the purpose of automatic selection,

d) identity/credentials provided by NSP(s) to which the MS has a business relationship, and

e) the mapping relation table between 24-bit NSP identities and corresponding realms of the NSPs.

Configuration information may be provided on a pre-provisioned basis or at time of MS dynamic service subscription and may be subject to periodic update in a method outside the scope of this standard.

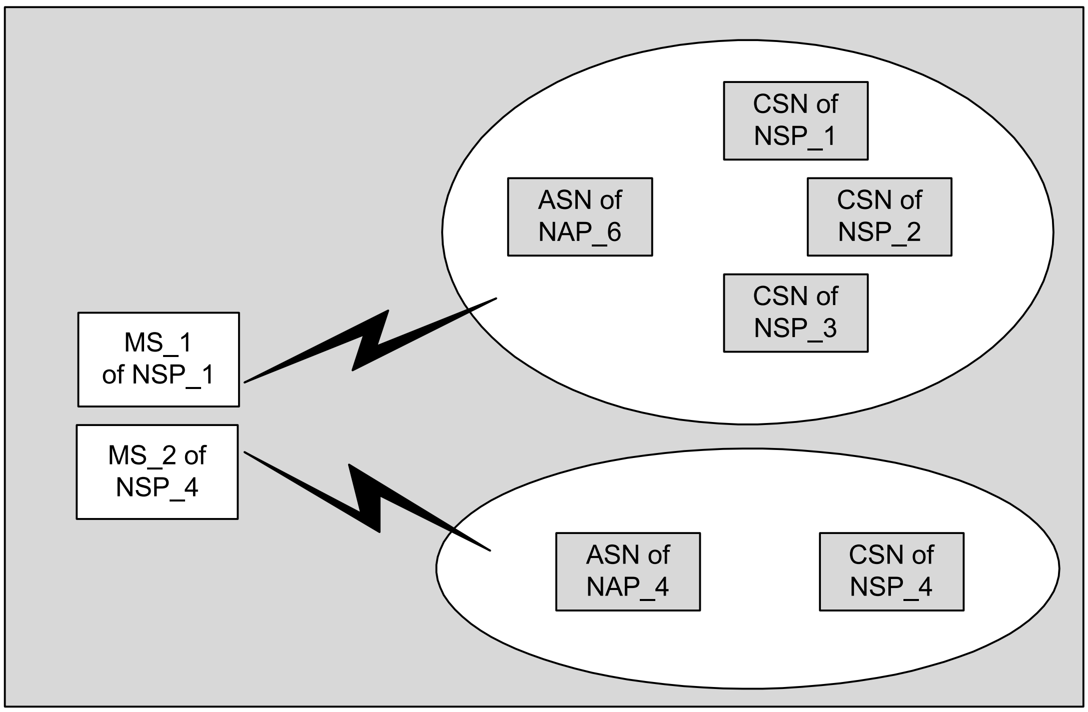


Figure 7-1 - Coverage Area with Overlapping ASNs

For example, as shown in Figure 7-1, MS_1 and MS_2 discover available NSPs and select one based on its configuration information. More specifically, MS_1 prefers to connect to ASN of “NAP_6” because it is directly affiliated with MS_1’s home NSP through NAP sharing. And, MS_2 prefers to connect to ASN of “NAP_4” because it is owned by MS_2’s home NSP (i.e., NSP_4).

There is a need for a solution framework that enables an MS to discover identities of available NSP(s) in a WiMAX coverage area, and indicate its selected NSP to the ASN. While the general method for MS selection of NSP for attachment is provided as part of Release 1.0.0, the specific mechanisms that an MS MAY use to select a particular NSP from the list of discovered NSPs are out of scope of Release 1.0.0, but would likely include reference to configuration information.

7.1.4 NAP, NSP Discovery and Selection

This subsection provides an overview of a solution for NAP, NSP discovery and selection.

The solution consists of four procedures:

a) NAP Discovery

b) NSP Discovery

c) NSP Enumeration and Selection

d) ASN Attachment

WiMAX NAP Discovery refers to a process wherein an MS discovers available NAP(s) in a detected wireless coverage area. *NSP* Access *Discovery* refers to a process wherein an MS discovers available NSP(s) in a coverage area. *NSP Enumeration and Selection* refers to a process of choosing the most preferred NSP and a candidate set of ASNs to attach, based on the dynamic information obtained during the discovery phase and stored configuration information. *ASN Attachment* based on *NSP Enumeration and selection* refers to a process wherein the MS indicates its selection during registration at ASN associated with the selected NSP by providing its identity (in the form of NAI [60]). The enumerated steps are not sequential and need not be completed in their entirety. That is, *NSP Access Discovery* and *NSP Enumeration and Selection MAY* well occur concurrent to *WiMAX NAP Discovery*. Also, there is no requirement that an MS discover ***all*** NAPs and NSPs in the available environment. An MS MAY stop the discovery process on discovery of a NAP and NSP meeting the MS *NSP Enumeration and Selection* criteria and proceed to *ASN Attachment*.

7.1.4.1 WiMAX NAP Discovery

An MS detects available NAP(s) by scanning and decoding DL-MAP of ASN(s) on detected channel(s). The 24-bit value of the "operator ID" (see 6.3.2.3.2 of IEEE Std 802.16) within the "Base Station ID" parameter in the DL-MAP message is the NAP Identifier and is used to indicate the ownership of the ASN. The value of the 24-bit "operator ID" shall be assigned as an IEEE 802.16 Operator ID by the IEEE Registration Authority[4]. Operator ID/NAP ID allocation and administration method, and field formatting are defined in IEEE Std 802.16. If information useful in MS discovery of NAP is available in configuration information, it may be used to improve efficiency of NAP discovery.

7.1.4.2 NSP Access Discovery

The NAP SHALL be served by one or more NSPs. In NSP discovery, an NSP identifier can be presented to the MS as a unique 24-bit NSP identifier. The value of the 24-bit NSP ID (i.e., NSP Identifier) SHALL be issued by a namespace authority to guarantee global uniqueness. NSP ID allocation and administration are managed by the IEEE RAC. NSP ID may either be a 22-bit globally-assigned ID or a combined MCC+MNC as described in ITU-T Recommendation E.212. Selection of the method used for NSP ID format is implementation specific.

During scanning, if the MS cannot deduce available NSP(s) from the NAP identifier based on the NSP Identifier Flag, detected NAP IDs, and the configuration information, then it SHOULD try to dynamically discover a list of NSPs supported by the NAP.

If the NAP and NSP are the same (i.e. there is a one-to-one relationship between these IDs), the network MAY advertise only the NAP ID and not separately present any NSP identifiers (NSP IDs). The NAP SHALL identify this case by setting the least significant 1st bit (1st LSB; the 25th bit of Base Station ID; the NSP Identifier Flag) of the Base Station ID to a value of '0'. For this case, the MS SHALL assume that the NSP ID is the same ID presented as NAP ID.

In the event that more than one NSP is served by a detected NAP, or that some regulatory or deployment requirement compels separate presentation of one or more NSP IDs, the NAP MAY transmit the NSP ID list as part of the Service Information Identity (SII-ADV) broadcast MAC management message. Also, the BS SHALL transmit the list of NSP IDs as part of SBC-RSP in response to an MS request through SBC-REQ. The NAP shall identify the presentation of a separate list of NSP IDs by setting the NSP Identifier Flag to a value of '1'

In this phase, if the list of NSP identifiers supported by a NAP does not exist in the configuration information of the MS, or the list of NSP identifiers supported by a NAP is changed, e.g. the optional NSP Change Count TLV (NSP Change Count TLV is described in the IEEE Std 802.16) obtained from the network as part of obtaining the NSP ID list, is different with that stored in the configuration information of the MS, the MS SHOULD get the list from the network. Otherwise, available NSP(s) associated with a NAP SHALL be enumerated locally based on the configuration information of the MS.

24-bit NSP identities received in this phase SHALL be mapped into realms of corresponding NSPs.

[4] The IEEE Registration Authority is a committee of the IEEE Standards Association Board of Governors. General information as well as details on the allocation of 802.16 Operator IDs can be obtained at http://standards.ieee.org/regauth.

7.1.4.3 NSP Enumeration and Selection

For automatic selection, an MS makes its NSP selection decision based on the dynamic information obtained within a coverage area (e.g., a list of available NSP Identifiers offering services), and configuration information. The specific algorithms that an MS MAY use to select the most preferred NSP from the list of discovered NSPs are out of scope of Release 1.0.0.

For manual selection, the user manually selects the most preferred NSP based on the dynamic information obtained within the coverage area. Manual selection can also enable use scenarios where a non-subscribed user wants to connect to a detected network. For example, the user wants to exercise an initial provisioning procedure with a specific NSP, or it wants to use the network on "pay for use" basis.

7.1.4.4 ASN Attachment Based on NSP selection

Following a decision to select an NSP, an MS indicates its NSP selection by attaching to an ASN associated with the selected NSP, and by providing its identity and home NSP domain in the form of NAI. The ASN uses the realm portion of the NAI to determine the next AAA hop to where the MS's AAA packets SHOULD be routed. The MS MAY use its NAI with additional information (also known as decorated NAI— described in section 2.7 of [48]) to influence the routing choice of the next AAA hop when the home NSP realm is only reachable via another mediating realm (e.g., a visited NSP). For example, as shown in Figure 7-2, MS_1 uses a normal/root NAI (i.e., user-name@NSP_1.com) as the AAA packets can be directly routed to the AAA server in NSP_1. Whereas, MS_2 needs to construct a decorated NAI (e.g., NSP_4!user-name @NSP_1.com) as the AAA packets cannot directly be routed to the home NSP (i.e., NSP_4). The specific use of realm is defined in section 7.3.7.

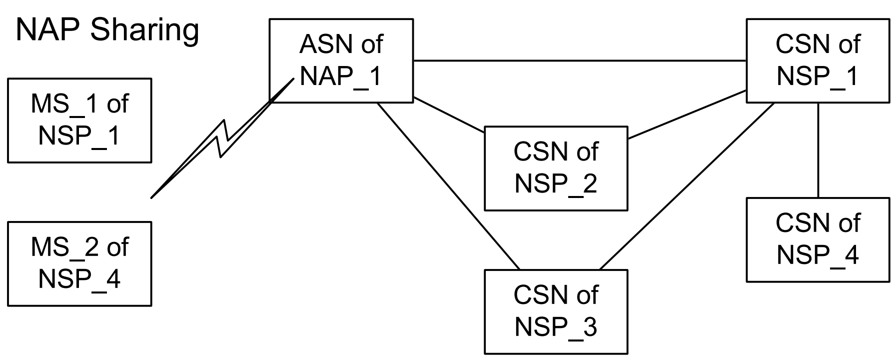


Figure 7-2 - Deployment example with NAP sharing

7.2 IP Addressing

This section defines IP addressing for both IPv4 and IPv6 protocols. IPv4 addressing details are described in Stage 2 section 7.2.1 and IPv6 addressing details are described in Stage 3 section 5.11.8

7.2.1 IPv4 address Management

IP address allocation refers to the Point of Attachment (PoA) address delivered to the MS. The discussion below refers primarily to allocation of Dynamic IP addresses. From the perspective of the MS, for MS that do not support Client MIP, DHCP [11] is used as the mechanism of dynamic IP address allocation. The home CSN may employ alternate techniques such as IP address assignment by a AAA server and deliver it to the MS via DHCP. Details of such alternate mechanisms for IP address allocation are out of scope of Release 1.0.0. These alternate techniques MAY include allocation of addresses between the home CSN and the ASN via AAA. Alternatives for DNS discovery include the use of DHCP or the use of Mobile IP extension as defined in IETF draft-ietf-mip4-gen-ext-00.txt. The following discussion focuses on the usage of DHCP to allocate PoA address to the MS. In the context of this section (and R3 Mobility Management section) PoA address corresponds to the HoA (Home Address).

7.2.1.1 Functional Requirements

Note - Considerations for overlapping IP addresses in the ASN is beyond the scope of Release 1.0.0.

a) When an MS is an IP gateway, a Point-of-Attachment IP address (PoA address) SHALL be allocated to the IP gateway. When MS is an IP host, a PoA address SHALL be allocated to the IP host.

b) For fixed and nomadic access, the PoA IP address has to be routable in the CSN and ASN and the PoA address SHALL be assigned from the CSN address space.

   For portable and mobile access, the PoA address SHALL be assigned from the address space of CSN of either Home-NSP or Visited NSP depending on:

   - Roaming agreement between Home NSP and Visited NSP.
   - User subscription profile and policy in Home NSP.

c) For fixed access, the PoA address allocated to MS MAY be static or dynamic.

d) The allocation of PoA address SHALL NOT preclude allocation of additional tunnel IP address to access specific applications (i.e., inner tunnel IP address allocated for VPN, etc.).This requirement is also applicable for overlay mobility based on MIP.

e) For billable IP services, a Point-of-attachment IP address SHALL be allocated to MS only after successful user/MS authorization. The allocated addresses SHALL be bound to the authorized user/MSs for the duration of the session. The binding MAY be maintained by an Address Allocation Server (e.g., a DHCP server or AAA server).

f) For mobile access (Proxy MIP and Client MIP), a PoA address (MIP home address, See note1[5]), routable in CSN domain SHALL be allocated to MS.

7.2.1.1.1 Fixed Access Scenario

Fixed usage scenario SHALL allow two types of PoA IP address allocations, static and dynamic. In both cases the PoA address SHALL be routable in the CSN:

a) Static IP address: static IP addresses MAY be assigned by manual provisioning in the MS or via DHCP.

b) Dynamic IP address: Dynamic IP address assignment is based on DHCP. The DHCP server SHALL reside in CSN domain that allocates the PoA address. A DHCP relay SHALL exist in the network path to the CSN.

The DHCP proxy MAY reside in ASN and retrieves IP host configuration information during access authorization (i.e. during AAA exchange).

7.2.1.1.2 Nomadic Access Scenario

Nomadic access scenario SHALL be based on dynamic IP address assignment. It SHALL be the default for nomadic access deployment scenarios. Static IP address assignment MAY be used; however details on use of static IP address assignment are beyond the scope of Release 1.0.0. Dynamic IP address assignment SHALL be based on DHCP. The DHCP server SHALL reside in home or visited CSN domains. The DHCP proxy MAY reside in ASN and retrieves IP host configuration information during access authorization (i.e. during AAA exchange).

7.2.1.1.3 Mobile Access Scenario

Mobile access scenario SHALL allow PoA IP address assignment based on DHCP for Proxy-MIP based SS/MSs. The DHCP server MAY reside in CSN domain. In this case, the PoA address (i.e., Mobile IP home address) and IP host configuration information SHALL be derived using DHCP. Alternatively, the DHCP proxy MAY reside in ASN, wherein it retrieves IP host configuration information and home address during Access Authentication AAA exchange with home NSP.

For CMIP-based mobile SS/MSs, MIP [43] based IP addressing SHALL be used instead of DHCP.

[5] Note 1: In this case, PoA=HoA

7.2.1.2 Functional Decomposition

As per WIMAX reference model, functional decomposition for MS IP address management feature SHALL be done across the following reference points:

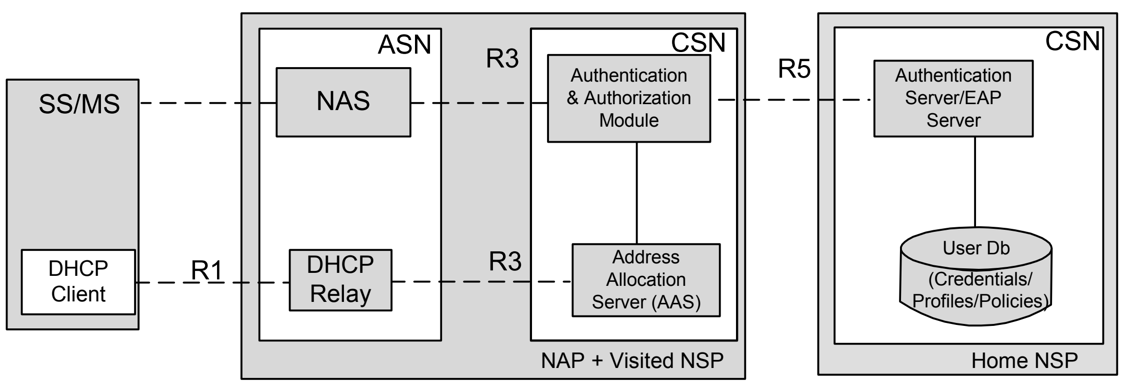
a) R1

b) R3

c) R5, if applicable

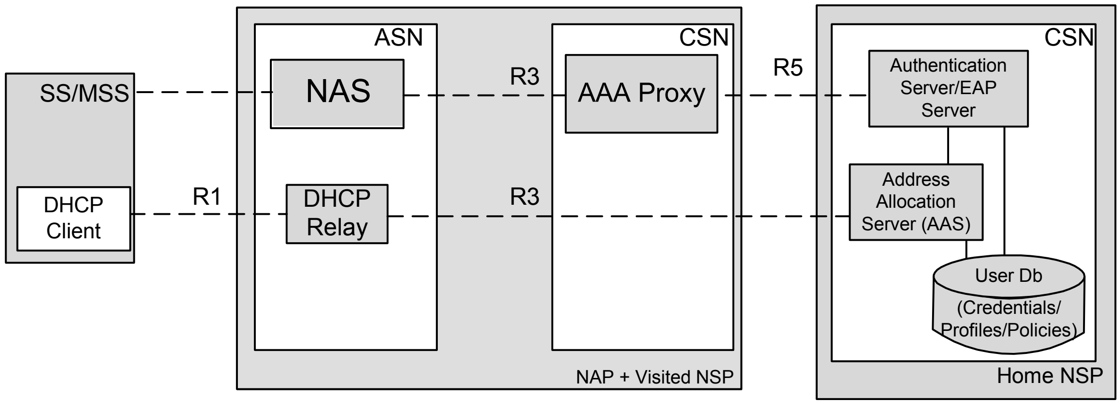
Reference points for PoA IP address are shown in Figure 7-3 and Figure 7-4:

- When PoA address is allocated by visited NSP, the Address Allocation Server, located in visited CSN, allocates PoA from its pool of addresses (as per roaming agreement with Home NSP). This case is shown in Figure 7-3.
- When PoA address is allocated by Home NSP, the Address Allocation Server, located in Home CSN, allocates PoA from its pool of addresses. This case is shown in Figure 7-4.
- In addition to the figures below, with the Ethernet case acting as a layer-2 MS, the DHCP client MAY reside in the hosts behind the MS. In this case, the MS simply forwards the DHCP messages between the hosts and Address Allocation Server.



Note: The DHCP client shown above may reside inside the SS/MS or behind the SS/MS

Figure 7-3 - Functional Decomposition for PoA from Visited NSP



Note: DHCP Client shown above may reside inside the SS/MS or behind the SS/MS

Figure 7-4 - Functional Decomposition for PoA from Home NSP

7.2.1.3 Dynamic IP Configuration Setup for Fixed and Nomadic Access Scenarios

This section defines the dynamic IP configuration setup for fixed and nomadic access. IP configuration for mobile access with in CMIP and PMIP is provided in [ref to section 7.8.1.8] and [ref to section 7.8.1.9], respectively. The following signaling flow describes IP configuration setup phase using AAA. In this flow, DHCP relay is located in the ASN and DHCP server is located in the CSN.

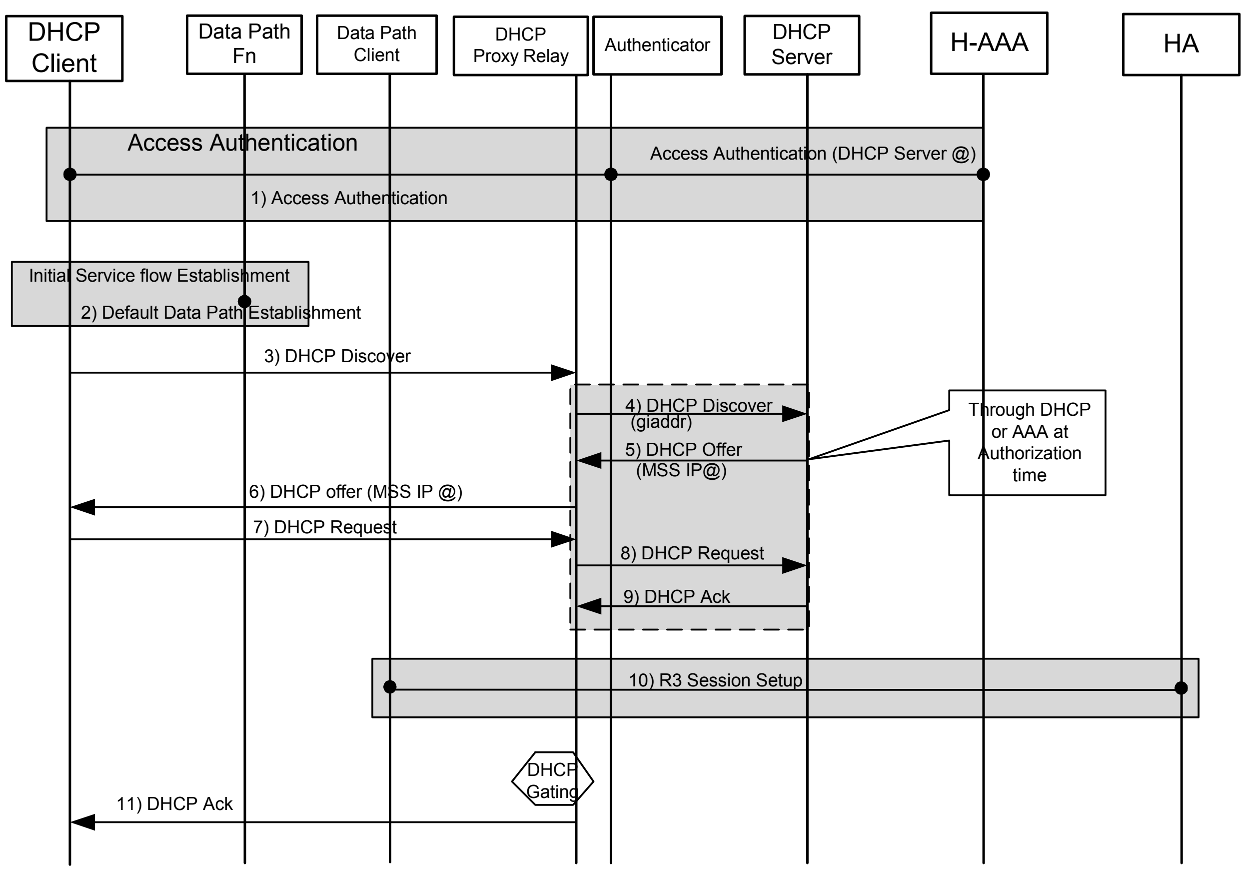


Figure 7-5 - MS IPv4 Address Management

The functional entity residing in ASN is a DHCP Proxy. However, when a PoA address is delivered via RADIUS access authentication, the functional entity in ASN is DHCP proxy.

The essential phases of the process shown in Figure 7-5, appear as follows:

1) *Access authentication*: During access level authentication— e.g., based on EAP-over-PKMv2— the network assigning the PoA address is determined. The DHCP server address is retrieved from the AAA access authentication or configured locally at the ASN. The DHCP relay in ASN is configured with the appropriate DHCP server address. The relay function in ASN can direct the DHCP messaging to the specific DHCP server selected based on the CSN membership of the MS.

2) At the completion of authentication and registration (.16e), an Initial Service flow (ISF) is established for the MS within the ASN. The ISF can be used for IP configuration of the host. DHCP messages can be transported over the ISF associated with the MS.

3–9) *IP address assignment and IP Host configuration:* After successful establishment of the ISF, the MS sends a DHCP discover message. Upon receiving a DHCP discover message the BS forwards the DHCP discover message to DHCP Proxy in ASN. The DHCP relay in ASN manages the DHCP exchange with the DHCP server.

Alternatively, the DHCP Relay in ASN can return the complete IP configuration to the MS. In this case the IP configuration including the PoA address data at the DHCP server is provided by the NSP through the access authentication AAA exchange. In the case of mobile node with PMIP, the address obtained using DHCP SHALL be the home address of MS. Dynamic Home Agent address assignment MAY be supported in compliance with RFC 4433

10) The PMIP Client and the HA complete R3 session setup.

11) *DHCP Ack*: Following step 10, the DHCP function relays the DHCP ACK to the MS.

For mobile access, detailed IP address assignment procedures for Proxy MIP and Client MIP are specified in Section 7.8.1.8 and Section 7.8.1.9.

7.2.1.4 IP Address Renewal

IP address renewal is initiated by the DHCP client in the MS.

The triggers which cause IP address renewal could be based on events such as :

- Address lease lifetime expiry threshold reached
- Inability to send packets using the address assigned
- Indication of network failure
- MS specific trigger

DHCP renewal messages are sent directly from the MS to the DHCP server without the need for relaying in the ASN since the MS obtains the IP address of the DHCP server from the siaddr address field in the DHCP Ack message during connection setup time.

7.2.2 IPv6

IPv6 in WiMAX can be operated in multiple ways. The packet convergence sublayer (CS) specified in the IEEE 802.16d/e specification is used for transport of all packet based protocols such as Internet protocol, IEEE Std 802.3/Ethernet and, IEEE Std 802.1Q. IPv6 can be run over the IP specific part of the packet CS or alternatively over the Ethernet (802.3/802.1Q) specific part of the packet CS. The operation of IPv6 over the IP specific part of the Packet CS is specified in [Reference to IETF I-D: draft-ietf-16ng-ipv6-over-ipv6cs-01] and should be referred to for understanding the basic mechanism. This section provides additional information about IPv6 operation that is WiMAX specific. IPv6 over 802.3 and 802.1Q specific parts of the packet CS are described in [REF draft-riegel-16ng-ip-over-eth-over-80216-01.txt]. It should be noted that only the IP specific part of the packet CS is a mandatory requirement and support for 802.3 and 802.1Q parts of the packet CS is optional.

7.2.2.1 Link Model

The MS and the IPv6 AR are connected at the IPv6 layer by a point-to-point link. The combination of the transport connection over the air interface (R1) between the MS and the BS and, a GRE tunnel between the BS and the IPv6 AR (R6 in the case of profiles A and C) creates a point-to-point link. Each MS is assigned a unique IPv6 prefix(es) by the AR. In the case of Profiles A and C the AR is a function at the ASN-GW. The IPv6 AR is a function within the ASN in the case of profile B. A GRE tunnel, the granularity of which is on a per-MS or a per-service flow basis is established between the BS and the AR. In the case of profile B the link between the BS and the AR is unspecified. The figure below shows the link model in profiles A and C:

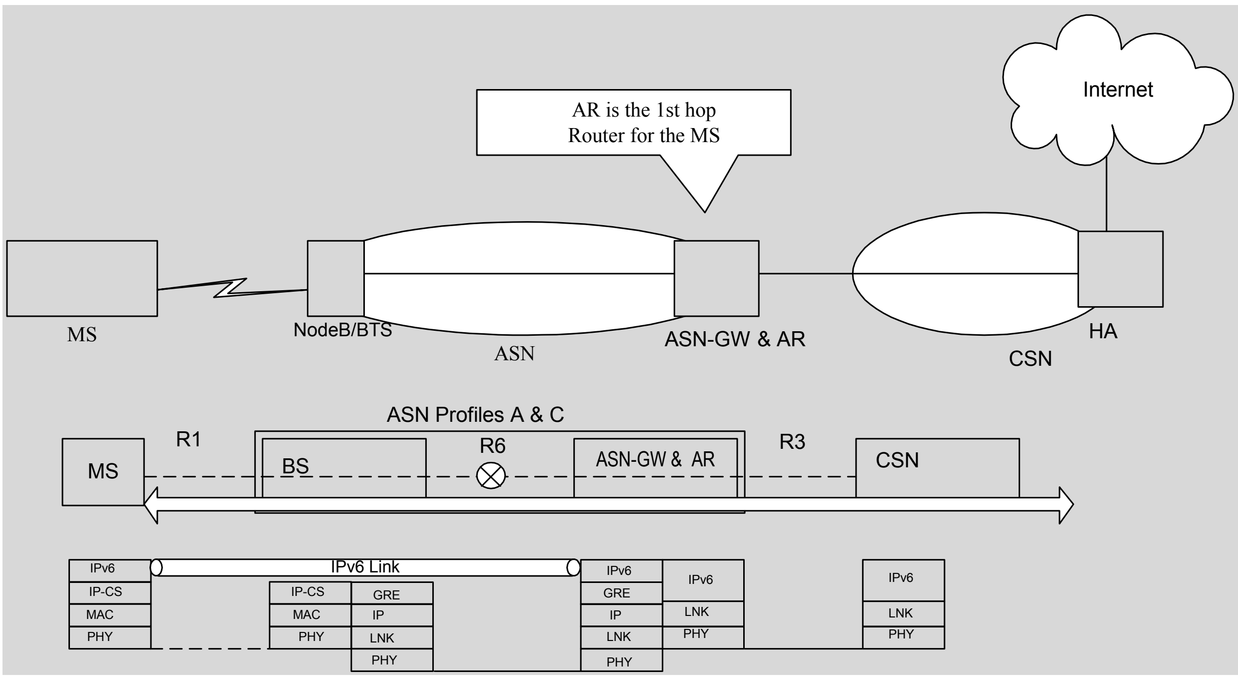


Figure 7-6 - IPv6 link model for Profiles A and C

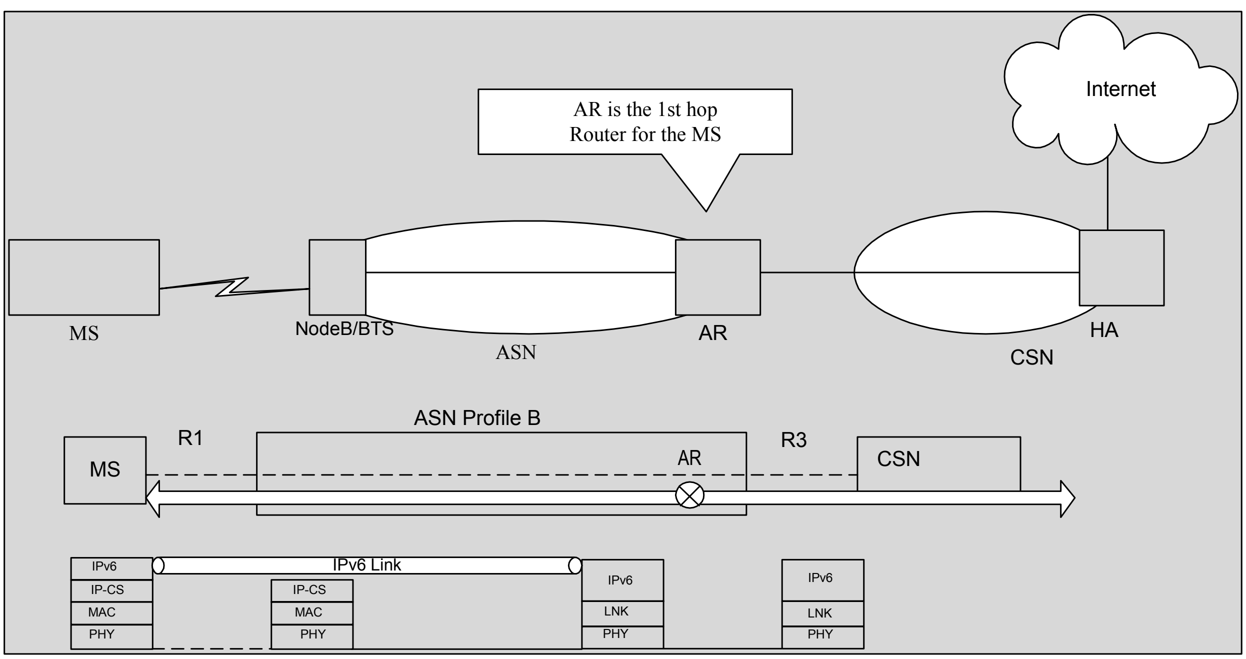


Figure 7-7 - IPv6 link model for Profile B

7.2.2.2 IPv6 Address Management

The PoA address in the context of Mobile IPv6 can be either the CoA or the HoA. The CoA is the address whose scope is at the IPv6 AR in the ASN. The HoA is the address whose scope is at the MS' home agent. Only a MIP6 MS has an HoA and a CoA. The MIP6 MS can use either the HoA or the CoA for its IP sessions. All IPv6 MS' that attach to the network and establish an IPv6 connection have a prefix assigned by the IPv6 AR. The address associated with the AR can be used by an MS for IP sessions. A MIP6 MS also uses this address to register it with the HA in the binding update message. The PoA address for an MS that does not use MIP6 is the address obtained via DHCPv6 or the address generated by stateless address autoconfiguration based on the prefix advertised to the MS by the IPv6 AR.

IPv6 address assignment requirements and procedures are detailed in the following sections:

7.2.2.2.1 MS Functional Requirement

a) For fixed/nomadic access, a MS MAY be allocated a PoA address for simple IP connectivity by either static, stateless address autoconfiguration (SLAAC) means or stateful DHCPv6 [42] assignment.

b) MS should support static, stateless or stateful [42] address assignment for home address assignment.

c) MS should support stateful address autoconfiguration [42] or stateless autoconfiguration ([16] and [30]) for CoA allocation.

d) For nomadic access, MS MAY be allocated a PoA address for IP connectivity by stateless address autoconfiguration ([16] and [30]) or DHCPv6.

e) MS SHALL use DHCPv6 [42] to determine system configuration information such as DNS servers, NTP servers, etc.

f) MS SHALL support the ability for multiple CoAs as per the description in Section 11.5.3 of [54].

g) Allocation of PoA SHALL NOT preclude the allocation of additional tunnel IP addresses to access applications (i.e., VPN).

h) For billable IP services, the PoA SHALL be allocated only after successful user/device authorization.

i) PoA SHALL be bound to user/device for the duration of the session.

j) When PoA=CoA, it SHALL always be allocated by the serving network (visited or home).

k) MS MAY use Neighbor Discovery [15] to acquire IP configuration information such as prefix, router address, etc.

7.2.2.2.1.1 Fixed Access /Stationary Networks Scenario

Fixed usage SHALL allow two types of PoA IP address allocations via static/manual configuration, DHCPv6 and stateless address autoconfiguration (SLAAC):

- Static IP address: An MS may be provisioned with a static IPv6 address. In the case of an MS operating IPv6 over IPv6CS, the IPv6 AR is located in the ASN and the address assigned to the SS is based on the prefix/subnet of the AR. In the case of IPv6 over Ethernet CS, the address pool comes from an AR that acts as the 1st hop router for the SS. An example of such an AR would be the BRAS in a DSL type of deployment.
- Stateful address autoconfiguration: Stateful address autoconfiguration is based on DHCPv6 [42]. The DHCPv6 server SHALL reside in the Visited CSN domain that allocates the PoA address. A DHCPv6 relay MAY exist in the network path to the CSN
- Stateless address autoconfiguration (SLAAC): An SS at the completion of the establishment of the initial service flow (ISF) sends a router solicitation to the all-routers multicast address. The AR in the ASN can also send an unsolicited router advertisement to the SS on completion of the ISF establishment. The AR in the ASN responds to the router solicitation with a router advertisement which contains the prefix(es) that can be used by the SS to do SLAAC. The SS SHALL perform DAD on the address that it autoconfigures.

7.2.2.2.1.2 Nomadic Access Scenario

Nomadic access SHALL allow two types of PoA IP address associations.

- Stateful address autoconfiguration: Stateful address autoconfiguration is based on DHCPv6 [42]. The DHCP server SHALL reside in the Visited CSN domain that allocates the PoA address. A DHCP relay SHALL exist in the network path to the CSN.
- Stateless address autoconfiguration: The SS/MS sends a router solicitation to the all-routers multicast address at the completion of the establishment of the ISF. The AR in the ASN responds with a router advertisement which includes the prefix(es) that can be used to autoconfigure an address. The MS SHALL perform DAD on the address that it autoconfigures. The AR should also send an unsolicited router advertisement to the MS at the completion of the establishment of the ISF.

7.2.2.2.1.3 Portable, Simple and Full-Mobility Access Scenario

Mobility (R3 mobility) in the case of IPv6 is enabled via Mobile IPv6. IPv6 in Release 1.0.0 is an optional feature. Mobile IPv6 is hence an optional feature as well. Mobile IPv6 in Release 1.0.0 is as per RFC 3775. Mobility service requires the MS having a home address (HoA) and at least one care-of-address (CoA). Both addresses are globally routable. CoA is the address whose scope belongs to the AR in the ASN. The HoA is the address the scope of which is at the MIP6 Home Agent. Address assignment is via stateful and SLAAC means. The HoA may also be statically configured at the MS. The CoA address allocation occurs as follows:

- SLAAC: An Initial Service flow (ISF) is established on completion of .16e Registration by the MS. The MS sends a Router solicitation to the AR. The AR in the ASN responds with a router advertisement (RA) which includes the prefix(es) that enable the MS to autoconfigure an address. The AR should also send an unsolicited RA on completion of the establishment of an ISF for an MS.
- Stateful address autoconfiguration: The MS acquires an address from the ASN via DHCPv6. DHCPv6 is initiated only after the establishment of the ISF.

The HoA for an MS is assigned as follows (RFC 3775 and related IETF standards):

- Stateless DHCP : During initial access authentication, the Home AAA determines the MS is authorized for MIP6 service and sends the bootstrap parameters required by the MS in the Access Accept message to the visited AAA in the ASN. The ASN inserts the MIP6 bootstrap parameters which include the address of the HA, the home link prefix or the HoA in the stateless DHCPv6 server in the ASN. On completion of the establishment of the ISF, the MS sends a DHCPv6 query to the DHCP server in the ASN and receives the MIP6 bootstrap parameters. If the MS receives the Home link prefix, the MS does SLAAC to configure the home address. If the DHCP response includes the HoA then the MS uses the HoA in the binding update to the HA. If the Home AAA does not provide either the home link prefix or the HoA, the MS can send a binding update to the HA with the HoA set to the unspecified address. In such a case the HA will assign the MS an HoA in the binding Ack.

7.2.2.2.2 Functional Decomposition

As per WIMAX reference model, functional decomposition for MS PoA IP address management feature SHALL be done across the following reference points:

a) R1

b) R3

c) R5 if applicable

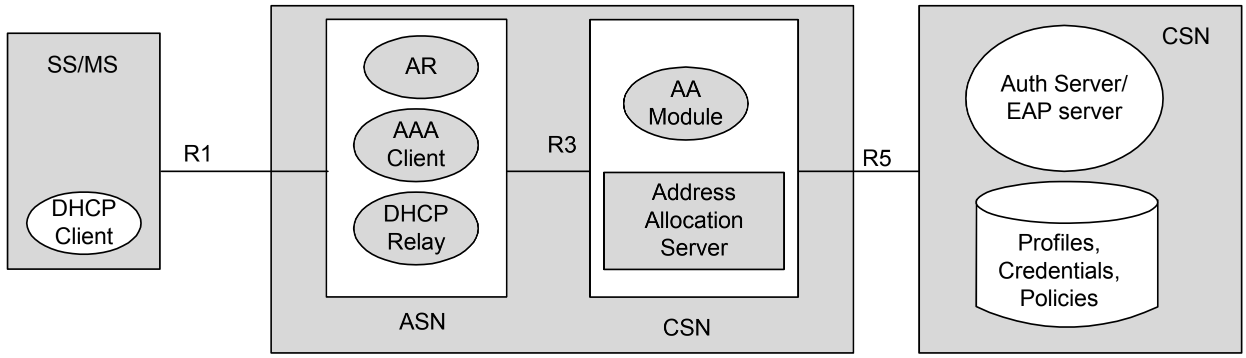


Figure 7-8 - Stateful MS IPv6 Address Management

There are two methods for address allocation:

- The PoA address MAY be allocated by the Address Allocation Server in the Serving Network [42]. This could be in the home network if the device is not roaming or in the visited network if the device is roaming (as per roaming agreement with the Home NSP).
- The PoA MAY be derived using SLAAC. The CoA prefix belongs to the address range assigned to and managed by the V-NSP.

The link-local address is always autoconfigured by the MS as soon as the IPv6 radio bearer is established. Link-local address is formed by using the MS MAC address and the well-known link-local prefix, as described in [15] and [16]. The MS SHALL perform duplicate address detection on its link-local address [16]. If later the MS autoconfigures a CoA by combining the same interface identifier it used for link-local address with an advertised prefix, the MS doesn't need to perform duplicate address detection process for such address. The MS will use its link local address as source address in any IPv6 datagrams that it sends before it has acquired a global address.

7.2.2.3 IP Address Renewal

An MS that is assigned an address via DHCPv6 should renew the address when the lease lifetime nears expiry. The MS triggers DHCP renewal and the process is as per [42].

If an MS has an address that is acquired via SLAAC, the MS needs to renew the address by sending a neighbor solicitation to the AR.

7.2.2.4 DNS discovery

The MS can discover the address of the DNS via either one of the following methods:

- DHCPv6
- Well known DNS address
- Address of the DNS server in the router advertisement

7.3 AAA Framework

The WiMAX AAA framework is based on IETF specifications, in particular on [23] and [24]. The term AAA is used to refer to the AAA protocols, RADIUS or Diameter.

The AAA framework provides the following services to WiMAX:

- Authentication Services. These include device, user, or combined device and user authentication.
- Authorization Services. These include the delivery of information to configure the session for access, mobility, QoS and other applications.

- Accounting Services. These include the delivery of information for the purpose of billing (both prepaid and post paid billing) and information that can be used to audit session activity by both the home NSP and visited NSP. Accounting is described in section 7.5.

7.3.1 Functional Requirements

The following functional requirements are considered:

a) The AAA framework SHALL support global roaming across WiMAX operator networks, including support for credential reuse and consistent use of authorization and accounting.

b) The AAA framework SHALL support roaming between home and visited NSPs.

c) The AAA framework SHALL be based on use of RADIUS or Diameter in the WiMAX ASN and CSN. Where applicable, an Interworking gateway SHALL translate between either of these Diameter and RADIUS protocols. As well an interworking function maybe required for translating between one of these protocols and a legacy domain-specific protocol.

d) The AAA framework SHALL be compatible with the AAA 3-party scheme — with an MS as a "Supplicant," "Authenticator" in ASN, and an AAA backend as an "Authentication Server."

e) The AAA framework SHALL be compatible with AAA authorization requirements as per [27].

f) The AAA framework SHALL accommodate both Mobile IPv4 and Mobile IPv6 Security Association (SA) management.

g) The AAA framework SHALL accommodate all the scenarios of operation from fixed to full mobility as defined in WiMAX Forum Stage 1 document [79].

h) The AAA framework SHALL provide support for deploying MS authorization, user and mutual authentication between MS and the NSP based on PKMv2.

i) In order to ensure inter-operability, the AAA framework SHALL support EAP-based authentication mechanisms that MAY include but are not limited to the following: passwords or shared secrets, Subscriber Identity Module (SIM), Universal Subscriber Identity Module (USIM), Universal Integrated Circuit Card (UICC), Removable User Identity Module (RUIM), and X.509 digital certificates.

j) AAA framework SHALL provide appropriate support for policy provisioning at ASN or CSN, for instance by carrying policy related information from AAA server to ASN or CSN.

k) The AAA framework SHALL support dynamic change of authorization updates e.g. as described in [48]. This information includes but not limited to the identity of the visited network, and the location of the MS as known by the ASN.

l) The AAA framework SHALL be capable of providing the Visited CSN or ASN with a "handle" that represents the user without revealing the user's identity. This handle MAY be used by entities external to the Home CSN for billing and for enforcement of service level agreements.

m) In order to support some applications such as dynamic authentication, the AAA framework MAY be required to maintain session state. In the case of RADIUS [23] (a stateless protocol) the maintenance of session state is an implementation detail.

7.3.2 Reference Point Security

In order to ensure end-to-end security of the NWG architecture, security of each reference point must be considered. Privacy, authentication, integrity and replay protection must be ensured either at the lower layers (phy, mac, or network layer) or at the higher layers. Security at the lower layers comes in the form of a secure channel that can be utilized by any one of the signaling protocols and data traffic running above it.

It should be noted that the lower layer security and the higher layer security are complementary. Absence of one should be compensated by the presence of the other. At times both may be present. Lower layer security between two end points can be a substitute for the higher layers that terminate on the same end points. If the end points are different, the substitution may not apply. For example, a secure channel between the BS and the ASN GW alleviates the need to secure any R6 signaling, but pass-through R2 signaling cannot rely on this security.

Deployments must be aware of the necessity and availability of layered-security for each reference point. This section provides a guideline to deployments.

R1 – The 802.16 primary management connection over R1 is authenticated, integrity and replay protected at the IEEE 802.16 MAC layer upon successful Device Authentication. All the subsequent R1 messaging over these connections can rely on this lower-layer cryptographic security. On the other hand, transport connections may not be crypto-protected at all. For that, any signaling protocol and data traffic that run above these connections shall provide their own security when necessary. (Note: Although enabling security on the transport connections is optional, it is recommended that deployments take advantage of this feature).

R2 - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are insecure and the signaling protocols and data traffic shall provide their own security when necessary.

R3 - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are insecure and the signaling protocols and data traffic shall provide their own security when needed. Examples: Mobile IPv4 using authentication extensions, RADIUS using authentication attribute, etc.

R4 - This reference point has an end-to-end secure channel, including privacy. The channel security may be implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R4 end points, or be on-path between the two to ensure end-to-end security.

R5 - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are insecure and the signaling protocols and data traffic shall provide their own security when needed. Examples: RADIUS authentication attribute, etc.

R6 - This reference point has an end-to-end secure channel, including privacy. The channel security may be implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R6 end points, or be on-path between the two to ensure end-to-end security.

R8 - This reference point has an end-to-end secure channel, including privacy. The channel security may be implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R8 end points, or be on-path between the two to ensure end-to-end security.

7.3.3 Functional Decomposition

RFC2904 [25], presents three models for deploying AAA framework namely, Agent sequence/model, Pull sequence/model and Push sequence/model. The models mainly differ in two aspects namely, a) how the supplicant and authentication server communicate and b) how the control information (e.g., keys, policy details) are configured into the bearer plane MSs. The [25] does not recommend one model over another. On the contrary it suggests that it is appropriate to deploy a hybrid model. A related [26] provides examples of various key applications deployed using the models defined in [25]. As per examples in the [25], the pull model is a preferred model for deploying AAA framework and other models can be mixed in when required. Pull model is recommended for AAA deployments within WiMAX networks. For more details on these models and terms like supplicant, authentication server please refer to [25].

The NAP MAY deploy an AAA proxy between the Network Access Server NAS(s) in the ASN and the AAA in the CSN in order to provide security and enhance maintainability. This is particularly the case where the ASN has many NASs and the CSN is in another administrative domain. In this case, the AAA proxy will make it easier to configure the AAA infrastructure between the NAP and the visited CSN, reducing the number of shared secrets that need to be configured and making it easier to configure the network for failover. 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. Note: This Proxy AAA is not shown in the subsequent figures in this section.

7.3.3.1 Non-Roaming Pull Model

Figure 7-9 shows the non-roaming pull model as per [25].

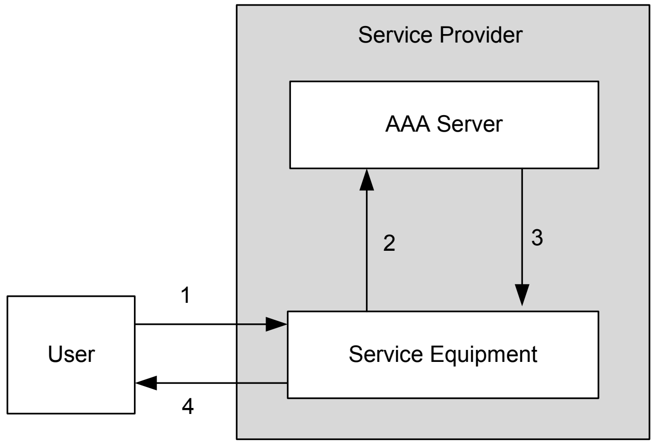


Figure 7-9 - Generic Non-roaming AAA Framework

The User (e.g., MS) sends a request to the Service Equipment (e.g., Network Access Server—NAS).

The Service Equipment forwards the request to the Service Provider's AAA Server.

Service Provider's AAA server evaluates the request and returns an appropriate response to the Service Equipment.

Service Equipment provisions the bearer plane and notifies the user that it is ready.

Figure 7-10 shows the non-roaming pull model mapped to the WiMAX non-roaming reference model.

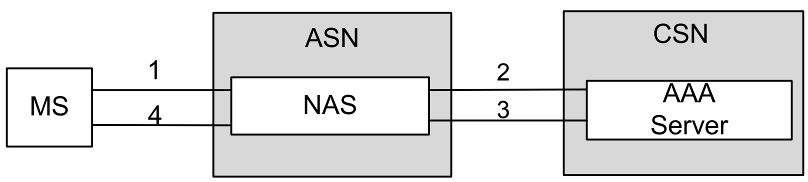


Figure 7-10 - Greenfield Non-roaming AAA Framework

For more details on WiMAX reference model, please refer to Section 6. As shown in Figure 7-10, the Service Provider is split into ASN and CSN, while the Service Equipment in the ASN becomes a NAS. The CSN hosts the AAA server whereas the ASN hosts one or more NASs.

Figure 7-11 shows the corresponding WIMAX non-roaming reference model when the CSN is belonging to an incumbent NSP whose authorization and authentication backend is not AAA protocol compliant. The incompatibility can be at the protocol level or at attributes level, etc.

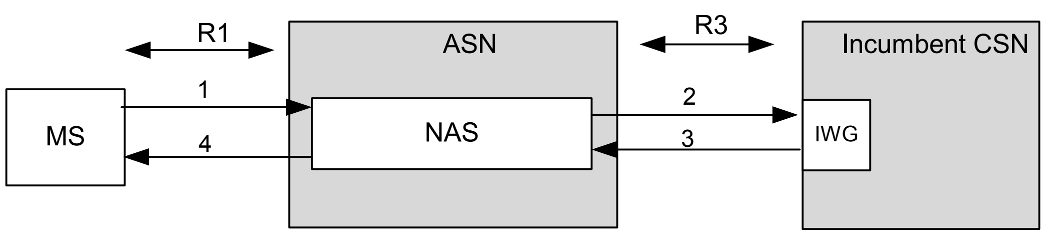


Figure 7-11 - Non AAA Compliant Incumbent Non-roaming AAA Framework

In this scenario, the CSN of an incumbent NSP needs to host an internetworking gateway (IWG) to map AAA protocols and attributes to incumbent NSP specific protocols and attributes and vice-versa Since the IWG translates the AAA protocol the Incumbent Non-roaming case is functionally identical to the Non-roaming case presented earlier.

7.3.3.2 Roaming Pull Model

Figure 7-12 shows the roaming pull model as per [25].

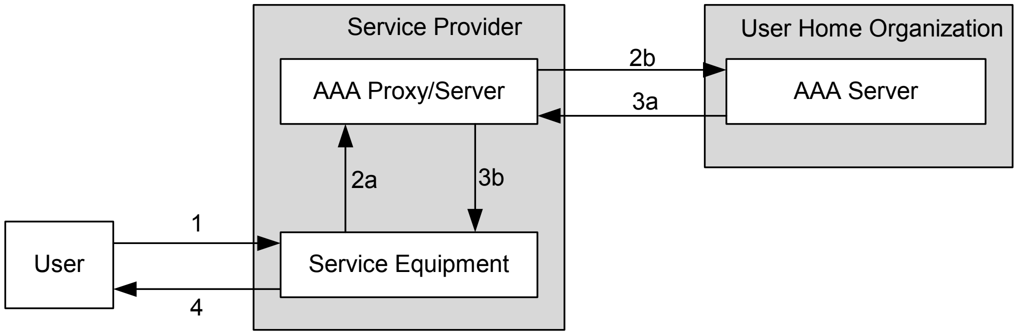


Figure 7-12 - Generic Roaming AAA Framework

Figure 7-13 shows the corresponding WiMAX roaming reference model.

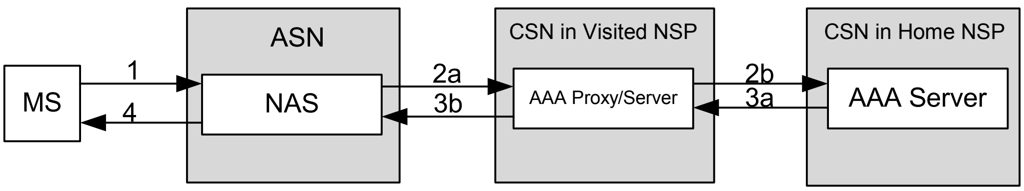


Figure 7-13 - Greenfield Roaming AAA Framework

In case of roaming deployments, optionally one or more AAA proxy/server entities exist between ASN and the home CSN.

Figure 7-14 shows the corresponding WiMAX roaming reference model when CSN is in an incumbent home NSP whose authorization and authentication backend is not RADIUS compliant. As in the non-roaming case, the incumbent home NSP will host an IWG to map the AAA protocols and attributes to incumbent NSP specific protocols and attributes, and vice-versa.

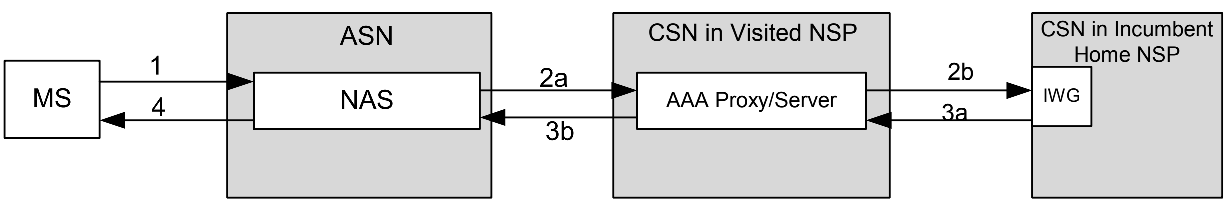


Figure 7-14 - Non AAA Complaint Incumbent Roaming AAA Framework

7.3.3.3 Decomposition of AAA in the ASN

As was shown in the above diagrams, the ASN is composed of one or more NASs. A NAS is considered as the first AAA client where AAA messages originate and authentication and authorization attributes are delivered to. It is also one source of accounting information (the accounting client may also be located in the CSN/Home Agent).

The Authentication and authorization attributes are delivered to AAA "Applications" such as, the Authenticator, mobility applications (PMIP, FA), prepaid applications, QoS applications, which collectively are assumed to live in the NAS. With respect to the implementation of the ASN, these applications MAY actually reside in different physical elements in the ASN. That is, the NAS MAY be implemented on multiple physical functional entities in the ASN.

7.3.4 RADIUS Reference Protocol Stack

The following figure describes the RADIUS Reference Protocol Stack.

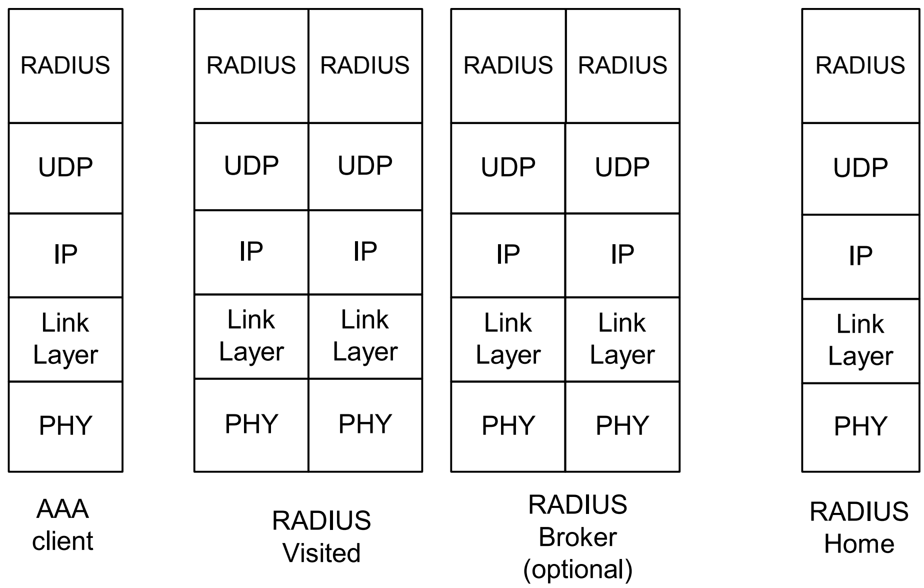


Figure 7-15 - RADIUS Reference Protocol Stack.

As shown RADIUS is based on UDP protocol and as such RADIUS protocol uses a handshake (request reply) to provide its own robustness. Retry and Failover mechanisms are left as an implementation detail.

Therefore, the WiMAX network should define a retransmission strategy that reacts to network congestion and thus does not contribute to the congestive collapse of the network.

7.3.5 Routing of AAA messages

As specified above, AAA protocols are hop by hop protocols. During operations the AAA messages SHALL be routed between the NAS and the home AAA server. In RADIUS, the routing of the messages typically depends on the NAI but MAY also depend on other attributes in the RADIUS packets. Each RADIUS based operational scenario SHOULD discuss how messages are routed.

7.3.6 AAA Security

The IETF AAA protocols are hop-by-hop secure. That is, the AAA nodes are assumed to be trustworthy.

The AAA protocols provide protection against multiple types of external threats e.g. man-in-middle attacks. In RADIUS the protocol provides a mechanism to provide integrity protection, privacy, and protection against replay attacks. This mechanism is protected by a key that is shared between the RADIUS hops.

RADIUS may also be protected using IPsec. However, IPsec is not part of the RADIUS protocol.

This specification strongly recommends to protect the reference points and interfaces between all interconnected RADIUS client, proxy and server entities; however, the decision on a specific protection method remains a deployment-specific decision.

RADIUS uses a number of data stores. These include the user's identity store, policy stores, and an accounting store that contains accounting information collected for a period of time. These stores must be secured and maintained. The procedures for provisioning, maintaining, and securing these stores are not part of this specification.

7.3.7 Authentication and Authorization Protocols

IEEE 802.16-2004 October 2004, and IEEE 802.16e-2005 March 2006 specify PKMv1 and PKMv2 with Extensible Authentication Protocol (EAP) for user authentication and MS authorization. PKMv1 provides support for only Device Authentication whereas PKMv2 provides a flexible solution that supports device and user authentication between MS and home CSN.

In the architecture specified within this document, authentication and authorization must be based on EAP (Extensible Authentication Protocol, compliant to [52]). In order to work with EAP, IEEE Std 802.16e PKMv2 must be used between MS and ASN. Within the ASN, Intra ASN security describes additional steps to transfer EAP messages and keys within the ASN entities. Between AAA server and authenticator in ASN, EAP runs over RADIUS [49].

The AAA framework used for network access authentication and authorization can transparently support different EAP methods. However, all EAP methods

- must fulfill the requirements to EAP methods specified in 802.16e for PKMv2 (e.g. those related to [81]),
- must generate MSK and EMSK as required by [52], and
- have to be chosen to support the provisioned credential types (details of allowed credential type mappings to specific authentication modes (user/device/user and device) and the location of the EAP server (ASN/Visited CSN/home CSN) are provided as part of the WiMAX Stage-3 specifications.

The different credential types supported in WiMAX network access authentication and authorization are listed in Table 7-1.

Table 7-1 - Credential Types for User and Device Authentication

Credential	Instances	Description
SUBC	0-1	The Subscriber Root Key (SUBC) is used to authenticate the subscriber. The size of the SUBC is EAP-method specific. The SUBC is also known by the HAAA. This is a long term key. If device-Only authentication is performed, then the SUBC need not be provisioned. The SUBC must be stored securely and is never transported from the user or the HAAA.
Device-Cert	1	Private/Public Certificate based keys used to authenticate the device. The certificate conforms to X.509. This is a long term credential. The Private/Public Certificate based keys are configured at the device. The private key must be stored securely and is never transported outside the device.
Device-PSK	0-n	Preshared Key (PSK) used to authenticate the device. The PSK is also provisioned at the realm responsible for authenticating the device. There may be a PSK provisioned for each realm or PSK maybe shared by more then one realm. The later case should be avoided since sharing of the PSK increase security risk. The PSK is indexed by a NAI used during the EAP authentication. This PSK must be stored securely.

The provisioning of such credentials is not in scope of this document.

7.3.7.1 User Authentication

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 (e.g. over R6 reference point) 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.

Figure 7-15 illustrates the layering of user/Device Authentication protocols.

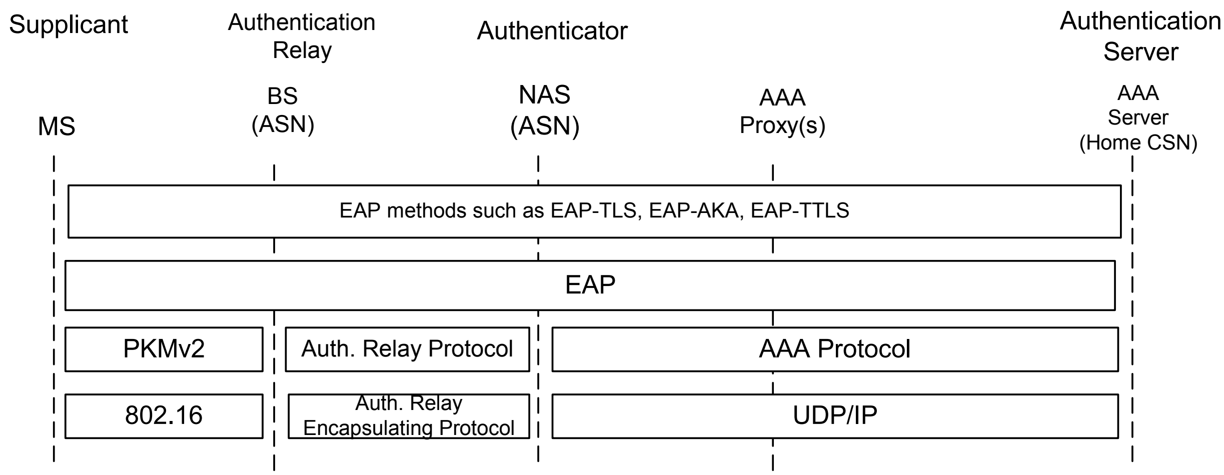


Figure 7-16 - PKMv2 User Authentication Protocols

7.3.7.2 Device Authentication

EAP must be used for Device Authentication. The RSA-based Device Authentication modes and the no authorization mode specified in 802.16e are not supported. Only EAP-based authentication (single-EAP) and Authenticated EAP-after-EAP (double-EAP) are supported.

EAP methods used for Device Authentication must generate the MSK and EMSK key.

7.3.7.2.1 NAI (Network Access Identifier)

The network access identifier (NAI) used in WiMAX shall conform to [60]. It is used as identifier within EAP-based user and device network access authentication.

In EAP there are two instances where the identity is to be specified. This is when the mobile responds to the EAP-Request Identity message (outer-identity), and the identity specified in the EAP method itself (inner-identity). The outer-identity, as recommended by [81] and section 5.1 of [2], should be used primarily to route the packet and act as a hint helping the EAP Authentication Server select the appropriate EAP method. The outer-identity is used to populate the User-Name attribute of the RADIUS access-request message.

The inner-identity is used to identify the user, or authenticated credentials. EAP methods that provide identity hiding will transmit the inner-identity within an encrypted tunnel created by the EAP method.

In order to support identity hiding it shall be possible to carry the real identity of the MS in the inner-identity only. For the outer-identity, in this case a pseudonym is used that can be resolved to the real user identity only by the MS itself and the home CSN.

Device credentials can be either a Device-Cert or a Device-PSK. The EAP device identifier should be a MAC address or an NAI in the form of MAC_address@NSP_domain, depending on where the Device Authentication terminates.

7.3.7.2.2 Device Authentication Policy

It is assumed that MS and home CSN know the Device Authentication policy applicable for the home CSN, with regard to when the Device Authentication needs to be performed. MS should learn the Home CSN Device Authentication policy as part of the MS provisioning process. The policy may dictate not performing Device Authentication at all, performing Device Authentication only after power-on, or something else. The policy is an operator decision. A typical policy can be to perform both device and user authentication at each power on only.

Until the next time the MS powers off, user-only re-authentication may be sufficient to authorize IP access of the MS.

Upon access to the serving system, the MS must inform the system of its capability to perform the Device Authentication. Based on the local policy of the Visited ASN, the MS may be requested to perform the Device Authentication if it is capable of doing so. Alternatively, based on the local policy, the Visited CSN may grant the access bypassing Device Authentication, or refuse the service to the roaming MS.

The serving ASN does not have to know the Device Authentication policy of the Home CSN.

7.3.7.2.3 Executing User and Device Authentication

If both user and Device Authentication need to be performed separately, Double EAP Mode must be selected. This is typically the case when user and Device Authentication terminate in different AAA servers, e.g. if these are located in different CSNs. These two cases are illustrated in Figures 7-16 and 7-17, respectively. In case of joint authentication of device and user, a single EAP authentication will be performed if both user and Device Authentication terminate in the same CSN. This selection is driven by the CSN as it knows the Device Authentication policy.

If the MS negotiated double EAP mode, the ASN must perform Device Authentication. In this case, if Device Authentication terminates in the ASN, a MAC address is used as the MS identifier instead of a fully formed NAI to ensure the authentication is not forwarded to another domain.

The credentials for Device Authentication may be of the type Device-Cert, such that the ASN or CSN can locally perform verification based on the availability of an appropriate public key infrastructure. Local authentication reduces the round trip delays by not involving the CSN.

If a preshared key is used, then the MS identifier must be an NAI of the form (MAC_address@NSP_domain).

If a pre-shared key (PSK) is used, a PSK-based EAP method is used for authenticating the MS. The EAP method must run between the MS and the home CSN. The target CSN is determined from the realm portion of the MS NAI.

If the Device Authentication fails, the ASN may deny access. If Device Authentication fails at the CSN, it should notify ASN of Device Authentication failure by sending additional information.

Following a successful Device Authentication, the second EAP authentication must be engaged if user authentication is required and Double EAP Mode was selected. The first RADIUS Access-Request message generated in response to EAP/PKMv2 and sent to the home NSP must indicate successful Device Authentication to the AAA server for user authentication and must carry the authenticated MS identifier in Calling-Station-ID attribute. Additionally, a new vendor specific attribute (Authenticated_MS) is needed to convey the message that the identifier is already authenticated. It is generated and added to the AAA exchange by the Authenticator. If the home mandates Device Authentication, and the Authenticated-MS VSA is not included, that means the MS has not complied with the policy. The access should be denied by the home/visited CSN in that case.

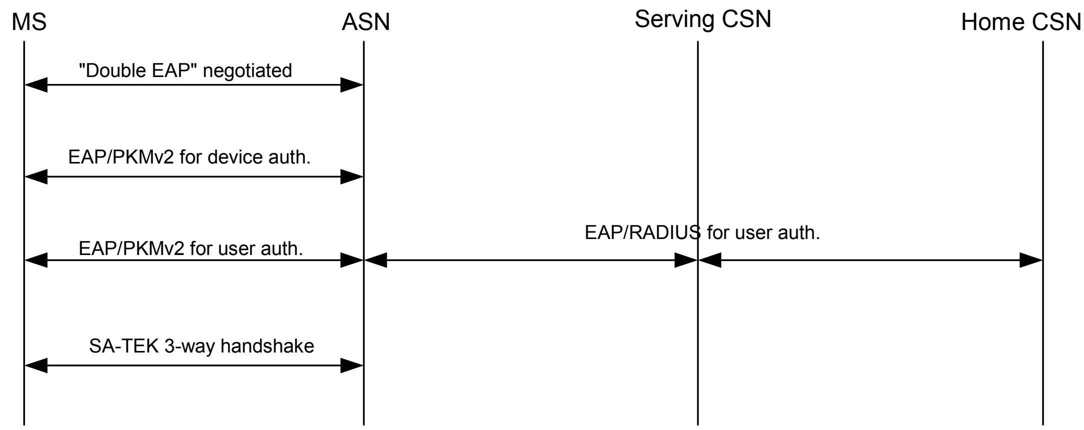


Figure 7-17 - Device Authentication Terminating in ASN, User Authentication in Home CSN

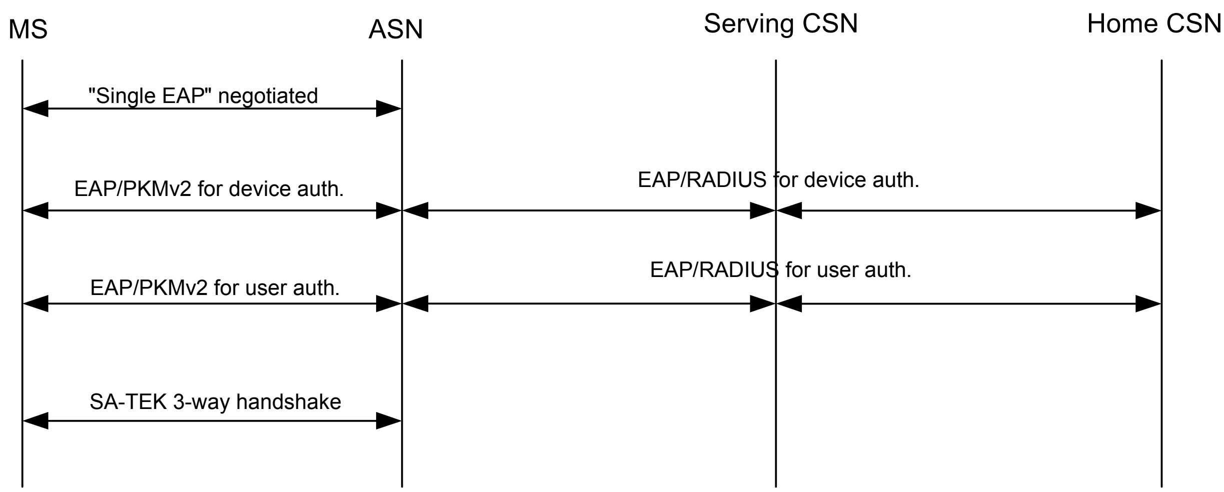


Figure 7-18 - Device and User Authentication Terminating in Home CSN (tunneled EAP)

When both the user and Device Authentication are based on PSK and terminate in the home CSN, the two will be performed jointly as one single EAP authentication. In this case, a combined identity is generated. One PSK-based EAP authentication must be performed using the computed credential. A successful authentication between the MS and home CSN implicitly authenticates both the device and the user. This optional optimization aims at reducing the authentication setup latency. The MS is assumed to be informed of the availability of this CSN feature either during the provisioning process, or throughout the negotiations phase.

In some deployments only Device Authentication is required. Device Authentication must terminate in the home CSN in this case.

7.3.8 Authentication and Authorization Procedures

7.3.8.1 PKMv2 Procedure During Initial Network Entry

Figure 7-18 illustrates PKMv2 procedure during initial network entry of the MS

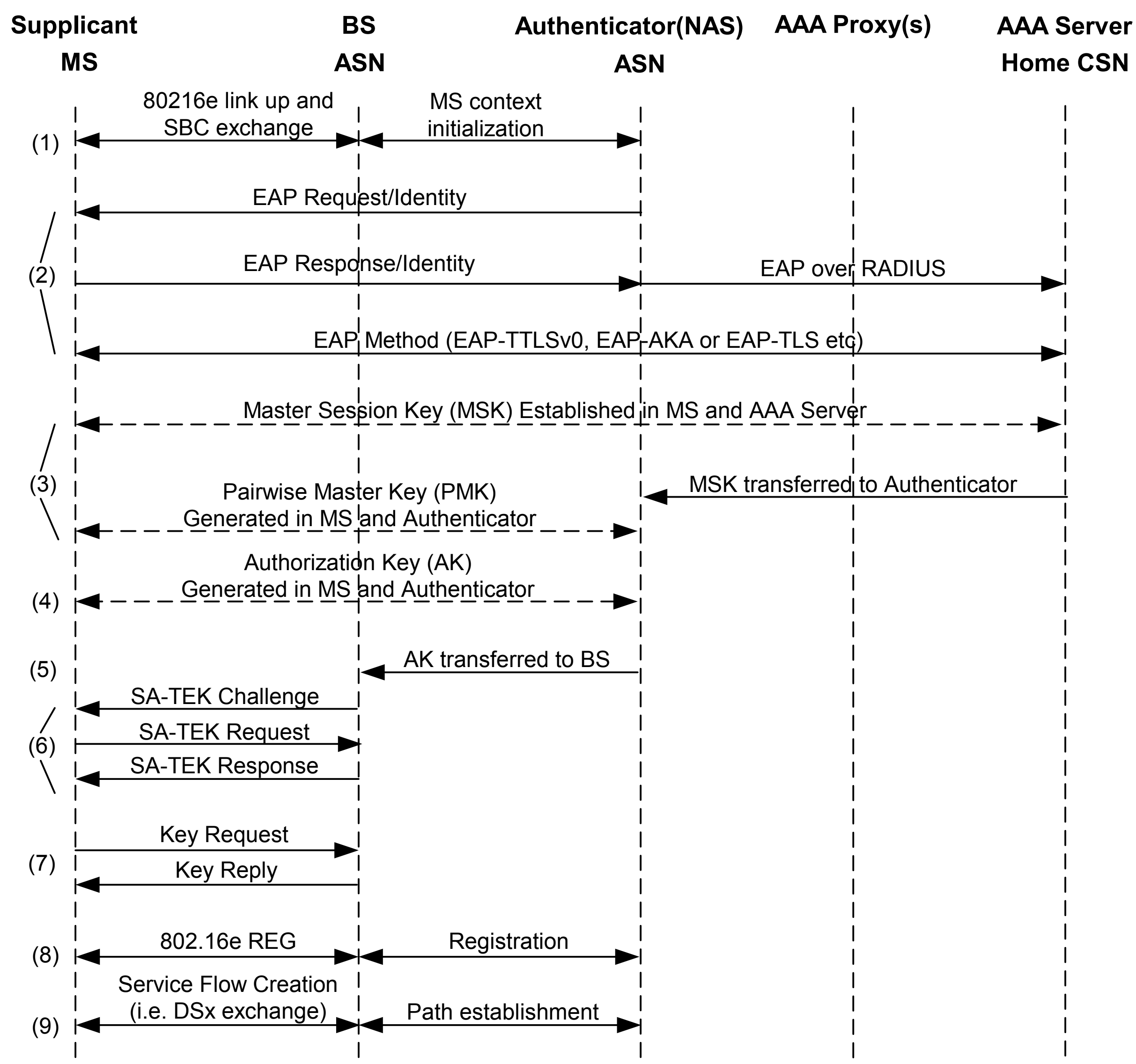


Figure 7-19 - PKMv2 Procedures

Steps for flow setup using PKMv2:

(1) Initiation of network entry according to IEEE std 802.16e

a) Upon successful completion of ranging, the MS SHALL send the *SBC_Req* message.

b) The ASN SHALL respond to the MS by sending the *SBC_Rsp*. During this SBC negotiation, the MS and ASN SHALL negotiate the PKM version, PKMv2 security capabilities and authorization policy including requirements and support for Device Authentication.

As a result of the successful establishment of an 802.16 air link between the BS and the MS, a link activation is sent (e.g. over R6) to the Authenticator. This causes the Authenticator to begin the EAP sequence.

(2) EAP Exchange

The authenticator sends an EAP-Identity request to the supplicant i.e. MS. Depending on the Authenticator location (i.e. BS or ASN-GW), the message may be transferred over the Authentication Relay protocol (across the R6 reference interface), is next encapsulated into a MAC management PDU at the BS, and is then transmitted in a EAP-Transfer message [PKM-REQ(PKMv2 EAP-Transfer)].

The supplicant receives the PKMv2 EAP-Transfer message, passes its payload to the local EAP method for processing, and then when response is received, transmits it in a PKMV2 EAP-Transfer message [PKM-REQ(PKMv2 EAP-Transfer)]. From now on the authenticator forwards all the responses from the MS to the AAA proxy, which then routes the packets based on the associated NAI realm.

(3) Shared Master Session Key (MSK) and Extended Master Session Key (EMSK) establishment

As part of successful EAP exchange in step 2), a Master Session Key (MSK) and an Extended Master Session key (EMSK) are established at the MS and the Home AAA Server. The Home AAA Server then transfers the generated MSK to the Authenticator (NAS) in the ASN. The MSK is included as a VSA in the RADIUS Accept message, which is sent over a secured path from the AAA Server to the ASN. The EMSK is retained at the Home AAA Server. From the MSK, both the MS and the Authenticator generate a PMK as per IEEE 802.16e specifications. From the EMSK, the MS and the Home AAA Server generate the mobility keys.

The authentication part of the authorization flow (and the involvement of the generic EAP layer) is now complete.

(4) Authentication Key (AK) generation

The Authenticator and the MS generate the AK from the PMK based on the algorithm specified in the IEEE 802.16e specification.

(5) AK Transfer

The Key Distributor entity in the Authenticator delivers the AK and its context to the Key Receiver entity in the Serving BS. The Key Receiver caches the AK and relevant security context related to the MS and is responsible of generating subsequent subordinate IEEE 802.16e- specified keys from the AK and its context.

(6) AK Liveliness establishment and SA transfer

To mutually prove possession of valid Security Association based on AK, the MS and the BS perform PKMv2 three-way handshake procedure.

The BS transmits the *PKMv2 SA_TEK_Challenge* message as a first step in the PKMv2 three-way handshake at initial network entry and at reauthentication. It identifies an AK to be used for the Security Association, and includes a unique challenge, i.e. BS Random, that can either be a random number or a counter.

The MS responds with the *PKMv2 SA_TEK_Req* message after receipt and successful CMAC verification of an *PKMv2 SA_TEK_Challenge* from the BS. The *PKMv2 SA_TEK_Req* message contains the number, called MS-Random, which can also be either a random number or a counter.

The *PKMv2 SA_TEK_Req* proves liveliness of the Security Association in the MS and its possession of the valid AK. Since this message is being generated during initial network entry, it constitutes a request for SA-Descriptors identifying the primary and static SAs, and GSAs the requesting SS is authorized to access, and their particular properties (e.g., type, cryptographic suite).

The BS transmits the *PKMv2 SA_TEK_Rsp* message as a third step in the PKMv2 three-way handshake. It constitutes a list of SA-Descriptors identifying the primary and static SAs, the requesting SS is authorized to access and their particular properties (e.g. type, cryptographic suite).

After the successful completion of PKMv2 three-way handshake, the MS and the BS shall start using the newly acquired AK for MAC management messages protection (by CMAC) as per IEEE 802.16e specification.

(7) Traffic Encryption Key (TEK) generation and transfer

For each SA, the MS requests two TEKs from the BS. The TEKs are randomly created by the BS, encrypted using the KEK as the symmetric secret key, and are transferred to the MS. This step is repeated for each SA.

(8) IEEE 802.16e Network Registration

After the successful PKMv2 three-way handshake completion (the MS receives *PKMv2 SA_TEK_Rsp* message from the BS), the MS SHALL send REG Request message to the BS providing ASN with the supported registration parameters. The BS SHALL respond with REG Response message. During this REG exchange, the MS and ASN negotiate network registration parameters. The BS may negotiate these parameters with the Authenticator entity in ASN GW (over R6). The completion of REG process is made known to Authenticator/ ASN GW (over R6) and it triggers Service Flow and Data Path establishment process.

(9) Service Flow Creation

The Anchor SFA entity collocated with the Authenticator starts Service Flow and the corresponding Data Path establishment process toward the BS.

The BS uses DSA-REQ/RSP/ACK MAC management messages to create a new service flow and map an SA to it thereby associating the corresponding TEKs with it.

7.3.8.2 PKMv2 Procedure During Hand-off

The PKMv2 procedure during handoff SHALL be optimized according to the following guidelines:

a) When a mobile moves within the same mobility domain, the AK is validated by signing and verifying a frame via the CMAC using the AK which is newly generated from the same PMK as long as the PMK remains valid.

b) Validating the AK is usually combined with the procedure of ranging which include 802.16e RNG-REQ and RNG-RSP with CMAC tuple.

c) Sharing TEK within a same mobility domain is possible when Handover procedure between two base stations can transfer TEK context information. If the TEK is shared among BSs, the set of BSs are considered as same security entities within a same trusted domain

7.4 ASN Security Architecture

The security architecture inside the ASN consists of the following functional entities, namely, *Authenticator*, *Authentication Relay*, *Key Distributor* and *Key Receiver*. Authenticator is defined per the Authenticator in the EAP documentation [52]. Authentication Relay is defined as the functional entity that relays EAP packets without snooping into or modifying the EAP packet via an Authentication Relay Protocol defined in Section 7.4.3 between the Authentication Relay and the Authenticator. Key Distributor is defined as the functional entity that is a key holder for both MSK and PMK resulting from an EAP exchange. The MSK is sent to the Key Distributor from the home AAA server, and the PMK is derived locally from the MSK. Additionally, Key Distributor also derives AK and creates AKID for an <MS, BS> pair and distributes the AK and its context to the Key Receiver in a BS via Context Transfer protocol. Key Receiver is the key holder for AK and is responsible for generation of IEEE 802.16e specified keys from AK.

In profiles A and C, the Authentication Relay and Key Receiver always reside in the BS. The Authenticator and Key Distributor are usually co-located. There are two deployments models: the Integrated deployment model and Standalone deployment model. In the Integrated deployment model, the Authenticator and Key Distributor are collocated with the Authentication Relay and Key Receiver and thus reside in the same BS as shown in Figure 7-20.

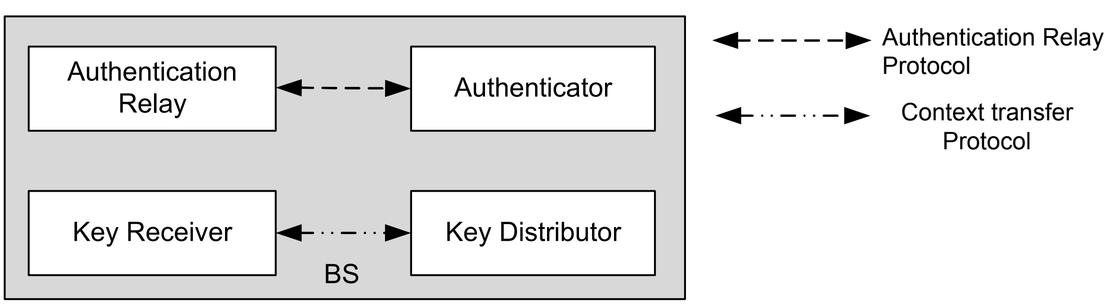


Figure 7-20 - Integrated Deployment Model

In the Standalone deployment model, the Authenticator and Key Distributor are collocated together on a physical functional entity other than the BS as shown in Figure 7-21. It is possible to think about an architecture where Authenticator and Key Distributor are not collocated but that model is not considered here.

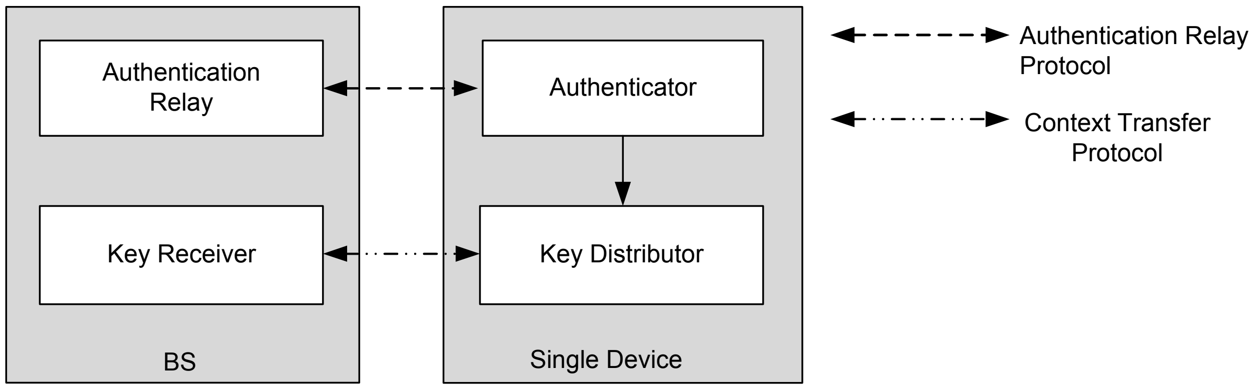


Figure 7-21 - Standalone Deployment Model

In the Integrated deployment model the Authentication Relay and Context Transfer Protocols are internal to the implementation. In the Standalone deployment model, an Authentication Relay Protocol is defined between Authentication Relay and Authenticator for relaying EAP packet as shown in Figure 7-22.

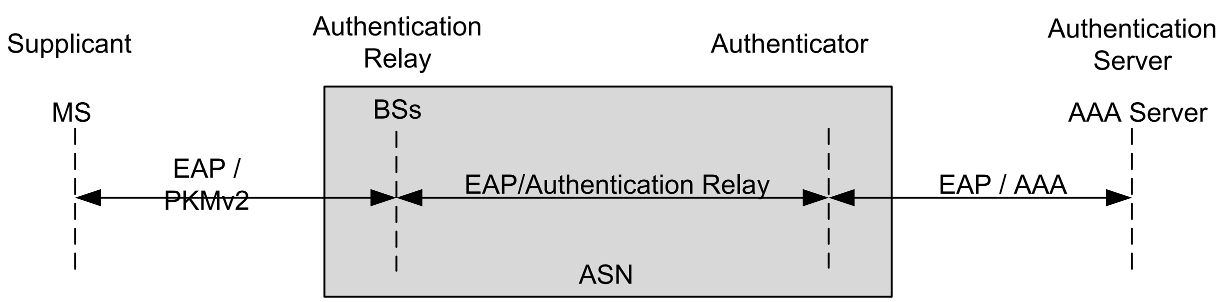


Figure 7-22 - Authentication Relay Inside the ASN

Additionally, for both Integrated and Standalone deployment models, the Context Transfer Protocol is defined to securely transfer the keying material namely AK, and it's context (e.g. CMAC_KEY_COUNT, AK Sequence Number, AKID, AK lifetime, EIK, etc.) from the Key Distributor to the Key Receiver in the target BS to which an MS does a HO as shown in Figure 7-23. Since the Integrated deployment model is a sub-set of the Standalone deployment model, this document just refers to Standalone deployment model.

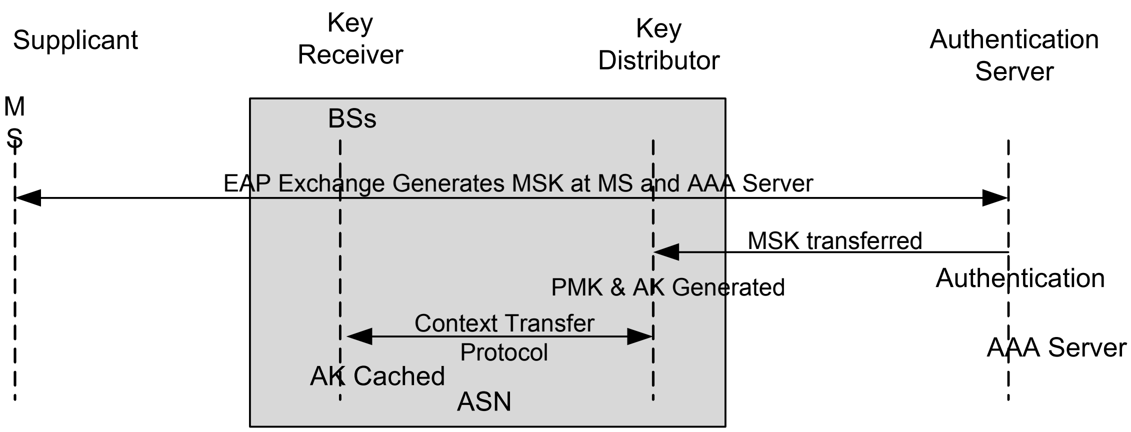


Figure 7-23 - AK Transfer Inside the ASN

7.4.1 Architectural Assumptions

The function of authenticator as mentioned in [52] and EAP keying draft, [61], is not split. All authenticator functions are implemented in one place.

The authenticator and BSs belong to the same administrative entity. Communications between them is assumed to be secure, e.g., via proper encryption and integrity protection. This implies that the authenticator and BSs share secrets required for secure communications. The mechanisms regarding how these shared secrets are established are outside the scope of this specification. In essence this document assumes that the BSs are like physical ports of an authenticator as per the EAP keying draft. Figure 7-24 shows two variants, i.e., a single or multiple BS/port(s) per Authenticator.

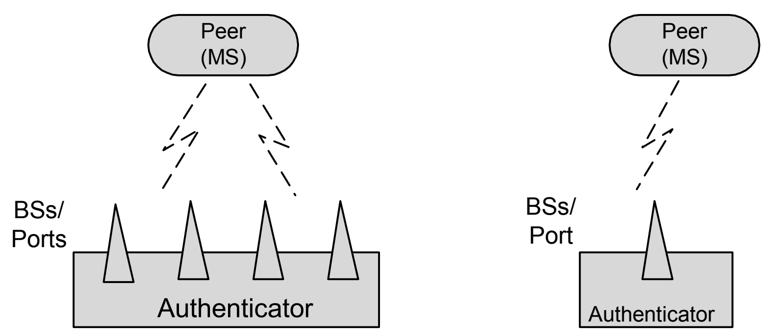


Figure 7-24 - Single Versus Multiple BS per Authenticator

7.4.2 Authenticator Domain and Mobility Domain

The architecture defines a concept of *Authenticator Domain*, which consists of one or more of BSs (stand alone or Integrated BS) that are under the control of a single Authenticator. All BSs within a given Authenticator Domain SHALL forward EAP messages to and from the Authenticator of the domain of a given subscriber. Each BS can belong to more than one Authenticator Domain.

When an MS enters a network, the BS forwards its EAP packets to the Authenticator of the given Authenticator Domain, which becomes its *Anchor Authenticator* residing within a given trusted domain. The Anchor Authenticator caches the PMK and related authentication information for MS that enter the network via one of the BSs in the domain, and retains this cached information until the MS re-authenticates with a different Authenticator (which then becomes the new Anchor Authenticator for the MS). If the MSK/PMK lifetime is expired (e.g. the MS leaves the network), the cached information SHALL be discarded. Every MS is, at a given time, anchored at exactly one Authenticator located within a NAP. Association between MS and Anchor Authenticator does not have to physically match any association between MS and other ASN functions (e.g. page controller, FA).

The architecture also defines a concept of *Mobility Domain*, which consists of a set of BSs for which a single PMK can be used to derive BS-specific AK and its contexts as the MS performs handoffs. A Mobility Domain MAY be equal to a NAP, and maps to one or more Authenticator Domains. However, as the PMK SHALL be generated by the Authenticator, the PMK CANNOT be shared across the Authenticator Domains within the mobility domain.

A *Key Distributor* belongs to a Mobility Domain, and there MAY be multiple Key Distributors in a domain, and Figure 7-25 and Figure 7-26 show the relationships between the two domains and the Authentication Relay and Context Transfer protocols in context of integrated and standalone models.

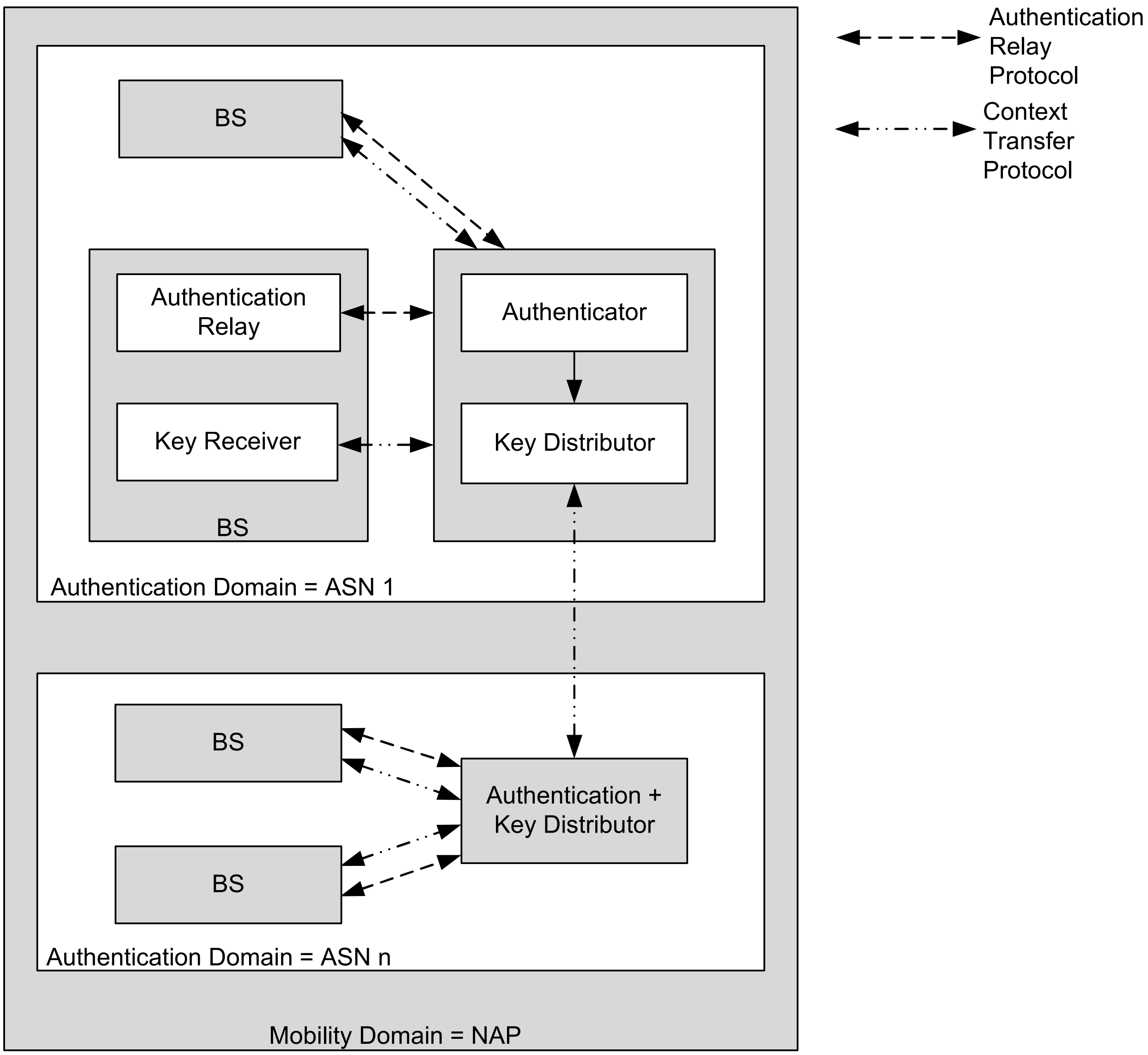


Figure 7-25 - Mobility and Authenticator Domains – Standalone Model

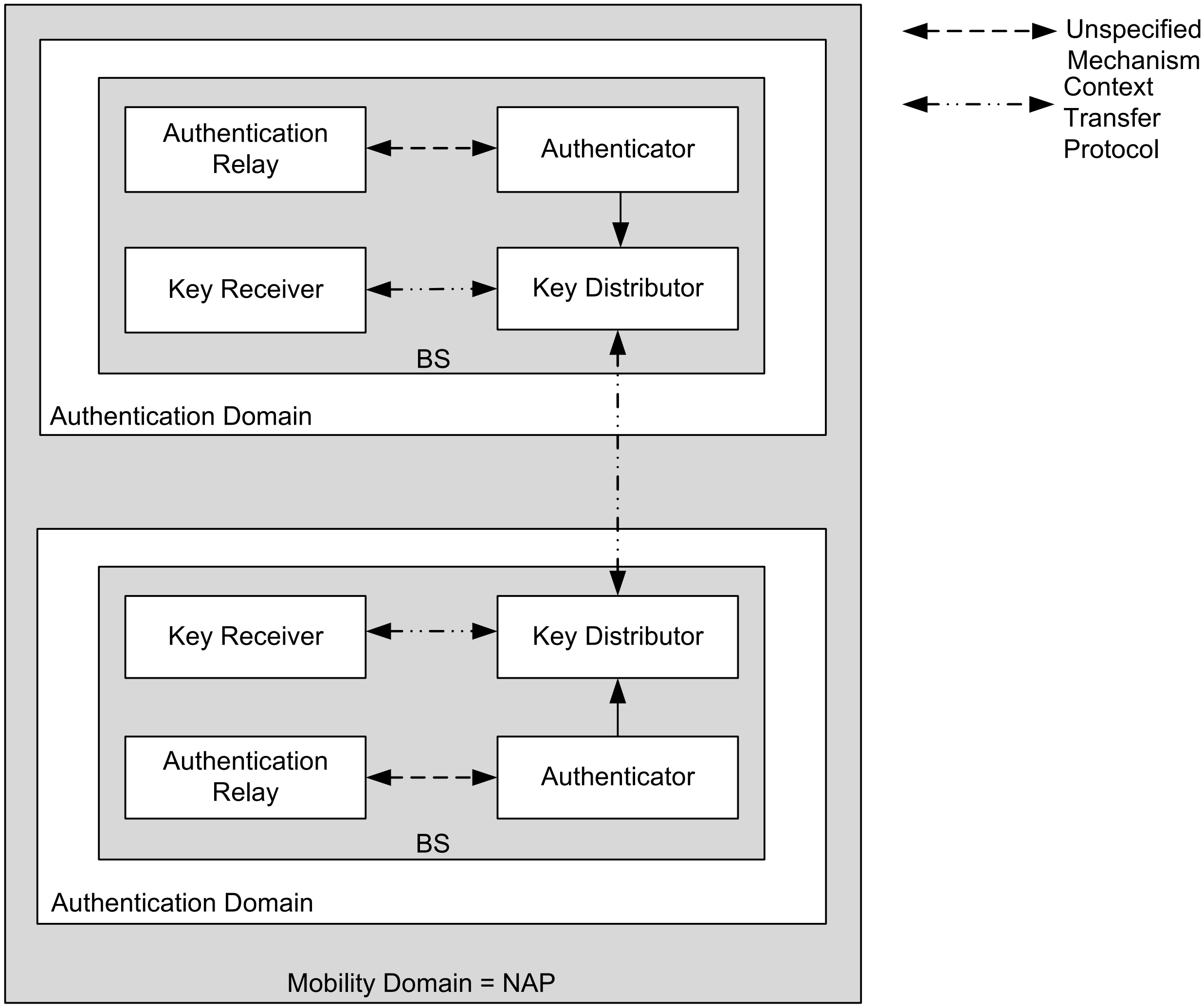


Figure 7-26 - Mobility and Authenticator Domains – Integrated Model

7.4.3 Re-Authentication Procedure

The full re-authentication EAP exchange like the initial authentication EAP exchange is done via the authenticator associated with the current serving BS. Typically, this MAY lead to a change of authenticator, if the current serving BS is associated with a different authenticator than the one which is current acting as the authenticator for the MS.

The re-authentication MAY be initiated by either:

The target authenticator: In this case, the target Authenticator autonomously initiates and executes the full EAP exchange authentication. Once the EAP exchange authentication is successfully completed, the target Authenticator becomes an Anchor Authenticator, and MAY send to the serving Authenticator an optional "RE-AUTH-IND" message including the MS identity. Thus the serving Authenticator can free resources.

Or the serving Authenticator: In this case the serving (current Anchor) Authenticator informs the target Authenticator that the full EAP exchange authentication is required. The re-authentication is initiated by a RE-AUTH-REQ message from the serving to the target Authenticator. Once the EAP exchange authentication is successfully completed, the target Authenticator sends a RE-AUTH-CONF message to the serving Authenticator so that it can free resources.

7.4.4 Authentication Relay Protocol

In the Standalone model a transport protocol is needed to exchange the EAP PDUs between the Authentication Relay and Authenticator as shown in Figure 7-27.

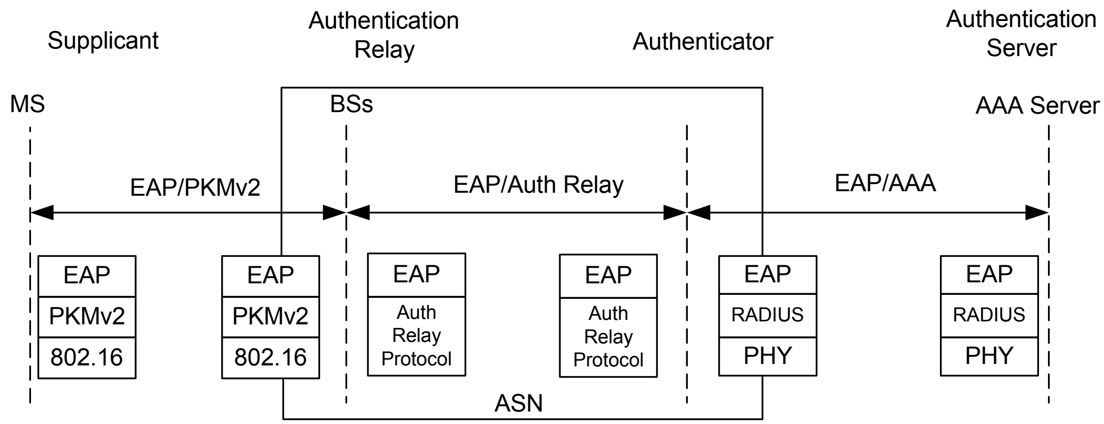


Figure 7-27 - Authentication Relay Protocol

Also, the protocol SHOULD address all the requirements placed by [52] on the EAP lower layer. Authentication Relay Protocol MAY transfer EAP.

7.4.5 Context Transfer Protocol

When the MS handoffs between BSs that belong to the same mobility domain, the key receiver in the target BSs need to be populated with AKs derived from the PMK stored in the Key Distributor if it has not expired. The Key Distributor uses the Context Transfer protocol to populate AK in the Key Receiver in the target BS to which the MS conducts HOs.

The Context Transfer protocol[6] is a two-message exchange between the Key Distributor and the Key Receiver, consisting of an optional Request message and a mandatory Transfer message. The *Context_Req* message requests a new AK from the Key Distributor, and the *Context_Rpt* message either delivers an AK, AKID, AK Lifetime, AK Sequence Number and EIK or indicates a failure. The identity of the Key Distributor is determined based on the MS identifier in the *Context_Req* message. This is depicted below:

Key Receiver → Key Distributor: *Context_Req*

Key Distributor → Key Receiver: *Context_Rpt*

The following figures show example scenarios of how the *Context_Req* and *Context_Rpt* exchange is triggered. The actual instance during a handoff when this transfer is triggered is controlled by ASN mobility management protocol.

[6] It is expected that Context Transfer Protocol primitives will be implemented in form of TLVs that will be exchanged as part of intra-ASN and inter-ASN mobility management protocols.

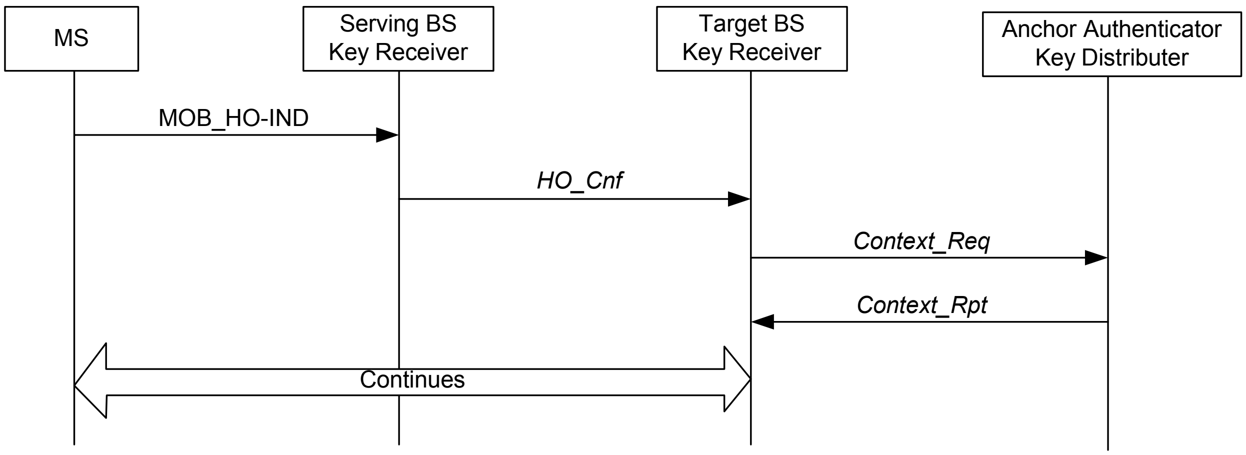


Figure 7-28 - *Context_Rpt* Triggered by MOB_HO-IND

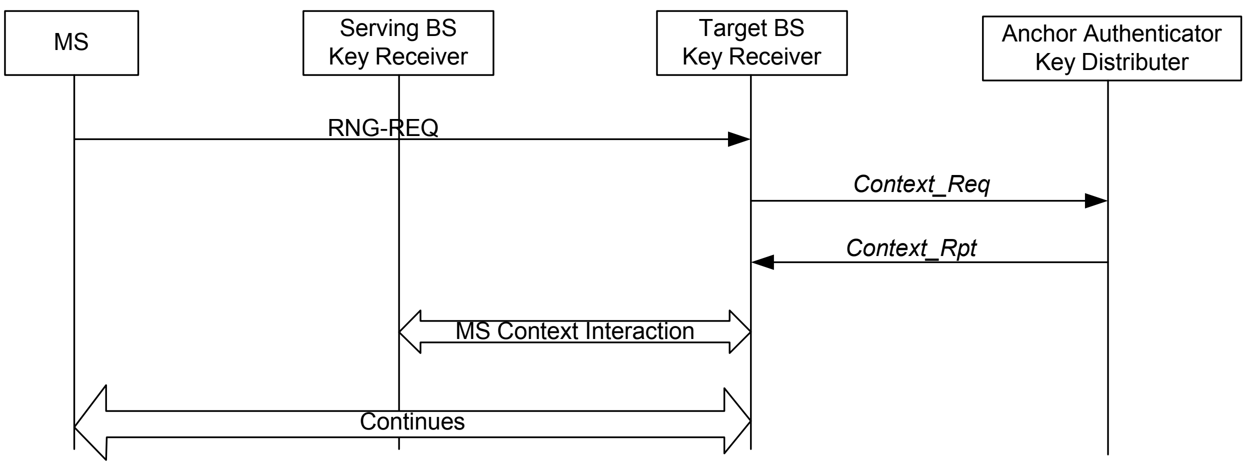


Figure 7-29 - *Context_Rpt* Triggered by RNG-REQ

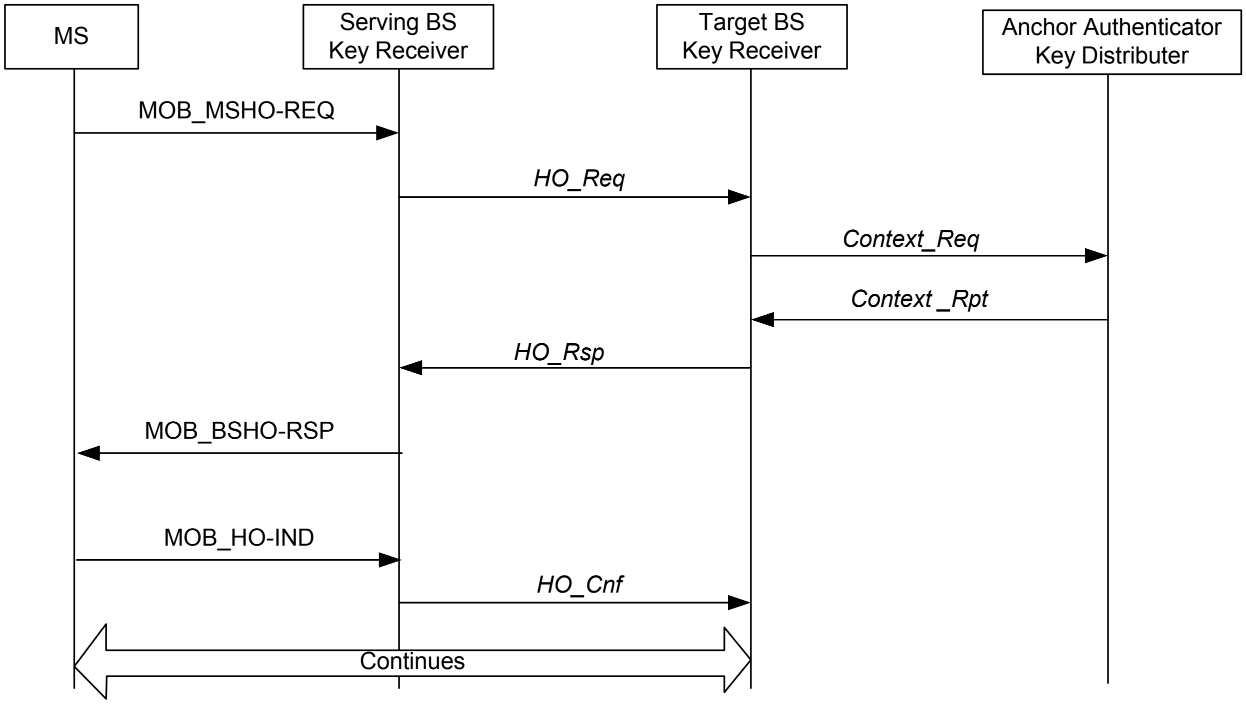


Figure 7-30 - *Context_Rpt* Triggered by MOB_MSHO-REQ

In both the Integrated model and Standalone model, AK can be transferred to a Key Receiver that is not co-located with the Key Distributor. Therefore, a secure association SHOULD exist between Key Receiver and Key Distributor in order to secure the transfer of AK, etc. AK, AKID, AK Sequence Number and EIK are derived as per 802.16e draft. The BS upon receiving the *Context_Rpt* message, decrypts the AK, AKID, AK Lifetime, AK Sequence Number, CMAC_KEY_COUNT and EIK etc., and stores them locally for future use.

Lastly, when MS does a handoff such that serving and target BSs are associated with different Key Distributors, Context Transfer protocol exchanges occur between the Key Distributors as shown in Figure 7-31. Any intermediate Key Distributors just act as relay in such a situation.

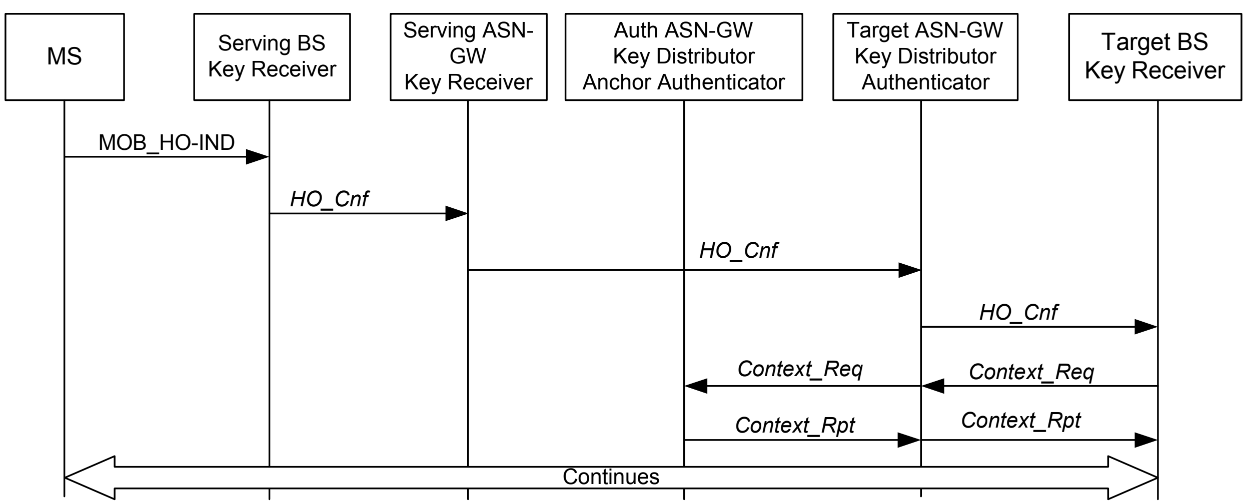


Figure 7-31 - *Context_Rpt* Triggered by MOB_HO-IND

Considering the Target BS address Anchor Authenticator, it is necessary to exchange Anchor Authenticator ID information during HO preparation between Serving BS and Target BS.

7.5 Accounting

Accounting in NWG Release 1.0.0 will be based on RADIUS. Both offline (post-paid) and online (prepaid) accounting capabilities are supported. The accounting architecture, protocols and procedures are described in the following sections.

7.5.1 Accounting Architecture

Accounting architecture is shown in Figure 7-32 below. The figure shows network elements for both offline and online services. The figure also shows the network elements for Hot-lining support and negative volume count for ASN. A description of each entity is provided in the following sections.

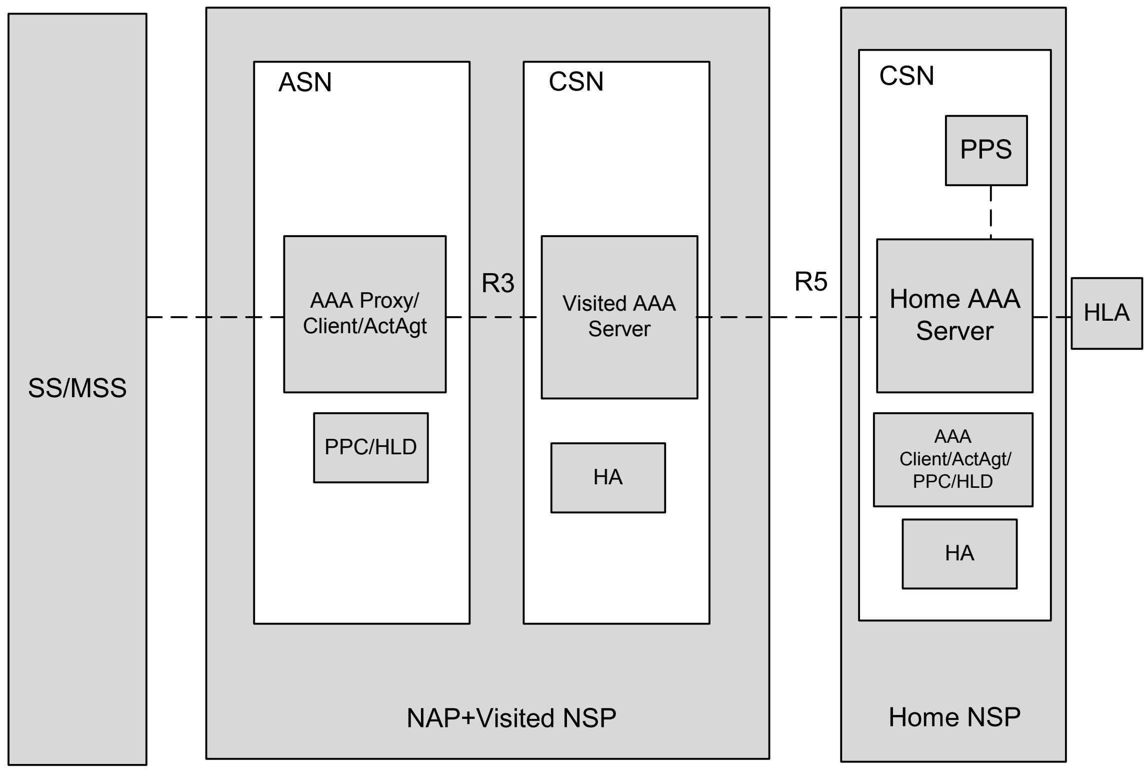


Figure 7-32 - Accounting Architecture

7.5.1.1 Accounting Primitives

7.5.1.1.1 Accounting Information Request

This primitive is sent from AAA client to accounting agent to configure accounting agent or request accounting information**.**

7.5.1.1.2 Accounting Information Report

This primitive is sent from accounting agent to AAA client to report accounting information which can be triggered by accounting information request or automatically report to AAA client per configuration.

7.5.1.1.3 Accounting Information Acknowledge

This primitive is sent from AAA client to accounting agent to acknowledge the receiving of accounting report.

7.5.2 Accounting Protocols

7.5.2.1 Negative Volume Count in ASN

The AAA Proxy/Client sends all downlink data to the Account Agent over the interface in the ASN. Any discarded or unsent data between MS and the Account Agent causes inaccurate charging, as the AAA Proxy/Client cannot account for this and subsequently causing overcharging. Negative Volume count records the packet volume of lost packets which can be measured as number of packets, octets, etc.

The following figure illustrates negative volume count protocols:

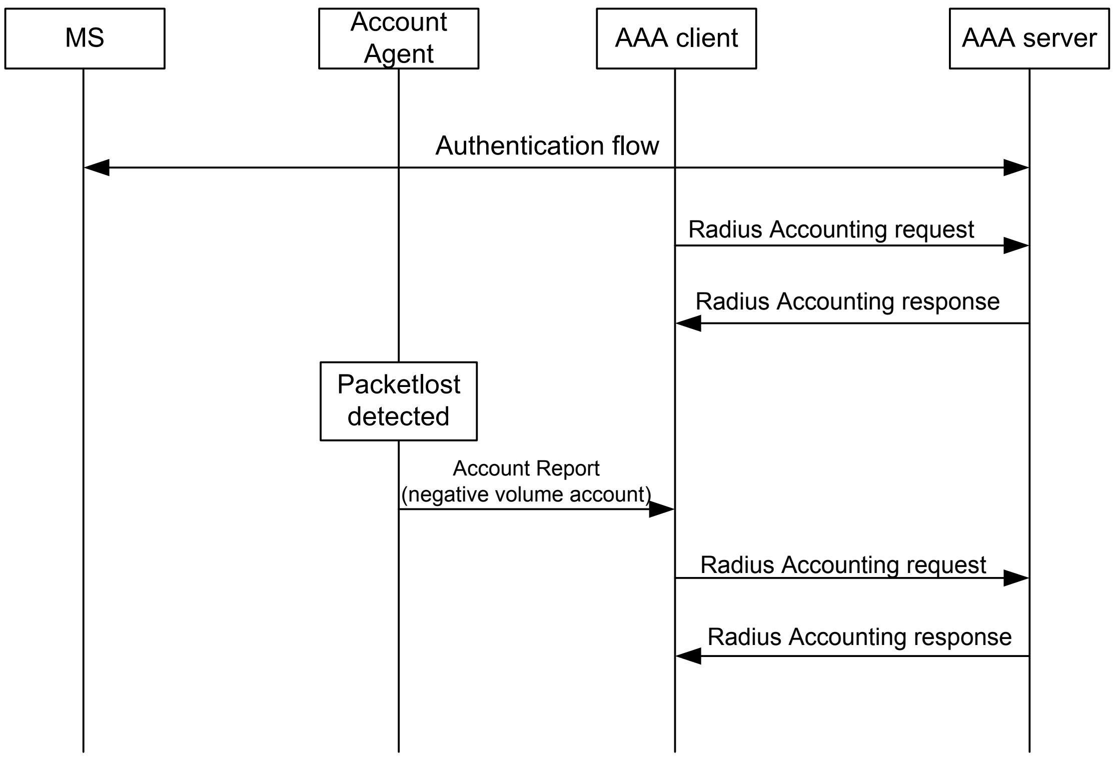


Figure 7-33 - Negative Volume Count

7.5.3 RADIUS Server Requirements

The RADIUS Server SHALL follow the guidelines specified in [23], [24], and [36].

The Visited and Home RADIUS server SHALL support the attributes as specified in Stage 3 RADIUS Message section 5.4.1.

Upon receiving RADIUS Accounting-Request records from the ASN, the Visited RADIUS server SHALL forward the RADIUS Accounting-Request records to the home or broker network.

The communication between RADIUS client and RADIUS server or between RADIUS servers SHALL be protected using the secret shared with the next hop RADIUS server using the procedures described in [23].

7.5.4 HA Requirements as RADIUS Client

If the HA supports the Radius client then the HA SHALL support RADIUS client as specified in [23] and RADIUS Accounting as specified in [24] and [36].

The HA SHALL send a RADIUS Access-Request to the Home RADIUS server when it receives an RRQ (Registration Request) containing the authentication extension to request authentication and authorization of the user by the RADIUS infrastructure. The HA SHALL include the RADIUS attributes and VSAs in the Access Request as specified in Stage 3 section 5.4.1.

7.5.5 Offline Accounting

This section describes the off-line (post-paid) accounting procedures and the Usage Data Records (UDRs). It also describes the RADIUS standard attributes and VSAs used to support accounting capabilities in the WiMAX network.

It is important to note that a lower case letter implies an accounting attribute in an Airlink Record whereas an uppercase letter implies an accounting attribute in a UDR.

Packet data accounting parameters are divided into radio specific parameters (e.g., number of bytes/packets dropped at the BS), and IP network specific parameters collected by the Serving ASN. The Serving ASN SHALL merge radio specific parameters called Airlink Records with IP network specific ones to form one or more Usage Data Records (UDR). After merging, the Serving ASN SHALL use RADIUS accounting messages to send UDR information to the home RADIUS Server (via the visited AAA server if the subscriber is roaming). The detailed procedures for creating UDRs are described in the following sections.

7.5.6 Airlink Records

The ASN generates the following airlink records:

- An Active Start Airlink Record when the MS has connected the associated over-the air service flow.
- An Active Stop Airlink Record when the MS has released the associated over-the-air service flow.

7.5.7 ASN Procedures

The following events cause the ASN to take accounting action:

- R6 Connection Setup Airlink Record received over R6 reference point.
- Data service establishment on the ASN-GW for profile A or C or data path establishment for a MS at the ASN for profile B.
- Data service termination on the ASN-GW for profile A or C or data path termination for a MS at the ASN for profile B.
- Reception of Active Start Airlink Record.
- Reception of Active Stop Airlink Record.
- Interim-Update record trigger.
- Stop record trigger.
- Time of day timer expiry.
- Hot-lining
- Inter-ASN hand-off trigger.
- The location information for postpaid (Only location based postpaid accounting is specified in this release. Location based prepaid will be specified in a later release)
- The QoS of the service flow or the session is changed.

Each individual session SHALL be accounted for independently. All UDR information is stored and transmitted per assigned IPv4 address or IPv6 prefix, or per packet data flow. During the lifetime of the session, UDRs are created, modified, maintained, copied, and released for each individual connection. The Serving ASN SHALL create one UDR per R6 connection ID or other data path ID established for the MS

The ASN closes a UDR when any of the following events occur:

- An existing service flow is deleted, denied, or failed.
- The ASN determines the packet data session has ended.

At an initial R6 connection establishment, a UDR is created and initialized from the R6 connection setup airlink record. When there is a new R6 connection due to a handoff for an existing packet data session, or when there is a new R6 connection for an existing packet data session, a UDR is created by copying data from a previous UDR.

During a inter ASN handoff either two R6 connections, or an R4 and an R6 connection, or two R4 connections with the same SFID and MSID MAY exist momentarily due to the ASN bicasting. Since the MS can connect to only one ASN for a given service flow, the ASN accounting procedures SHALL ensure that double counting between the current and new (copy) never occurs despite the ASN bicasting of data to both service flows.

RADIUS accounting messages are generated from the information in the UDR. The Acct-Multi-Session-Id is used to match different accounting records (Account Session IDs) across R6, R4 or both connections for a single packet data session. One Acct-Multi-Session-Id for all R6 connections is maintained for a packet data session for each NAI and IP pair within the same Visited CSN. The Account Session ID is used to match a single RADIUS Start and Stop pair. A different Account Session ID is used for each R6 connection.

A new R6 connection due to intra-ASN handoff between BSs SHALL result in a new R6 Connection ID and Account Session ID. The MSID and SFID are used to select the proper UDR after an intra-ASN handoff. One R6 Connection ID MAY be associated with multiple simultaneous NAI, IP pairs in the Serving ASN (i.e., multiple packet data sessions).

In profile A and C, airlink records are only associated with an R6 connection ID. The Serving ASN matches the R6 Connection ID in the airlink record to the R6 Connection ID in the appropriate UDR(s). If more than one UDR matches, the actions are applied to all UDRs.

Some events cause certain UDR fields to change in the middle of a session. When this happens, the ASN MAY send a RADIUS Accounting-Request-Stop record to capture accounting data before the event, followed by a RADIUS Accounting-Request-Start record with the new field values. In fact, an ASN MAY send a RADIUS Accounting-Request-Stop and RADIUS Accounting-Request-Start anytime during a single session as long as no accounting data is lost. In these cases, the ASN SHALL send the same Acct-Multi-Session-Id in both the RADIUS Accounting-Request-Start and RADIUS Accounting-Request-Stop records.

The subsequent sections specify the actions to take for each event.

7.5.8 Online Accounting (Prepaid)

This section describes the online (prepaid) accounting procedures in the WiMAX network. The prepaid packet data service allows a user to purchase packet data service in advance based on volume or duration. Account status is stored on a prepaid server (PPS) that is located in the user's home network and accessed via the HAAA server. To provide service to roaming prepaid users, the visited ASN or CSN needs to support the prepaid service and the local and broker AAA servers need to forward the new prepaid accounting attributes transparently to and from the home AAA server. The HAAA server and the prepaid server could be collocated or could be separate entities (see Figure 7-32).

From the ASN perspective, the HAAA and the prepaid server are indistinguishable. Although this document does not make assumptions about the prepaid server – HAAA interface, the call flows MAY show the prepaid server and the HAAA as separate entities.

The prepaid billing solution can provide the following services:

a) Simple IP based service metering in real time.

b) Undifferentiated Mobile IP services in real time with support for multiple Mobile IP sessions per user. "Undifferentiated" means that all the Mobile IP sessions for a single user will be rated equally.

c) Rating measurement based on data volume and/or call duration. Data volume is measured as total octets, uplink octets, downlink octets, total packets, uplink packets or downlink packets and total duration. The rating function can be done either by the prepaid client or prepaid server.

Prepaid service for multiple simultaneous data sessions is also allowed. As the network does not have any a priori knowledge of the user usage behavior, the solution is built on an iterative authorization paradigm. The prepaid server will apportion a fraction of subscriber's balance into a quota, each time an authorization request is made. Multiple sessions from the same user will each obtain their own quota, each session needs to seek reauthorization when the previously allocated quota is depleted thus minimizing any leakage. The granularity and the magnitude of the quota are implementation details of the prepaid server; therefore, it is beyond the scope of this specification. The limitation with this method is as the number of session increases, the quota for each session will be diluted. The user might need to close some sessions in order to collect all remaining quota that was allocated to his active sessions.

In order to support prepaid packet data service the ASN and/or the CSN SHALL support the prepaid client (PPC) function and the prepaid server (PPS) function MAY be collocated with the Home RADIUS server. In this specification, the prepaid packet data service supports a set of capabilities as described in the next section. Additional capabilities MAY be supported in future revisions of this specification. When the prepaid account of user is depleted, the PPC SHALL stop the online accounting service. If the user also has a postpaid account and is authorized to hand off off-line accounting base on profile or rule, the PPC of the ASN can notify the AAA client of ASN that SHALL create the UDR and send an off-line RADIUS accounting-request to AAA server but the service flow SHOULD not be terminated.

7.5.9 Online Accounting Capabilities

In this revision of the specification, the following prepaid capabilities are supported:

- Volume based prepaid, with quota assigned at a service flow level if the PPC resides in the ASN.
- Volume based prepaid with quota assigned at the packet data session level (IP/NAI) if the PPC is located in the CSN.
- Duration based prepaid, with quota assigned at a service flow level if the PPC resides in the ASN.
- Duration based prepaid, with quota assigned at the packet data session level (IP/NAI) if the PPC is located in the CSN.
- Ability for the Home AAA/PPS to allow/deny/select a PPC based on the Home AAA/PPS policy, user profile, PrePaidAccountingCapability (PPAC) VSA and the Session Termination Capability (STC) VSA of the ASN and/or the CSN.
- The prepaid packet data service is based on the RADIUS protocol.
- Home AAA/PPS ability to manage the prepaid packet data service when the quota allocated to a PPC is consumed or a pre-determined threshold value is reached, through triggers provided to the PPC.
- The capability of the PPC based in the ASN to support VolumeQuota and a tariff switch time interval concurrently per service flow. The capability of the PPC based in the CSN to support VolumeQuota and a tariff switch time interval concurrently per packet data session.
- The capability in the PPC and the Home AAA/PPS to provide tariff switch volume based prepaid packet data service, with tariff switch trigger controlled at the Home AAA/PPS. This capability includes:
- Charged by volume, different tariff for different time of a day.
    - Charged by volume, different tariff for different volume consumed, and the PPS SHALL allocate the quota so that the quota does not overlap the two charging rates.
    - Charge by volume, different tariff for different QoS. When the Qos is changed, the PPC can report the consumed volumes before the change and the PPS SHALL allocate the new quota for new QoS.

Tariff switching with duration based prepaid at the Home AAA/PPS. This capability includes:

- Charged by duration, different tariff for different time of a day.
- Charged by duration, different tariff for different duration consumed, and the PPS SHALL allocate the quota so that the quota does not overlap the two charging rates.
- Charged by duration, different tariff for different QoS.
- Account balance updated by the Home AAA/PPS according to the quota consumed by the user and reported by PPC and the tariff information in the user's profile.
- The prepaid account SHALL be reconciled at the Home AAA/PPS at inter-ASN handoff.

7.5.10 QoS-based Accounting

The QoS-based accounting is charging on service session, not user connection as traditional accounting does. The WiMAX network is capable of support multiple services for one user simultaneously with appropriate QoS level. The accounting on QoS is both feasible and useful.

The accounting function SHOULD be capable of separating one service session from others by characteristics of the service such as TCP/UDP port, protocol type, etc. RADIUS accounting messages, added with the information of service session and QoS level, are generated in AAA client and sent to AAA server.

7.5.11 ASN Requirements for Prepaid

If the ASN supports a PPC, it SHALL also support Dynamic Authorization with RADIUS [48] and Registration Revocation for Mobile IPv4 capabilities [45]. The ASN is referred to as a prepaid capable ASN, and the prepaid capability is based on the following principles:

- The ASN includes in the RADIUS Access-Request message to the Home RADIUS server/PPS, the PPAC VSA and the STC VSA. The values for each VSA are set appropriately and will be specified in the stage 3 specifications.
- Except for quota initialization for the Initial service flow (ISF), which is included in the RADIUS Access-Accept message by the Home RADIUS server/PPS, on-line quota update operation is performed by the prepaid capable ASN using on-line RADIUS Access-Request/Accept messages with Service-Type (6) set to "Authorize Only". The on-line RADIUS Access-Request SHALL contain the PrePaidAccountingQuota (PPAQ) VSA.
- The Home RADIUS Server/PPS initializes a quota for a user at authentication and authorization if it determines that the user is a prepaid user with positive prepaid balance and that the home network policy allows the ASN to provide prepaid service. The initialized quota is sent to the PPC in the RADIUS Access-Accept message associated with the creation of the Initial service flow. The RADIUS Access-Accept message includes the PPAQ and PPAC VSAs.
- The processing of off-line Accounting Request/Response messages proceeds independent of prepaid service.
- RADIUS Accounting (Stop/Start) messages caused by events such as parameter change, time of the day change, intra-ASN handoff do not cause the prepaid counters (such as VolumeQuota used, DurationQuota used etc.) to be re-set to zero.

If the RADIUS Access-Accept message includes the initial quota and contains the Service Profile attribute which indicates that the user is allowed to establish multiple service flows, the prepaid capable ASN MAY immediately initiate an on-line RADIUS Access-Request message to request pre-initialization of quota for any additional service flow that the user MAY establish.

If the user requests establishment of a service flow for which quota pre-initialization is not done, the ASN sends an on-line RADIUS Access-Request message to request initialization of quota.

The PrePaid capable ASN and the Home RADIUS/PPS MAY support tariff switch for volume based PrePaid packet data service.

7.5.12 CSN Requirements for Prepaid

The prepaid capable CSN SHALL support prepaid for packet data sessions identified by IP/NAI.

The prepaid capable home CSN SHALL enforce reverse tunneling for all the authorized volume based prepaid packet data sessions.

The prepaid capable CSN SHALL send a RADIUS Access-Request message to the Home RADIUS/PPS upon receiving the initial RRQ, re-registration and updated (new CoA) RRQ. The RADIUS Access-Request message SHALL include the additional VSAs: PPAC, STC and a Acct-Multi-Session-Id generated by the CSN. For the initial RRQ, the CSN SHALL include in the RADIUS Access-Request the MIP Lifetime VSA containing the RRQ Lifetime Sub-Type with the value corresponding to the lifetime received from the RRQ message. For the re-registration or the updated RRQ (new CoA) for the user, the CSN SHALL include the Session Continue VSA set to TRUE, the Correlation ID VSA with the same Acct-Multi-Session-Id value that is in use and the MIP Lifetime VSA containing both the RRQ Lifetime Sub-Type (lifetime value received in the RRQ) and the Used Lifetime From Existing Session Sub-Type (value of used lifetime of the existing Mobile IP session) if duration based prepaid is being provided for the session.

If the RADIUS Access-Accept message from the Home RADIUS/PPS contains the PPAC VSA indicating that prepaid accounting SHOULD be provided for the user, the RADIUS Access-Accept message SHALL include a PPAQ VSA with an initial quota unless the Acct-Multi-Session-Id sent in the RADIUS Access-Request is the same as an existing prepaid session for which there exists an outstanding quota.

If a new MIP Lifetime VSA is included in the RADIUS Access-Accept message from the Home RADIUS/PPS, the prepaid capable CSN SHALL include the value in the MIP RRP back to the ASN.

If both DurationQuota and TariffSwitchInterval are received for the same prepaid packet data session, the prepaid capable CSN SHALL discard the TariffSwitchInterval and SHALL provide prepaid based on the DurationQuota only.

If the PTS VSA is received, it SHALL include the TariffSwitchInterval (TSI) Sub-Type, and MAY include the TimeIntervalafterTariffSwitchUpdate timer (TITSU) Sub-Type. TITSU Sub-Type MAY be included when more than one tariff switch boundary exists, and the user MAY not reach the VolumeThreshold before the next tariff switch boundary is crossed. The prepaid capable CSN SHALL monitor both the Volume and the Duration concurrently to support tariff switching. The detailed accounting procedures for various prepaid services (Volume-, Duration- and Tarrif-Switched-base) are specified in the stage 3 of this specification.

7.5.13 Hot-Lining

The Hot-lining feature provides a WiMAX operator with the capability to efficiently address issues with users that would otherwise be unauthorized to access packet data services. When a problem occurs such that a user MAY no longer be authorized to use the packet data service, a wireless operator using this feature MAY hot-line the user, and upon the successful resolution of the problem, return the user's packet data services to normal. When a user is hot-lined, their packet data service is redirected to a Hot-line Application (HLA) which notifies the user of the reason(s) that they have been hot-lined and offers them a means to address the concerns meanwhile blocking access to normal packet data services. Reasons for hot-lining a user are: prepaid users whose account has been depleted; or users who have billing issues such as expiration of a credit card; or users who have been suspected of fraudulent use.

As a result, hot-lining performs the following four fundamental activities:

- Blocking normal packet data usage.
- Notifying MS that packet data usage is blocked.
- Directing MS to rectify blockage.
- Restoring normal operations when the User has rectified issues that triggered the hot-lining of their service. Or,
- Terminate service if the user failed to address the issues that triggered the hot-lining of their service.

Hot-lining would help provide a consistent user experience for all users, irrespective of which MS application is using the packet service. This includes preventing negative user experience resulting from arbitrarily blocking packet data service without notifying the MS of packet data block and a mechanism to rectify the blockage. Hot-lining would further provide consistency across all applications that utilize the packet data service plus it would lower operating costs.

7.5.14 Hot-Lining Capabilities

The following section describes the general hot-line capabilities supported for this release:

a) Hot-lining is supported for both CMIP and PMIP operations both at the ASN and the CSN.

b) A user can be hot-lined at the start of their packet data session or mid-session as described below:

Active-Session Hot-lining:	The user starts a packet data session. In the middle of the session it is hot-lined and after the account is reconciled by some manner, the hot-lining status off the session is removed. The hot-lining is done with RADIUS Change of

	Authorization (COA) message.
New-Session Hot-lining:	The user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session.

c) Similarly, hot-lined status can be removed mid-session or at the start of a new session.

d) There are two methods in which the HAAA indicates that a user is to be hot-lined:

Profile-based Hot-lining	The HAAA sends a hot-line profile identifier in the RADIUS message. The hot-line profile identifier selects a set of rules that are pre-provisioned in the Hot-line MS (HLD) that cause that user's packet data session to be redirected and/or blocked.
Rule-based Hot-lining	The HAAA sends the actual redirection-rules (HTTP or IP) and filter-rules in the RADIUS messages that cause the user's packet data session to be redirected and/or blocked.

e) In order to properly account for the hot-lining state of the user, the user's hot-line state SHOULD be recorded in the accounting stream.

The following capabilities are not covered by this specification but are described in so far that they are needed to implement a complete hot-lining solution:

a) The trigger(s) that cause an operator to hot-line a user is not in scope for this specification. These triggers could come from a number of sources such as a billing system, fraud detection system, etc.

b) The means to notify the HAAA that a user is to be hot-lined is not in scope for this specification.

c) The means by which the user is notified that they have been hot-lined is not in scope of this specification. Typically, the user will be notified that they have been hot-lined via their browser or other means.

d) The means by which the user interacts with the system to correct the symptoms that caused them to be hot-lined are not in scope for this specification.

e) The means by which the system notifies the HAAA that user need not be hot-lined, that their packet data session is to be returned to normal is not covered as part of this specification.

f) The details of what happens when the ASN or CSN performs Profile-based Hot-lining are out of scope. It is assumed that the user's traffic is blocked and that the user gets notified.

When the packet data session is hot-lined some IP flows will be blocked and some IP flows will be redirected. The intent of the redirection is not to continue the normal operation of the flow but rather to provide information to the Hot-line application so that the Hot-line application can determine how to notify the user of their hot-lined state.

7.5.15 Hot-Lining Operation

Hot-lining involves the following packet data network entities (Figure 7-34):

- Visited/Home CSN
- ASN
- HAAA
- VAAA

The CSN and ASN contain certain MSs that implement the hot-lining rules requested by the HAAA. In this document, any of these MSs that apply the hot-line rules for a user is called the Hot-lining MS (HLD). The role of the VAAA with respect to Hot-lining is to act as proxy and as such will not be discussed further.

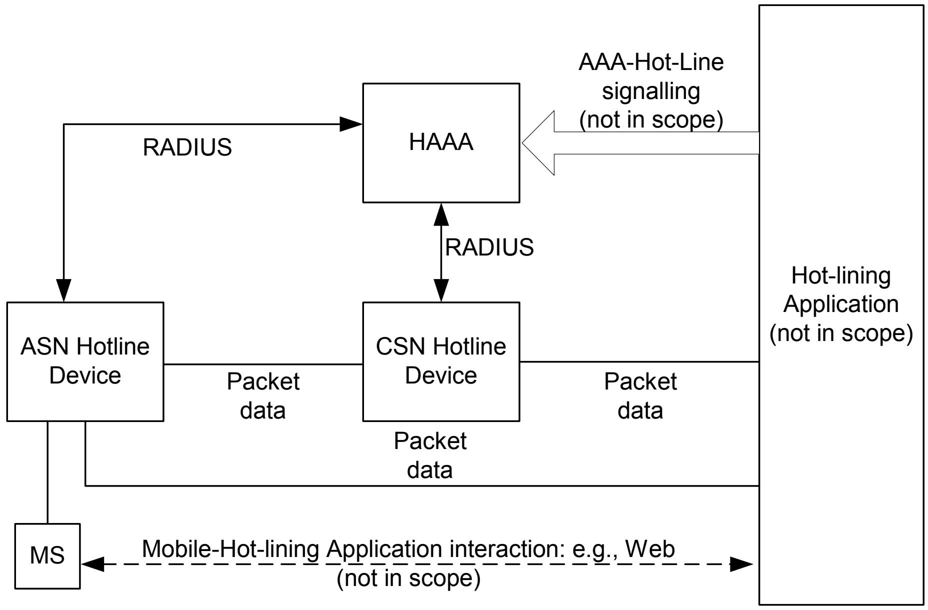


Figure 7-34 - Hot-Lining Operation

Hot-lining also involves the Hot-Line Application (HLA). The Hot-Line Application is a functional entity that performs the following roles:

- Determines when the user SHOULD be hot-lined.
- Initiates the hot-lining signaling with the HAAA.
- Hot-lined flows are redirected to the Hot-Line Application.
- Responsible for initiating notification of the hot-line status to the MS. This could be done via a delivery of an HTML page to the subscribers' browser or via some other means.
- Provides a mechanism for the user to rectify the issue that triggered hot-lining.
- Upon successful resolution of the problem, return the user back to normal operating mode.
- Upon unsuccessful resolution of the problem, terminate the user's packet data session.

The implementation of the Hot-Line Application is not within scope of this document. The interface between the Hot-Line Application and the various entities is out of scope.

The Hot-Line Application can reside over multiple servers in the network. For example, the Hot-Line Application could reside in its entirety on a web server. Or certain parts of Hot-line Application can reside on ASN or CSN as shown in Figure 7-34.

Hot-lining of a user's packet data service starts when the Hot-Line Application determines that the user's service is to be hot-lined. This determination is entirely deployment specific and can be a result of many factors. Details are not in scope for this document.

To initiate Hot-lining of the user, the Hot-Line Application will notify the HAAA that the user is to be hot-lined. The method of notification is out of scope. Upon receiving the notification from the Hot-Line Application, the HAAA records the hot-lining state against the user record.

The HAAA will determine if the user is currently in-service or out-of-service. If the user is in-service the HAAA initiates the Active-Session Hot-Lining procedure, if the user is out-of-service the HAAA initiates the New-Session Hot-Lining procedure.

Hot-lining requires that the Hot-lining MS be able to support Profile-based Hot-lining and or Rule-based Hot-lining. When support for Active Session Hot-lining is not provided the operator could utilize RADIUS Disconnect Message to terminate the user's session or specify a time period after which the session would be terminated by the Hot-lining MS. To participate in Hot-lining an access MS (ASN-GW/FA or HA) SHALL advertise its Hot-lining capabilities using the Hot-line Capability VSA sent in a RADIUS Access-Request message. The HAAA uses the contents of the Hot-line Capability VSA and other local policies to determine which access MS will be the Hot-lining MS for the session.

The hot-line signaling for a given packet data session is communicated by the HAAA to the Hot-line MS by sending the Hot-Line Profile Id VSA; or by sending HTTP/IP Redirection Rule VSAs and Filter Rule VSAs.

7.6 QoS

The NWG Release 1.0.0 specification defines the following procedures: (1) Pre-provisioned service flow creation, modification, and deletion. (2) Initial Service Flow creation, modification and deletion. (3) QoS policy provisioning between AAA and SFA. Service Flow ID management. As the scope of Release 1.0.0 is limited to pre-provisioned service flows, PF-SFA interactions are not addressed in this section. Figure 7-38, 7-36, 7-37, section 7.6.5.2, are not applicable for Release 1.0.0

7.6.1 Introduction and Scope

The scope of the QoS section is focused on the WiMAX radio link connection. QoS specific treatment in the fixed part of the access and core networks are implementation specific and are not described. As a result, this release makes no guarantees concerning end-to-end QoS.

The IEEE 802.16 specification defines a QoS framework for the air interface. This consists of the following elements:

- Connection-oriented service
- Five data delivery services at the air interface, namely, UGS, RT-VR, ERT-VR, NRT-VR and BE
- Provisioned QoS parameters for each subscriber
- A policy requirement for admitting new service flow requests

Under the IEEE 802.16 specification, a subscription could be associated with a number of service flows characterized by QoS parameters. This information is presumed to be provisioned in a subscriber management system (e.g., AAA database), or a policy server. Under the static service model, the subscriber station is not allowed to change the parameters of provisioned service flows or create new service flows dynamically. Under the dynamic service model, an MS or BS MAY create, modify or delete service flows dynamically. In this case, a dynamic service flow request (triggered using mechanisms not specified in IEEE 802.16) is evaluated against the provisioned information to decide whether the request could be authorized. More precisely, the following steps are envisioned in the IEEE 802.16 specification for dynamic service flow creation:

a) Permitted service flows and associated QoS parameters are provisioned for each subscriber via the management plane.

b) A service flow request initiated by the MS or BS is evaluated against the provisioned information, and the service flow is created if permissible.

c) A service flow thus created transitions to an admitted, and finally to an active state either due to BS action (this is possible under both static and dynamic service models). Transition to the admitted state involves the invocation of admission control in the BS and (soft) resource reservation, and transition to the active state involves actual resource assignment for the service flow. The service flow can directly transit from provisioned state to active state without going through admitted state.

d) A service flow can also transition in the reverse from an active to an admitted to a provisioned state.

e) A dynamically created service flow MAY also be modified or deleted.

This specification extends the QoS framework established in the IEEE 802.16 specification to the NWG reference architecture. This specification does not address the provisioning of QoS in the access and core networks. There are many possibilities for enforcing QoS in L2 and L3 networks, and operators MAY require specific L2 and L3 interfaces in ASN network elements to use known methods for mapping IP traffic onto these networks.

Please note that dynamic service flow creation triggered by the MS or the AF is not planned for this release. One of the impacts is that no PF-SFA interface is defined in this release.

7.6.2 QoS Functional Elements

Based on the IEEE 802.16 specification and the Stage 2 architectural reference model, the QoS functional model includes the following elements, as illustrated in Figure 7-35

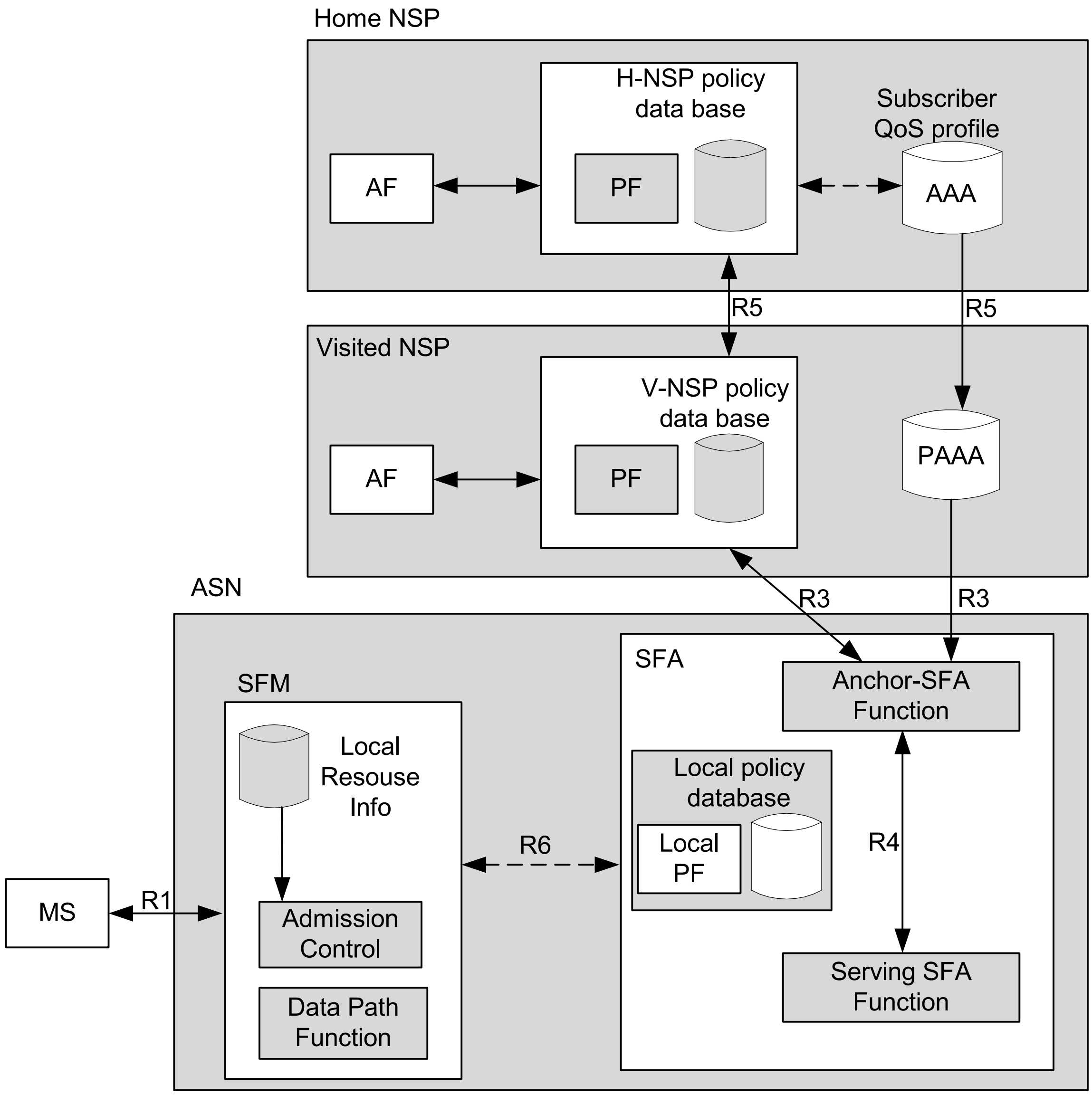


Figure 7-35 - QoS Functional Elements

a) MS and ASN. The WiMAX network SHALL support ASN-initiated creation of service flows. An MS MAY, but is not required to, have this capability (the MS must, however, respond appropriately to ASN-initiated service flow actions).

b) The home policy function (PF) and its associated policy database belong into the home NSP. Maintained information includes H-NSP's general policy rules as well as application dependant policy rules. The AAA MAY, in addition, provision the PF's database with user's QoS profile and associated policies. However, interaction between PF and AAA, represented by the dotted arrow, is out of scope of this specification. The

PF is in charge to evaluate service requests against these policies. The MS directly communicates with the AF using application layer control protocols, and the AF MAY issue WiMAX service flow triggers to the PF as a result (in roaming case, the AF could be located at the H-NSP as well as at the V-NSP where the corresponding PF's are triggered).

c) AAA server holds the user's QoS profile and associated policy rules. This information can be used in two different and exclusive ways: They can be downloaded to the SFA at network entry as part of the authentication and authorization procedure. Alternatively they can be provisioned in the PF, where this option is not part of WiMAX Release1.0. In the former case, the SFA evaluates the forthcoming service request against the user profile. In the latter case, it is up to the home PF to do so.

d) A Service Flow Management (SFM) logical entity in the ASN. The SFM entity is responsible for the creation, admission, activation, modification and deletion of 802.16 service flows. It consists of an Admission Control (AC) function, and associated local resource information. The AC is used to decide whether a new service flow can be admitted based on existing radio and other local resource usage. The precise definition of the admission control functions is left to implementations. The SFM entity is always located in the BS.

e) Service Flow Authorization (SFA) logical entities in the ASN. In case the user QoS profile is downloaded from the AAA into the SFA at network entry phase, the SFA is responsible for evaluating any service request against user QoS profile. For a given ASN/NAP there exists an *anchor* SFA assigned to each MS. The anchor SFA does not change for the duration of the Device Authentication session. Optionally, there MAY be one or more additional SFA entities that relay QoS related primitives and apply QoS policy for that MS. The relay SFA that directly communicates with the SFM is called the *serving* SFA (when there are no relays, the anchor SFA is also the serving SFA). The identity of the serving SFA, if different from the anchor, SHALL be known by the anchor SFA at all times. Similarly, the serving SFA SHALL know the identity of the anchor SFA. The anchor and/or serving SFA MAY also perform ASN-level policy enforcement using a local policy database and an associated local policy function (LPF). The LPF can also be used to enforce admission control based on available resources. The implementation of this is local to the SFA and outside the scope of this specification. A serving SFA MAY be in the bearer path towards the SS, but only the signalling interactions for SFA are in the scope of this document.

f) A network management system (not shown) that allows administratively provisioning service flows.

In case the QoS profiles and associated policies are downloaded from the AAA to the SFA they SHALL be expressed as depicted in the stage 3 part of the present specification. Based on service provider requirements, the provisioned information MAY include user priority, which is used to enforce relative precedence in terms of access to radio resources so that differentiated service categories (e.g., gold, silver, and bronze) across users can be realized. For example, the user priority MAY be taken into account in situations where the service flow requests across all users exceed the radio resource capacity and therefore a subset of those has to be selected for rejection.

The scope of the provisioned QoS profile is assumed to be specific to the MAC connections at the air interface. In other words, this profile does not imply specific QoS treatment in the wireless backhaul of the access and core networks. The latter would depend on the available QoS mechanisms in the fixed networks.

7.6.3 Triggers

The provisioned QoS profile serves to authorize dynamic requests initiated by the MS (not in scope of this release) or the BS. These dynamic requests (creation, admission, activation as well as modification and deletion of service flows) MAY result from different types of triggers including the ones described in the following subsection.

7.6.3.1 Pre-Provisioned Service Flows

A set of service flows can be created, admitted, and activated by default after a subscriber station registers with the WiMAX network, before any IP data begins flowing. This is the minimum capability mandated by this specification. This capability is realized by including the description of the service flows to be created and optionally, user priority.

After successful MS registration with the WiMAX network, an anchor SFA SHALL be assigned, and its location updated with the associated PF entity, unless the PF is aware of the anchor SFA through other means.

If the user's QoS profile has been downloaded from the AAA during the authentication procedure of the network entry, the SFA initiates the creation, admission and activation of the pre-provisioned service flow.

If the user's QoS profile has not been downloaded, then it is the PF or the LPF that initiates the creation and activation of pre-provisioned service flow (out of scope of Release 1.0.0.).

There MAY be circumstances under which a pre-provisioned service flow cannot be created or activated in the ASN. The action to be taken in this case will be dependent on the policies within the ASN, and the agreements between the NAP and the NSP. The QoS framework SHOULD allow the communication of the result of an attempt to pre-provision a service flow from the ASN to the CSN.

7.6.4 Messages

7.6.4.1 Message types

The following sets of abstract messages are required to convey triggers, initiate service flow actions, request policy decisions, download policy rules, and update MS location:

a) Resource-Reservation (RR): *RR_Req* messages could be originated by the anchor SFA. A *RR_Req* message is sent from the anchor SFA to the serving SFA (if different from anchor), and finally, from the serving SFA to the SFM, to request reservation of resources for one or more identified unidirectional traffic flow(s) from/to the same MS. *RR_Rsp* is sent from, the SFM to the serving SFA, from the serving SFA to the anchor SFA (if different) to indicate the result of a resource reservation request Traffic flows listed within a *RR_Req* message could behave dependent or independent. In case of dependent behaviour, the request will only be accepted if all of the listed traffic flows could be reserved successfully. The receipt of the *RR_Rsp* is acknowledged by sending a RR_Ack by the anchor SFA to the serving SFA (if different from anchor SFA) and finally from the serving SFA to the SFM.

.

7.6.4.2 Trigger Points for Dynamic SFs (not in scope of this release)

From the description above, it is clear that the trigger point could be the SFM, or the PF. Specifically, the trigger point is the SFM when the MS generates explicit create, admit, or activate request. Similarly, the PF could get explicit or administrative triggers where in the roaming case the source could be the visited PF as well as the home PF. The admission control function is located in the SFM in all cases.

7.6.5 QoS-Related Message Flow Examples

In this subsection, the control flows are illustrated for service flow creation and deletion, and updating of the SFA location. In all these examples, it is assumed that there is a security association between communication entities, and suitable retransmission mechanisms are implemented to ensure reliable communication.

7.6.5.1 Pre-Provisioned Service Flows

This procedure is initiated by the anchor SFA after the completion of MS registration.

If the user's QoS profile and associated policies have been downloaded from the AAA, the SFA applies them in order to identify the pre-provisioned service flow that need to be created admitted and activated. The procedure is shown in Figure 7-36.

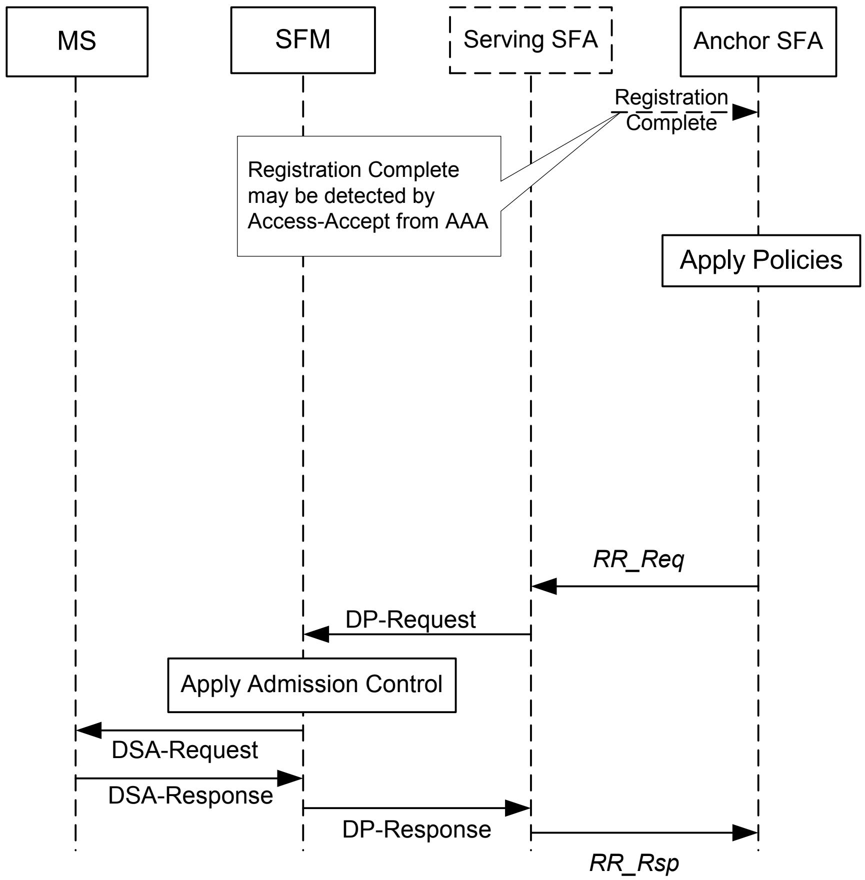


Figure 7-36 - Pre-Provisioned Service Flow Creation

If the user's QoS profile has not been downloaded, the PF or LPF (which, in that case, SHOULD hold it) initiates the creation and activation of pre-provisioned service flows, if so configured.

The PF applies policies configured for the MS and determines that one or more service flows SHALL be pre-provisioned. It then sends an *RR_Req* message to the anchor SFA to create and activate service flows. The rest of the message sequence is as shown in Figure 7-37 (*DSA_Req* and *DSA_Rsp* messages are defined in IEEE 802.16 specifications).

In case of roaming, the PF could be split up into a home and visited PF. In this case, the visited PF will act as a relay function where the visited PF could adapt the user profile data according local policies.

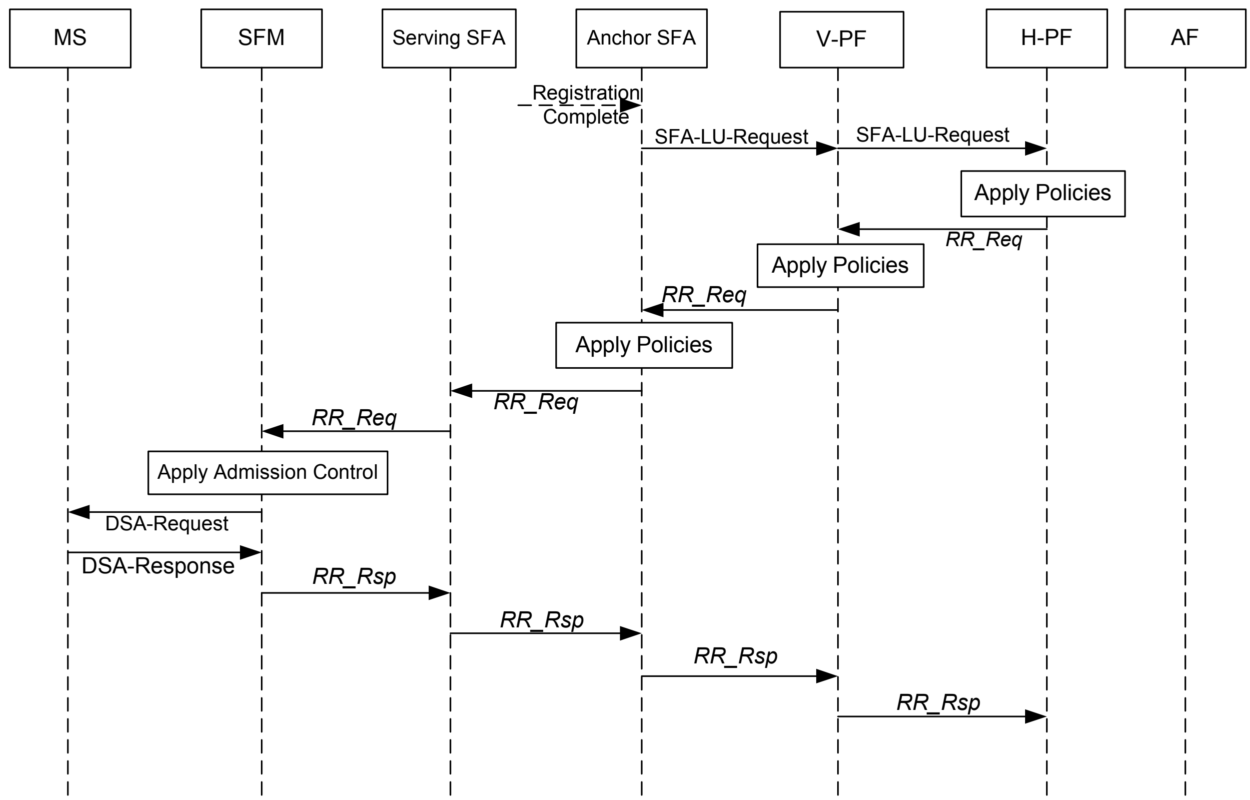


Figure 7-37 - Pre-Provisioned Service Flow Creation

7.6.5.2 AF-Triggered Service Flows

Service Flows could be triggered by an AF at the Home NSP as well as by an AF at the Visited NSP. Figure 7-38 illustrates AF-triggered service flow creation where the AF is located at the Home NSP. This is similar to the previous case, except that the service flow creation is initiated by the AF. User profile related policies are part of the policies applied by the SFA or are part of those applied by the H-PF depending whether the QoS profile and associated policies have been downloaded in the SFA or not (charts are the same in both cases).

In case of roaming, the PF could be split up into a home and visited PF. In this case, the visited PF will act as a relay function where the visited PF could adapt the user profile related policies according to the local policies.

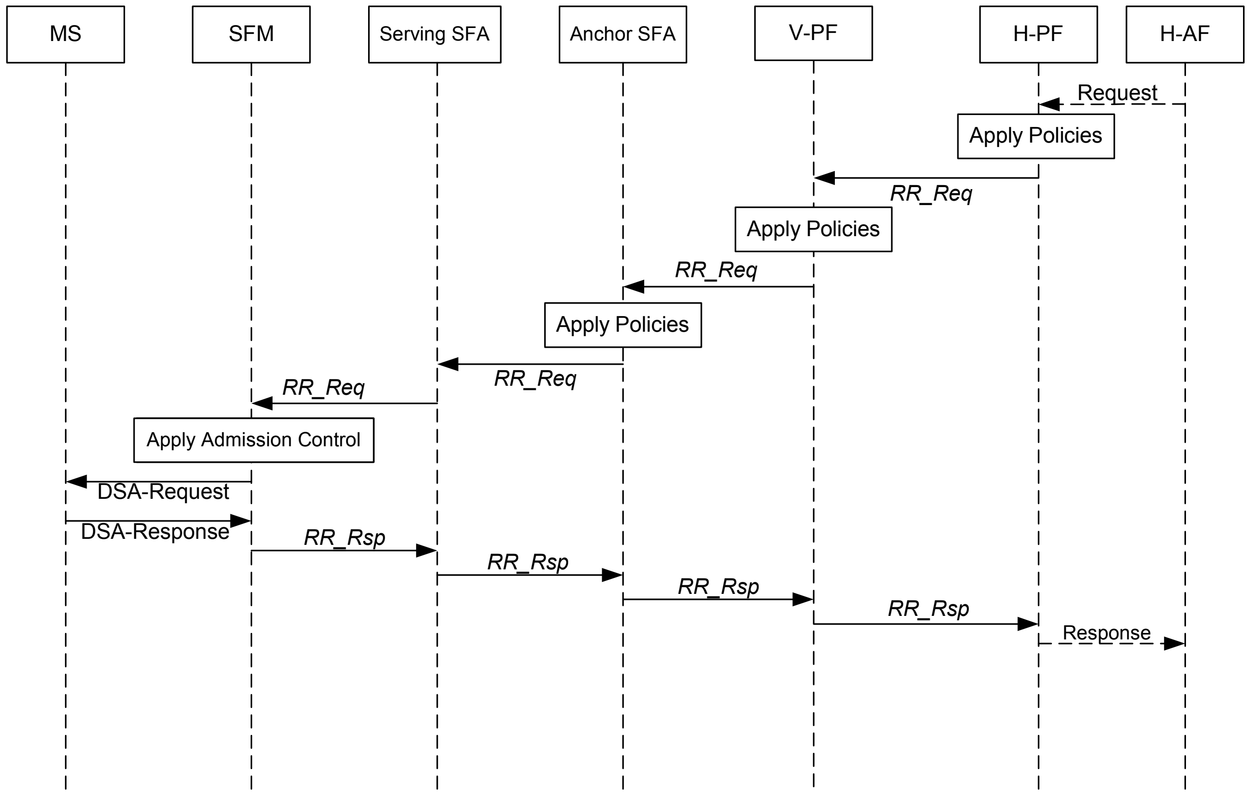


Figure 7-38 - Service Flow Creation triggered by the AF at the Home NSP

In case of roaming, also the AF of the visited network MAY trigger a service flow creation. In such a case, the PF of the visited network SHOULD send the request to the PF of the home network to check against local policies. The flow is similar to the previous case, except that the service flow creation is initiated by the Visited AF and the verification of the request by the PF of the home NSP. User profile related policies are part of the policies applied by the SFA or are part of those applied by the H-PF depending whether the QoS profile and associated policies have been downloaded in the SFA or not (charts are the same in both cases).

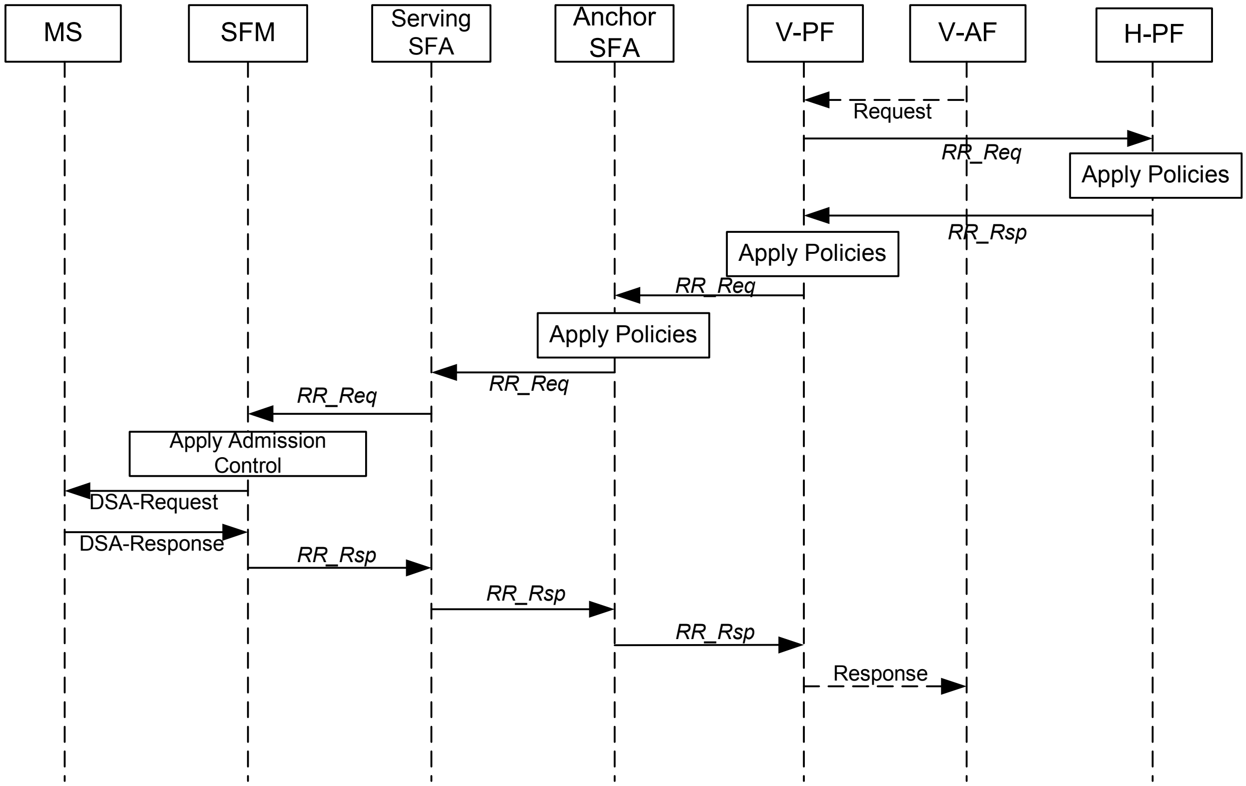


Figure 7-39 - Service Flow Creation triggered by the AF at the Visited NSP

7.6.5.3 Updating SFA Location

The anchor SFA remains invariant during the Device Authentication session as the MS moves in the network. The serving SFA, however, might change. The anchor SFA SHALL keep track of the current serving SFA when network-triggered service flows are implemented. For this, the serving SFA SHALL know the identity of the anchor SFA. This information can be achieved by the mobility procedures as the anchor SFA should be collocated with the AAA-client and SHALL be addressed by the Authenticator ID. The serving SFA should be collocated with the FA / AR and SHALL be addressed by the Anchor GW ID as the Serving-SFA triggers the DP-handling on the Anchor-DP function.

7.6.6 IP Differentiated Services

Differentiated services (diffserv) is an IP layer QoS mechanism, whereby IP packets are marked with diffserv code points at the network point of entry and network elements enforce relative priority of packets based on their code points. The diffserv methodology allows network resources to be reserved for classes of traffic, rather than for individual flows, as defined in [18].

In the context of the WiMAX air link, IP diffserv mechanism can be used to enforce priorities for packets within a service flow, or to establish service flows based on diffserv classes for a given subscriber. As an example, a single pre-provisioned service flow for a subscriber can be used to carry multiple types of traffic, with relative precedence established based on diffserv code points. On the other hand, service flows MAY be established dynamically to carry different diffserv traffic classes. An example of this is the establishment of a UGS service flow dynamically to carry a voice call, where the voice traffic is marked with diffserv EF class (described in [20]).

In the first case above, the diffserv code points are used to prioritize and schedule packet transmission within a service flow. The manner in which this is done is a matter of local implementation in the BS and the SS, subject to the prioritization rules of diffserv. In the second case, the diffserv code point is used to classify packets onto separate service flows. This scenario occurs when packets entering the BS or the MS are already marked with diffserv code points by an application or some prior network entity.

7.7 ASN Anchored Mobility Management

7.7.1 Scope

ASN Anchored Mobility Management is defined as mobility of an MS not involving a CoA update (i.e. a MIP re-registration). Procedures described for ASN Anchored Mobility Management also apply for mobility in networks not based on MIP. There MAY be scenarios involving "ASN Anchored Mobility Management", followed by subsequent CoA update and CSN Anchored Mobility Management. In this case the initial mobility management procedures up to the CoA update trigger are described here, while the procedures starting with CoA update triggering are in the scope of Section 7.8.

7.7.2 Functional Requirements for ASN Anchored Mobility Management

The functional requirements for ASN Anchored Mobility Management are:

a) The architecture SHALL accommodate three scenarios of operation (as described in [79])
   - Nomadicity (and fixed access)
   - Portability and with Simple Mobility
   - Full Mobility

b) The architecture SHALL consider:
   - Minimizing or eliminating packet loss
   - Minimizing handoff latency
   - Maintaining packet ordering

c) The architecture SHALL comply with the security and trust architecture defined in the IEEE 802.16 specification and IETF EAP RFCs.

d) The architecture SHALL support private addresses allocated by the Home NSP or the Visited NSP, as well as NAP sharing.

e) The architecture SHOULD support Macro-Diversity Handoff (MDHO) and Fast Base Station Selection (FBSS).

f) The architecture SHOULD support MS in various states— Active, Idle, and Sleep.

g) The number of roundtrips of signalling between BS and Intra-ASN mobility anchor point to execute a HO SHALL be minimized

h) The HO control primitives and Data Path enforcement control primitives SHALL be independent of each other such that it allows separation of HO control and Data Path enforcement control.

i) The Data Path enforcement mechanism SHOULD support and be compatible with the NWG QoS architecture.

7.7.2.1 ASN Anchored Mobility Management Consideration

This section mentions ASN Anchored Mobility Management:

a) It SHOULD support multiple deployment scenarios.

b) It SHOULD be agnostic to the ASN Decomposition, and SHOULD work with any defined form of ASN construction and profiles.

c) It SHOULD accommodate HO procedures for Data Path anchoring as well as procedures for re-anchoring.

d) It SHOULD accommodate signalling and data transmission protocols within an ASN or ASNs which are within a NAP administrative domain.

e) Its protocol SHOULD accommodate multiple Data Path types with varying granularities.

f) It SHOULD be independent of RRM procedures.

7.7.2.2 ASN Anchored Mobility Management Functional Decomposition

The ASN Anchored Mobility Management SHALL be defined by the following functions:

- **Data Path (Bearer) Function**: Manages the data path setup and includes procedures for data packet transmission between two functional entities
- **Handoff Function**: Controls overall HO decision operation and signaling procedures related to HO
- **Context Function**: Addresses the exchanges required in order to setup any state or retrieve any state in network elements.

Each of these functions is viewed as a peer-to-peer interaction corresponding to the function.

7.7.2.2.1 Generic ASN Anchored Mobility Management Functional Reference

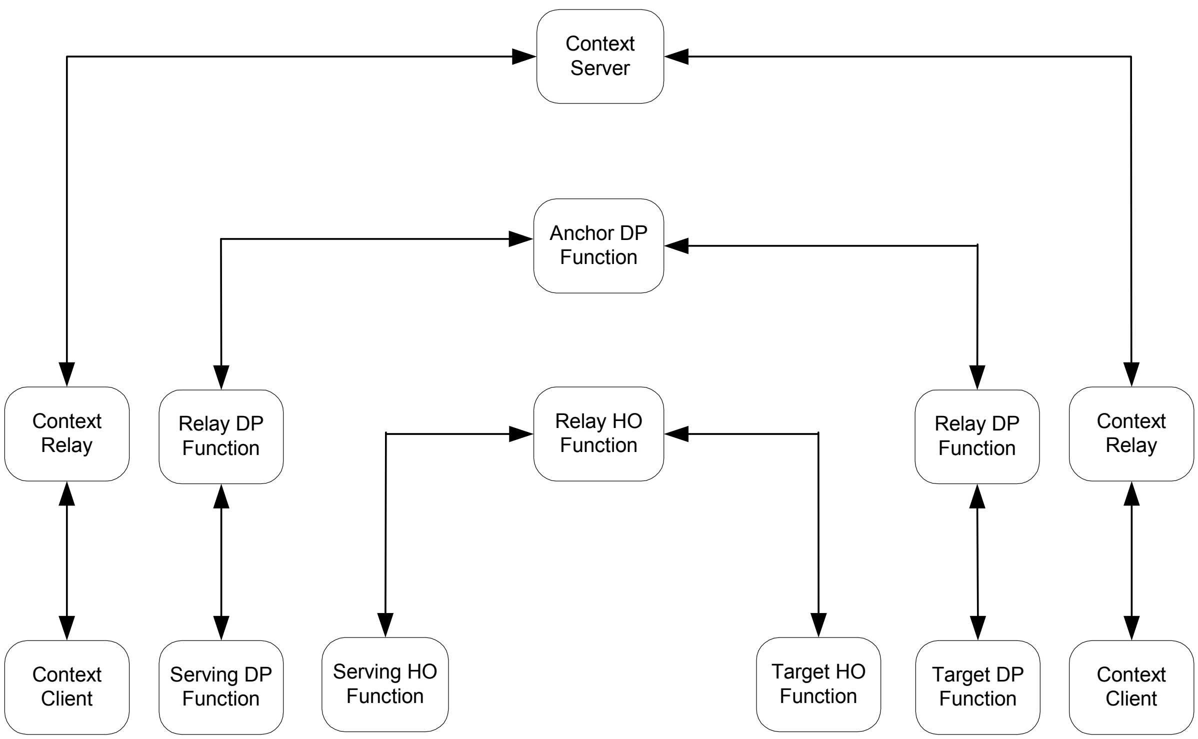


Figure 7-40 - Overall Reference for ASN Mobility Functions

Figure 7-40 depicts the relationship between the functional entities.

7.7.2.2.2 Data Path Function

The Data Path Function manages the setup of the bearer plane between two peers. This MAY include setup of any tunnels and/or additional functionality that MAY be required for handling the bearer plane. The Data Path function is used to setup the bearer plane between Base-Stations or between other entities such as Gateways or between gateways and base-stations. Any additional requirements such as support of multicast or broadcast are also handled by this function. Data Path Function shall support the use of packet sequence number. The Data Path Function is also used to optionally ensure a low latency connection during handovers.

Each Data Path function is responsible for instantiating and managing data bearer between it and another Data Path function and for selecting the payload traversing the established data bearer. There are two types of Data Path Functions:

Type 1: IP or Ethernet packet forwarding with layer-2 or layer-3 transport

For Type 1, data path bearer is typically a generic layer 3 tunnels (e.g. IP-in-IP or GRE) a layer-2 network such as Ethernet or MPLS. The payload is an IP datagram or an Ethernet packet. Additional semantics can be applied to the transport header and payload to handle scenarios such as header compression, sequenced delivery. The data bearer can be routed or bridged.

Type 2: forwarding with Layer-2 or layer-3 transport

For Type 2, data path bearer is also typically a generic layer 3 tunnels (e.g. IP-in-IP or GRE) a layer-2 network such as Ethernet or MPLS. The payload is a Layer-2 data packet which is defined as an 802.16e MAC Service Data Unit (SDU) or part of it appended with additional information such as CID of Target BS, Automatic Retransmission Request (ARQ) parameters, etc. In Type 2, layer-2 session state (e.g., ARQ state) is anchored in the Anchor Data Path Function.

The Data Path Function can be further classified by its roles in handover and initial entry operation as follows:

- **Anchor DP Function**: The DP (Data Path) Function at one end of the data path, which anchors the data path associated with the MS across handovers. This Function SHALL forward the received data packet toward the Serving DP function using either Type 1 or Type 2 Data Path. This Function MAY buffer the data packets from the network and maintain some state information related to bearer for MS during handovers.
- **Serving DP Function:** The DP Function at other end of a data path,, at the moment, has the association with the Serving PHY/MAC function and takes charge of transmission of all messages associated with the corresponding MS. This DP Function, associated with a Serving BS, communicates with the Anchor DP Function through Type-1 or Type-2 Data Path, to forward/receive MS data packets.
- **Target (New Serving) DP Function:** The DP Function which has been selected as the target for the handover. This DP Function, associated with a Target BS, communicates with the Anchor DP Function to prepare a Data Path to replace the current path after the completion of the handover. Upon successful handoff it will assume the role of Serving DP.
- **Relaying DP Function:** The DP Function which mediates information delivery between Serving, Target and Anchor DP Functions.

7.7.2.2.2.1 Data Path Considerations

Depending upon the level of classification used within Data Path Functions, uplink and downlink subscriber flows between Data Path Functions can be forwarded using different granularities, as an aggregate or as individual flows etc.

As shown in Figure 7-41, there are three levels of aggregations that can be used to transfer subscriber flows over a Data Path.

- **Case 1**: Per Service Flow per subscriber i.e. finest classification granularity.
  Each individual Service Flow of a subscriber is given a specific forwarding treatment across the ASN.
- **Case 2**: Per subscriber Flows belonging to a single subscriber MAY be transferred as an aggregate across or within ASNs.
- **Case 3**: Per Functional Entities, i.e. coarsest classification granularity.
  Flows belonging to all subscribers of a BS MAY be transferred as an aggregate across or within ASNs.

A Data Path is identified via the classification operation based on a set of classification criteria such as MS MAC address.

The flow classification of each Type of Data Path Function MAY use different parameters as the classifier. That is, for example, Type-2 Data Path Function SHALL use the information included in the layer-2 packets such as MS MAC address, CID, etc.

The protocols considered in the following discussion are GRE, MPLS and 802.1Q VLANs are examples of technologies that can be used to forward subscriber flows across ASN. These technologies provide for a level of keying or tagging between the two end-points. Such a tag or key MAY be used in a classification decision by the Data Path Function.

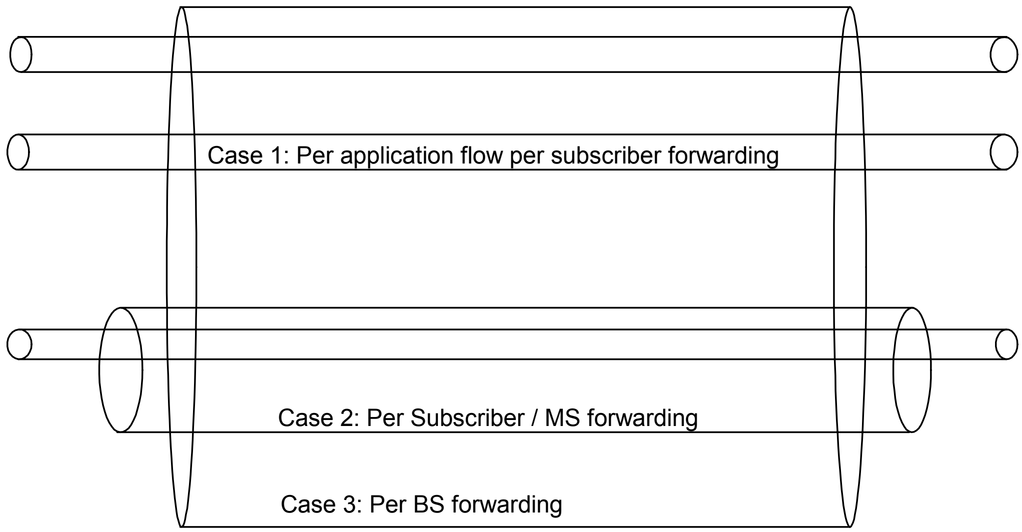


Figure 7-41 - Data Path Granularity

7.7.2.2.2.2 Type-1 Bearer Operation

Typically, a Type-1 Bearer is used to send IP or Ethernet packets tunneled or tagged using GRE, MPLS or 802.1Q etc. between the data path functional peers. In order to satisfy several requirements such as overlapping addresses as well as layer-2 transparency, a protocol which provides a level of tagging MAY be desirable for use with Type-1 Bearer. Such a tagging helps in identification of the MS and/or the specific QoS flows associated with the MS.

Type-1 Bearers are used to deliver the payload associated with a user to the respective data path peer function. A Type-1 Bearer can be created per MS or per MS QoS Flow (SFID), or can be shared across multiple MS (aggregate path). When a Type-1 bearer is created per MS or per MS QoS Flow, a directional key or tag MAY be associated with the bearer.

When a key or tag is used, the bearer is classified to the appropriate MS or MS QoS Flow (SFID) based on the classifier programmed for the traffic addressed to the specific MS. The traffic received from the MS MAY be mapped on to the data path based on the CID.

GRE shall be the tunneling protocol. ‘pure’ IP packet will be transported by a per-flow GRE tunnel.

Figure 7-41 below shows an example of the classification operations for Type-1 Bearer

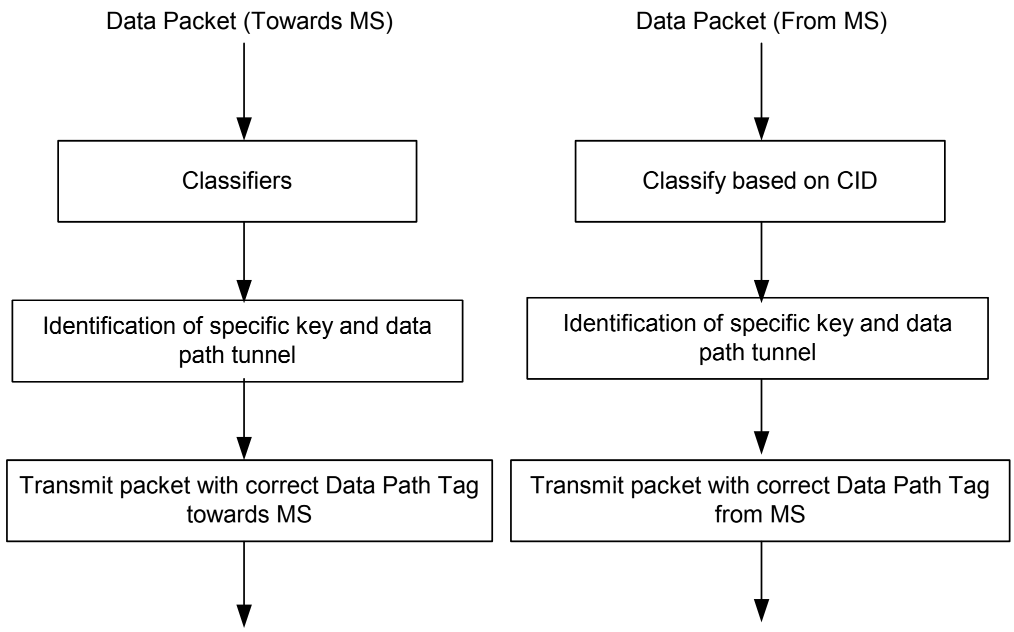


Figure 7-42 - Optional Classification Operations of Type 1 Bearer

7.7.2.2.2.3 Type 2 Bearer Operation

7.7.2.2.2.3.1 Data Anchoring: Data Packet or ARQ Block

When employing Type-2 Data Path Function for Intra- and Inter-ASN mobility support, layer-3 data communication path from the core network to the Anchor Data Path Function SHALL NOT be changed by HO and remains the same as what is before the HO. With the Type-2 Data Path Function, switching of path for layer-3 data communication MAY be deferred until a session relocation request from a HO Function becomes outstanding

Figure 7-43 below shows a typical mobility model that employs Type-2 Data Path Function.

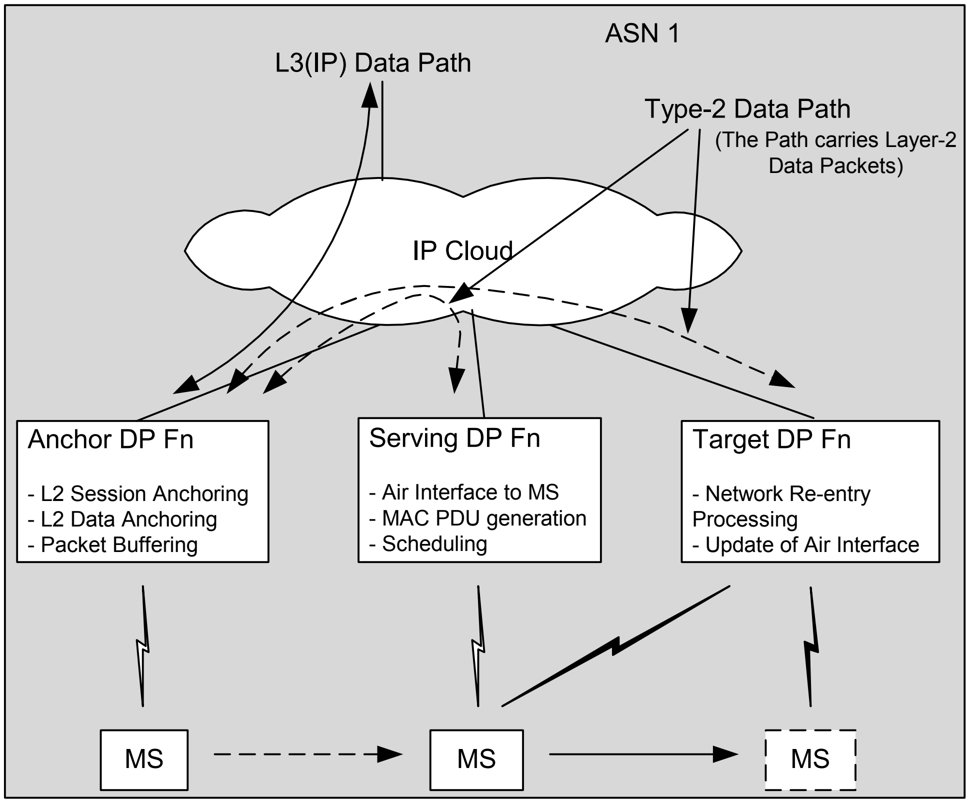


Figure 7-43 - Layer-2 Data Anchoring with Type-2 DP Function

In a mobility model that employs Type-2 Data Path Function, the Anchor Data Path Function MAY be located in the different entity from what has the Foreign Agent function. And, in this model, R3 mobility event MAY be deferred until the Anchor Handover Function triggers the R3 MM.

In Type-2, the Anchor Data Path Function SHALL anchor active Layer-2 sessions including ARQ States, and data paths used to transmit user IP packets to/from core network.

In Type-2, the Anchor Data Path Function SHALL generate Layer 2 Data Packets[7] from the received layer 3 IP packets, and then encapsulate them into the tunnel packets to forward them toward the appropriate destination Functional Entity.

In Type-2, the Serving Data Path Function, residing in the Functional Entity that has 802.16 physical associations with MS now, SHALL take charge of transmissions of all MAC messages to MS.

If MS moves to another cell and a handover is desired, the Target Data Path Function, residing in the Functional Entity that is determined as the target for the handover, SHALL perform backbone communication with Anchor Data Path Function to prepare a Type-2 Data Path to serve the pending MS handover.

7.7.2.2.2.3.2 Bearer Operation

In Type-2, bearer paths SHALL be used to deliver Layer-2 Data Packets between the Anchor Data Path Function and the Serving Data Path Function. A Layer-2 data packet is defined as an 802.16e MAC SDU or part of it which is appended with additional information such as CID of Target BS, ARQ parameters, etc.

Figure 7-42 below illustrates the overall data transmission process over a bearer of Type-2 Data Path Function.

[7] Here, the Layer-2 packet does not mean MAC Protocol Data Unit (PDU). It is rather MAC Service Data Unit (SDU) appended with additional information such as CID of Target BS, ARQ parameters, etc.

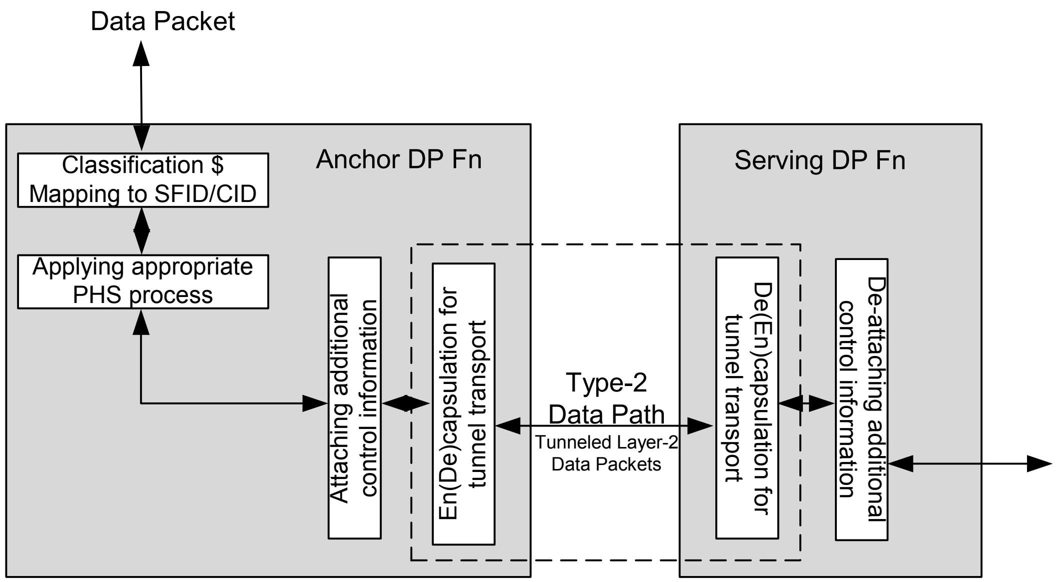


Figure 7-44 - Data Transmission over Type-2 Bearer

When an IP packet arrives at the Anchor Data Path Function through a data path, it SHALL be classified by the Anchor Data Path Function and mapped to an appropriate IEEE 802.16 Service Flow and SFID.

Then the Anchor Data Path Function MAY apply an appropriate Packet Header Suppression rule per SFID to the packet to make a MAC CS PDU (i.e., MAC SDU), segment the MAC SDU into an appropriate size, if required, and attaches additional control information such as CID, ARQ parameters, etc. to the MAC SDU.

The Anchor Data Path Function then encapsulates the output into IP tunnel packet to transmit to Serving Data Path Function through a Type-2 Data Path.

The Serving Data Path Function SHALL de-encapsulate the Layer-2 Data Packets and control information, which was attached by the Anchor Data Path Function, from the packet received through the data path bearer.

7.7.2.2.2.3.3 ARQ State Anchoring

In Type-2 Data Path Function, ARQ state is anchored at the Anchor Data Path Function. In this case, ARQ states, as well as the data packets themselves, SHALL be retained at the Anchor Data Path Function in spite of HOs, and data packets need not be retransmitted over the radio link to recover the state mismatch between MS and network or the state reset are caused by the handover process.

When the Anchor Data Path Function receives an IP packet for an ARQ-enabled connection from the network, it converts the IP packet into Layer-2 Data Packet(s) or packets, as specified in Section 7.7.2.2.2.3.2. If it converts the IP packet into a set of Layer-2 Data Packets, the size of each converted Layer-2 Data Packet SHALL be a multiple of ARQ block size and the content of each Layer-2 Data Packets SHALL be extracted around the ARQ block size boundaries. That is, only a datagram which consists of n tuples of ARQ block SHALL be transmitted through the Type 2 Data Path. For the ARQ-enabled connection, the Anchor Data Path Function SHALL attach ARQ control information, such as Retransmission State, Starting ARQ BSN, etc., to Layer-2 Data Packets. After all Layer-2 Data Packets which are produced from the same MAC SDU, the Anchor Data Path Function SHALL store the MAC SDU and the related ARQ control information locally for possible retransmission request from MS.

The attached information SHALL be used by the Serving Data Path Function to divide a received Layer-2 Data Packet into a set of ARQ Blocks. That is, the Serving Data Path Function divides the received packet into ARQ blocks with the pre-specified ARQ block size, and then assigns an ARQ BSN to each block, with starting from the Starting_ARQ_BSN received from the Anchor Data Path Function through Type-2 Data Path and increasing one for each block.

When an ARQ block(s) is requested to be retransmitted by MS or when an ARQ Ack has not been received for an ARQ block(s) within the pre-specified ARQ timeout, then the Anchor Data Path Function SHALL refer to the ARQ state of the connection to support retransmission according to the ARQ BSN information and update the ARQ retransmission state value. The remaining packet transmission process in the Serving Data Path Function will be the same excepting that it is treated as retransmission.

7.7.2.2.3 Handoff Function

The following types of handovers are supported by the handoff function.

- Mobile initiated handovers at a given serving Base-Station.
- Network initiated handovers.
- FBSS and MDHO (possibility to support MDHO SHOULD be further discussed)

The Handoff Function can be further classified by its roles in handover operation as follows:

- **Serving HO Function**: The Handover function which controls overall HO decision operation and signaling procedures related to HO. It signals the Target HO Function, via zero or more Relaying HO Functions, to prepare for handover, and sends the result to MS.
- **Relaying HO Function:** This Function relays HO related control messages between Serving and Target HO Functions. A Relay HO Function MAY modify the content of HO messages and impact HO decisions.
- **Target HO Function:** The Handover function which has been selected as the target for the handover, or a potential target for the handover.

7.7.2.2.4 Context Function

Due to intra-NAP mobility, there is an MS related context in the network and network related context in MS that need to be either transferred and/or updated. Specifically,

- MS specific context in the Context Function associated with the Serving/Anchor Handoff function needs to be updated.
- MS specific context in the Context Function associated with the Serving Handoff function that needs to be transferred to the Context Function associated with the Target Handoff function. This will also require some of Network specific context in MS to be updated.

This specification defines primitives between peer Context Functions that are used to transfer MS specific context between a Context Function acting as Context-Server and a Context function acting as Context-Client.

The information transfer regarding a specific MS can be triggered in the following scenarios (not exhaustive).

- To populate the context e.g. security context corresponding to a MS at a target Base-Station.
- To inform the network regarding the idle mode behaviors of the MS.
- To inform the network of initial network entry of a specific MS.

The Context Function can be further classified as:

- **Context-Server**: The Context function is the repository of the most updated session context information for MS.
- **Context-Client**: The Context function which is associated with the functional entity that has the 802.16 physical link. It retrieves session context information stored at the Context Server during the handover procedure.
- **Relaying Context Function**: The Context Function which relays information delivery between the Context Server and the Context Client.

7.7.2.2.5 SFID and CID Management

Per IEEE 802.16 Standard Specification, Service Flow ID (SFID) does not change upon HO across BSs belonging to a single NAP, while Connection ID (CID) is defined as temporary in a particular cell coverage area. SFID SHALL be set just once when a layer 2 service flow is originally established, and SHALL NOT be modified by HOs. On the contrary, CID SHALL be refreshed whenever MS moves into a new cell. SFID identifies a particular Layer 2 session while CID specifies a particular logical radio link.

SFID SHALL be assigned when a new service flow is set up and SHALL be maintained as the same value at the Anchor Data Path Function in spite of HOs. In normal situation, CID SHALL be assigned by the Serving BS. However, in handover situation, new CID SHALL be allocated by the Target BS during HO procedures.

In Type 2 Data Path Function, the new CID SHALL be transmitted from the Target Handoff Function to the Serving Handoff Function through the backbone communication and SHALL be mapped to the corresponding SFID at the Anchor Data Path Function to relocate the Data Path. The CID SHALL never be used to identify a session at the Anchor Data Path Function. It is only used as tag information for Layer-2 Data Packet (tunnel) transmission by the Anchor Data Path Function. That is, when a packet is transmitted from the Anchor Data Path Function to the Serving Data Path Function through Type-2 Data Path, the SFID for the packet will be translated into the corresponding CID at the Serving Data Path Function and be attached as a tag to the packet. Therefore, a connection is identified by SFID in the Anchor Data Path Function and by CID in the Serving Data Path Function.

7.7.2.2.6 Data Integrity Consideration During HO

Different class of services imposes different requirements in the quality of the traffic delivered to the MS, which is measured mainly on the basis of data integrity, latency and jitter. The impact of HO in any of these parameters shall be minimized. More concretely, maintaining data integrity during HO implies that the rate of packet loss, duplication or reordering will not be substantially increased as a result of HO, while, at the same time, impact on datapath setup latency /jitter shall be kept to a minimum

From QoS point of view, there are 2 types of HO: controlled and uncontrolled. A controlled HO is the one that respects the following conditions:

- If the HO is MS initiated, the MS shall communicate to the BS a list of potential targets via msg #1 (MOB_MSHO-REQ)
- The network SHALL perform target selection based on the list of potential targets provided by the MS (when MS initiated HO). The anchor DPF or serving DPF may start bi-casting or multicasting to all potential targets.
- The network SHALL communicate to the MS the list of available targets for HO (MOB_BSHO-RSP or MOB_BSHO-REQ). If the list is void, the network refuses to accept MS HO.
- The targets provided by the network to the MS should be a subset of the ones requested by the MS or reported by the MS via MOB_SCN-REP.
- The MS SHALL move to one of the targets provided by the network or reject the HO
- The MS shall perform HO or reject by sending MOB_HO-IND

If any of the above conditions is not respected, the HO is considered as uncontrolled or un-predictive, and QoS is not guaranteed.

If the MS leaves the serving BS before receiving MOB-BSHO_RSP but it succeeds to at least send MOB-BSHO-IND with an indication of the target BS, this is considered uncontrolled HO. In the worst case, the MS may suddenly connect in the target BS without any indication given to the target BS: this is considered as un-predictive HO

Several Data integrity mechanisms are provided, and the selection of Data integrity mechanism is configuration issue. These mechanisms can be classified in 2 main groups: datapath setup and datapath synchronization alternatives.

7.7.2.2.6.1 Data Path Setup Mechanism (Buffer Transferring vs Bi/Multicasting)

Datapath setup mechanisms refer mainly to R6 datapath, but when anchoring (i.e. R4 forwarding or R8 forwarding) the same concepts are applicable. Data integrity mechanisms available for guaranteeing data integrity:

- **Buffering:** Traffic of the services for which data integrity is required is buffered in the datapath Originator or in the Terminator. For one direction traffic, DP Originator is the DP function that sends data to another DP functions, and DP terminator is the DP function that receives data from another DP functions and delivers data through the air-interface. This buffering might be done only during the HO or for simplicity it might be done within the lifetime of the session. The buffering can be conducted in Datapath Originator or terminator. And the buffering in this section is referred to the buffering mechanisms during HO, the buffering point MAY change during HO base on data integrity mechanism selection.

- **Bi/Multi-casting:** This technique consists on multicasting downstream traffic at the Originator endpoint of the datapath. Bicasting is a particular case: traffic is bicasted to the serving element and to only 1 target. There's no such concept as upstream multicast in the context of data Integrity.

These two mechanisms are not mutually exclusive, in fact bi-casting offers a better result when combined with buffering.

While multicasting requires setting up multiple data paths, this is not the case for buffering. Buffering is considered as a datapath setup mechanism since the sequencing of the datapath switch will be determined by where the buffering is done.

7.7.2.2.6.2 Data Delivery Synchronization Mechanism

In order to synchronize guarantee the data delivery in different data functions which buffered the different data paths (serving and target) used to deliver the data during HO, certain synchronization methods can be used and the data need to be synchronized. This synchronization can be achieved in 3 different ways:

(1) Using Sequence number: A sequence number is attached to each SDU in the ASN datapath. This sequence number SHALL be increased by 1 every time a SDU is forwarded in the datapath. There are two options to obtain SN of last transmitted SDU by serving datapath function during handover. One is reported by serving datapath function, and the other is through SDU SN report by MS as described in IEEE802.16e-2005. The used of the SNs is different depending on the buffering mechanism used for maintain the data integrity, example:

a) Buffering in the datapath Originator: For downlink traffic, the serving datapath function MAY report to the Originator an acknowledgement of the SDUs delivered to the MS while the HO start. So after HO, the target DP function becomes Terminator and continue receive data from the SDU next to the last one acknowledged from originator. See section 7.7.6.1.1 for detail

These acknowledgements are not meant to guarantee reliable delivery in the ASN at all times since there's no retransmission)

b) Buffering in the datapath Terminator: if multi / bi-casting is used, the serving terminator SHALL report to the originator the SN of the first SDU need to multicast to the target(s) DP terminators. When actual HO is started, the target terminator start sending the SDU next to the last one acknowledged SDU to MS. See section 7.7.6.1.2 for detail.

If no multicasting is used, After HO, the DP terminating point is changed from serving to the target DP. The SN of last Ack SDU SN is reported to the target terminator. The datapath Originator MAY report to the Serving Terminator the SN of the last SDU for the Serving Terminator to validate that there's no packet in flight in the datapath. The example procedure is demonstrated in section 7.7.6.1.3.

Data retrieving: Without creating SN for each SDU, the Anchor DPF copy/buffer the data during HO preparation, when a final target BS is identified through HO-IND, the serving BS is asked to push back all of its un-sent/un-acked packets to anchor / target DF. See section 7.7.6.1.4 for detail. For sequential delivery, the method can be used with sequence number enable.

Ack window with Sequence number disable: Data Storage buffers in Anchor DP are released by full or partial ACKs from serving BS without sequence number needed. See section 7.7.6.1.5 for detail. The method can be used with sequence number enable also.

7.7.2.2.6.3 ARQ Synchronization

There are two types Data Path in ASN and how to maintain ARQ state synchronization differs between them.

In Type-1 Data Path, ARQ states SHOULD be synchronized. The details are in 7.7.2.2.6.3.1 and 7.7.2.2.6.3.2.

In Type-2 Data Path, ARQ states MAY also be anchored at the ARQ Anchoring which resides in Anchor Data Path Function. The detail is in 7.7.2.2.2.3.3.

7.7.2.2.6.3.1 ARQ Synchronization for Downlink

For ARQ enable traffic, IEEE 802.16e MAC divides the SDUs onto logical parts called ARQ Blocks. All Blocks are of equal size except from the last one in the SDU (the Block Size is a per Connection parameter). Each Block is assigned a sequence number called Block Sequence Number – BSN. The IEEE 802.16e MAC ARQ works with BSNs.

A typical situation with the transmission buffer in the Serving MAC Function, which MAY occur prior to MS leaving, is shown on the Figure 7-45. The transmission buffer in MAC Function might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN. The situation on the Figure 7-45 appears as follows:

- All the Blocks belonging to all the SDUs with SNs lower than Y have been transmitted and acknowledged.
- The first SDU with unacknowledged Blocks is labeled with SN = Y and the Block which corresponds to the beginning of that SDU is labeled with BSN = B. And, the Block with BSN = B has been transmitted and acknowledged.
- The Blocks labeled with BSN = B+1 and BSN = B+2 also belong to the SDU labeled with SN = Y. The Block with BSN = B+2 has been transmitted and acknowledged while the Block with BSN = B+1 has been transmitted but not acknowledged.
- The Blocks from BSN = B+3 to BSN = B+6 belong to the SDU with SN = Y+1. The Block with BSN = B+3 has been transmitted but not acknowledged. The Block with BSN = B+4 has been transmitted but and acknowledged. The Blocks with BSN = B+5 and BSN = B+6 have not been transmitted yet.
- No Block belonging to any SDU with SNs higher than Y+1 has been transmitted.

Thus in order to synchronize ARQ States between the Serving and Target MAC Functions the former SHOULD share with the later the information about the ARQ State and downlink SDU /ARQ Blocks buffers (per Service Flow)

The specific details of how the whole ARQ state is synchronized can be found in stage3.

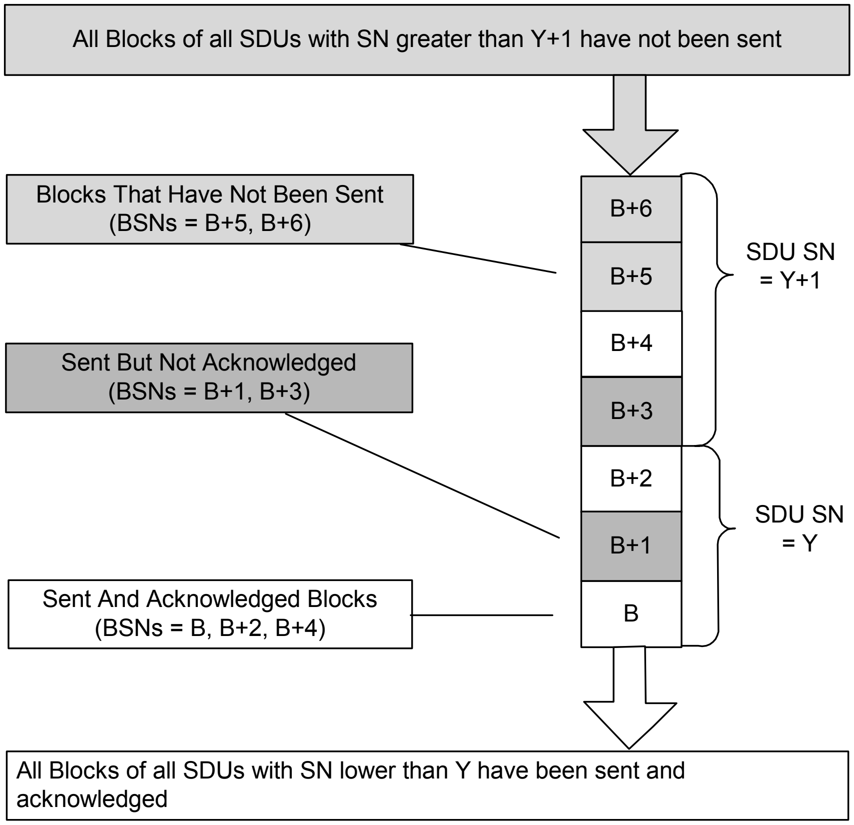


Figure 7-45 - Transmission Buffer in the Serving BS upon MS Leaving

7.7.2.2.6.3.2 ARQ Synchronization for Uplink

A typical situation with the reception buffer in the Serving MAC Function, which MAY occur prior to MS leaving, is shown on the Figure 7-46. The transmission buffer in MAC Function might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN. The situation on the Figure 7-46 appears as follows:

- All the Blocks belonging to all the SDUs with SNs lower than Z have been received and acknowledged.
- The first SDU with unacknowledged Blocks is labeled with SN = Z and the Block which corresponds to the beginning of that SDU is labeled with BSN = b. And, the Block with BSN = B has been transmitted and acknowledged.
- The Blocks labeled with BSN = b+1 and BSN = b+2 also belong to the SDU labeled with SN = Z. The Block with BSN = b+1 has been received and acknowledged while the Block with BSN = b+2 has been received but not acknowledged.
- The Blocks from BSN = b+3 to BSN = B+6 belong to the SDU with SN = Z+1. The Block with BSN = b+3 and the Block with BSN = b+4 have been received but not acknowledged. The Block with BSN = b+5 and the Block with BSN = b+6 have not been received yet.
- No Block belonging to any SDU with SNs higher than Z+1 has been received.

Thus in order to synchronize ARQ States between the Serving and Target MAC Function the former share with the later the information about the ARQ State and uplink SDU /ARQ Blocks buffers (per Service Flow).

When the Target BS receives the synchronization information discussed above it can proceed in one of three possible ways discussed in 7.7.2.2.6.3.2.1, 7.7.2.2.6.3.2.2 and 7.7.2.2.6.3.2.3.

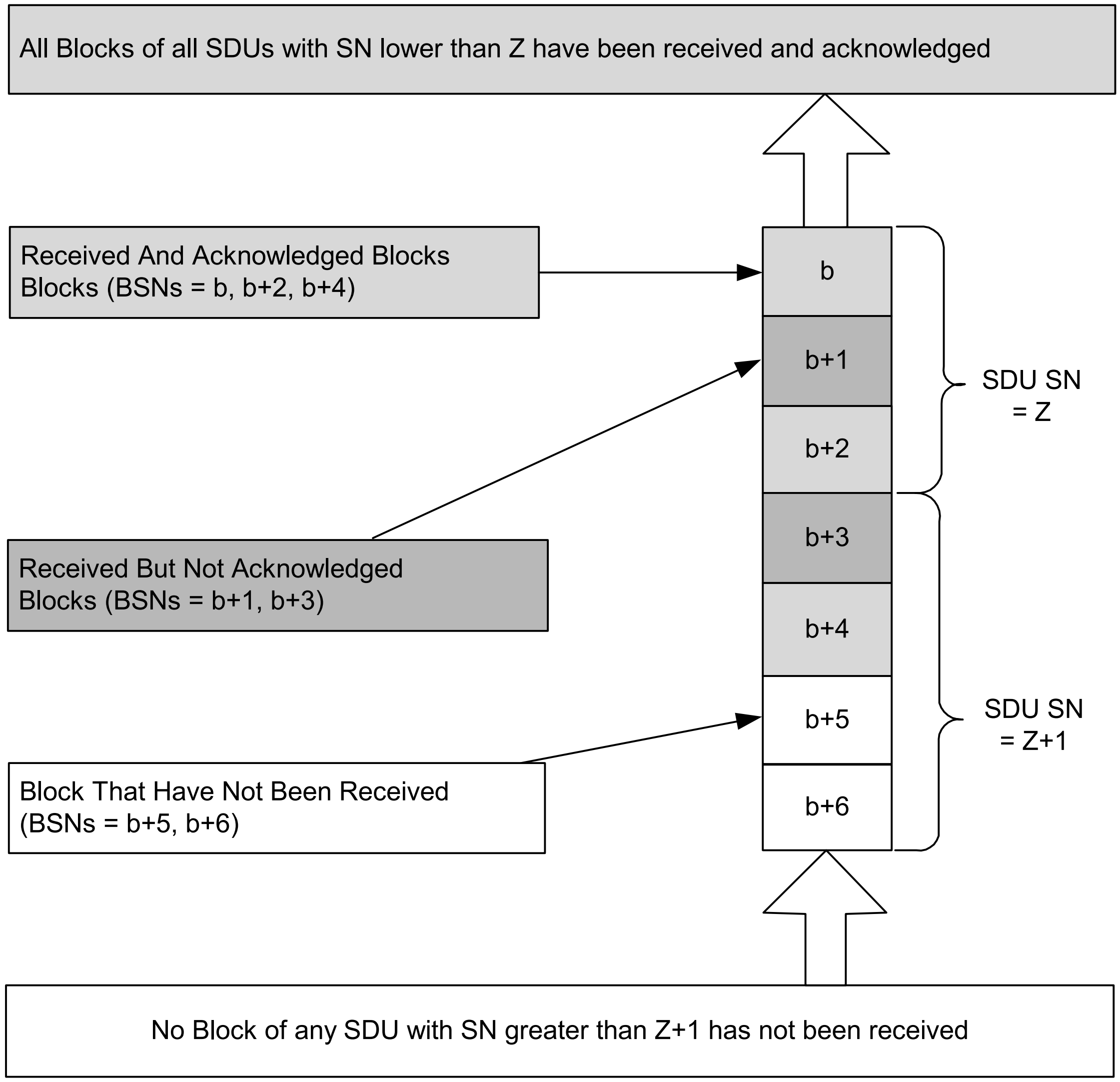


Figure 7-46 - Reception Buffer in the Serving BS upon MS Leaving

7.7.2.2.6.3.2.1 MS Resending Incomplete SDUs

This approach suggests that the Target MAC Function instructs the MS to reset its ARQ state and start transmitting again from the first Block of the first SDU with unacknowledged Blocks. In the example shown on the Figure 7-46 the MS will have to resend Blocks starting with the Block with BSN=b.

This approach allows simple implementation but introduces some overhead over the air.

7.7.2.2.6.3.2.2 Re-Assembly in the Anchor DP Function

This approach suggests that the Target DP Function MAY send fragments of the SDUs to the Anchor DP Function thus delegating reassembly of the SDUs to the latter.

This approach is more complex for implementation, but allows lower overhead over the air.

7.7.2.2.6.3.2.3 Re-Assembly in the MAC Data Path Function

In this approach, only complete SDUs SHALL travel between the MAC and FA function. Upon HO, the source MAC function SHALL transfer any received blocks to the target MAC function along with the acknowledged/un-acknowledged status. The target MAC function SHALL have the responsibility of completing acknowledgement of non-acknowledged blocks as well as re-assembling received blocks into complete SDUs before transmitting uplink to the FA function.

7.7.3 HO Function

7.7.3.1 HO Function Network Transaction

HO Function Transaction is shown in Figure 7-47

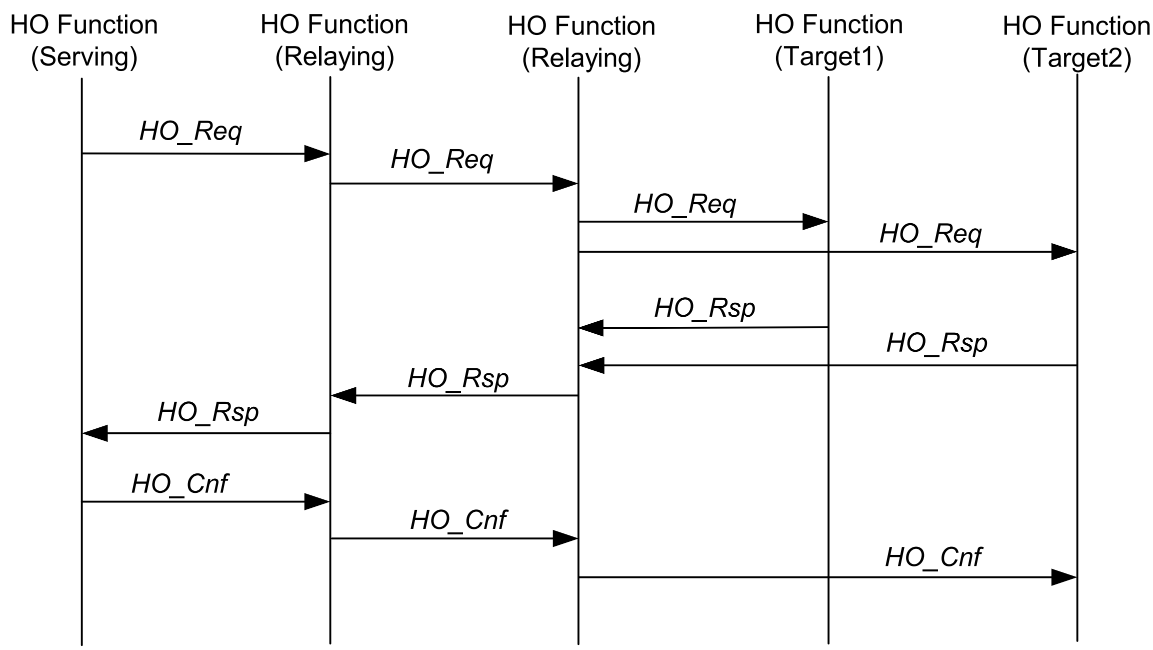


Figure 7-47 - HO Function Network Transaction

a) The Serving HO Function initiates an HO Network Transaction by sending *HO_Req*. There can be only one Serving HO Function for any given HO Network Transaction. After receiving HO IND from MS, serving HO Function the Serving HO Function confirms HO to only one Target HO Function by sending *HO_Cnf*.

b) The Target HO Function responds to the HO Network Transaction with *HO_Rsp*. There can be one or more Target HO Functions for an HO Network Transaction.

c) Serving and Target HO Functions MAY communicate either directly or with assistance of one or more or Relaying HO Functions. If the Serving and Target HO Functions cannot communicate directly for any reason, the Relaying HO Functions take care of delivering the relevant information to the corresponding Target HO Functions. A single HO Primitive (e.g. *HO_Req*) that is sent from the Serving HO Functions MAY contain information relevant for several Target HO Functions. In this case several behavioral policies might be applied, for example:

    - The Relaying HO Functions sends the relevant information in separate primitives to each Target HO Function via zero or more Relaying HO Function. It is the responsibility of the first Relaying HO Functions directly in communication with Serving HO Function to get responses from the Target HO Functions and compile the information into a single response, and it MAY but doesn't have to collect all the responses. This situation is shown in the Figure 7-47 where one of the Relaying HO Functions splits the original *HO_Req* into two ones and sends them to the Target HO Functions. Then the Relaying HO Function, which has split the original *HO_Req*, waits for *HO_Rsp* from both Target HO Functions and sends back a single *HO_Rsp*, which includes the information received from both Target HO Functions.

    - The Relaying HO Function sends the relevant information in separate primitives to each Target HO Function, however it relays only the first response and drops the others.

- The Relaying HO Function behaves like explained in the case) above, however it waits for the responses only for a limited period of time and ignores those that arrived after the time period has expired.

Other policies can be applied as well.

7.7.3.2 HO Function Primitives

7.7.3.2.1 HO_Req

This primitive is used by the Serving HO Function to inform the Target HO Functions about an incoming *HO_Req* from an MS.

HO_Req delivers at least the following Information Elements; other additional information elements MAY be included too:

- **MS ID** which identifies the MS that has requested HO.
- **The list of the Candidate Target BS Ids**.
- **MS/Session Information Content MAY** be attached to the *HO_Req* as well.
- **First requested Bi-cast SDU SN**. This IE is presented if it's lossless HO and synchronization method is sequence number method. It's the Sequence Number of the earliest SDU which hasn't been sent or Acked, and need to be delivered to target DP Function.

7.7.3.2.2 HO_Rsp

The Target HO Function responds to the Serving HO Function with the list of recommended Target BSs.

HO_Rsp is always sent in reply to the *HO_Req*. It delivers the following Information Elements at least:

- MS ID.
- The list of the Recommended Target BS IDs. The list must be a subset of the Candidate Target BS IDs list from the corresponding *HO_Req*. For each target BS in that list, service level prediction information will be included. Ideally the list would contain only one Target BS ID. If the list contains more than one Target BS ID the final selection of the Target BS is up to the MS.
- Info_Support_HO_Optimization Optional information for supporting HO Optimization.
- HO_ID. The optional HO_ID is assigned by Target BS.
- HO Action Time The optional HO Action time is specified by Target BS for assigning Fast_Ranging_IE time, and notifies MS performing re-entry network procedure. In the case TBS decides not to support it, the value 0 is delivered in this parameter.
- First Bi-cast SDU SN. Identifies the SN of the first SDU after the data path has been changed to deal with mobility. This might be used to indicate to the serving DP which is the first SDU bi-cast to the target. Another use of this field is to indicate to the serving DP which is the last SDU sent before the data path changed. The Serving HO Function should trigger the Serving PHY/MAC function to send MOB_BSHO-RSP after the announced SDU has been delivered to the MS. If the IE is omitted the Serving PHY/MAC function may trigger sending MOB_BSHO-RSP at any moment.

7.7.3.2.3 HO Directive

This primitive is used by the related ASN functions to indicate Serving HO Function to trigger a HO procedure, such as .16e function entity, RRC or NRM Entity. HO Directive MAY deliver following Information Elements:

- **The list of the IDs of the handover MSs** which identifies the MS that has been requested HO.
- **The list of the Candidate neighbor BSs Info** This parameter is optional and indicates the HO MS's Candidate neighbor BSs information, such as neighbor BSID, signal quality, etc.
- **Trigger source** which identifies the HO source, such as RRC, NRM, or 16e function entity.

7.7.3.2.4 HO Directive Response

This primitive is used to reply HO Directive primitive, and indicate that the Serving HO Function have already received the HO Directive primitives from the related function entity, such as RRC or NRM Entity. HO Directive Response delivers following Information Elements:

- **Transaction ID**.

7.7.3.2.5 HO_Cnf

This primitive indicates the final HO action such as initiation, cancellation or handover rejection. It is sent from the Serving HO Function to the Target HO Function and conveys at a minimum the following Information Elements:

- **Target BS ID**.
- **MS ID.**
- **Downlink ARQ Sync Info (per Service Flow):** ARQ Context that is necessary to restore communication from the very point it has been interrupted. See discussion in 7.7.2.2.6.3.1.
- **Uplink ARQ Sync Info (per Service Flow):** ARQ Context that is necessary to restore communication from the very point it has been interrupted. See discussion in 7.7.2.2.6.3.2.

Primitives/Content Elements for data flow integrity and sequence synchronization are TBD

7.7.4 Data Path Function

Data Path ID included in Request message means opposite direction's Data Path, and in Response message means opposite direction's Data Path

7.7.4.1 Data Path Function Network Transaction

Data Path Establishment or Release is initiated from the Anchor or Target Data Path Function and terminated by the Anchor or Serving Data Path Function.

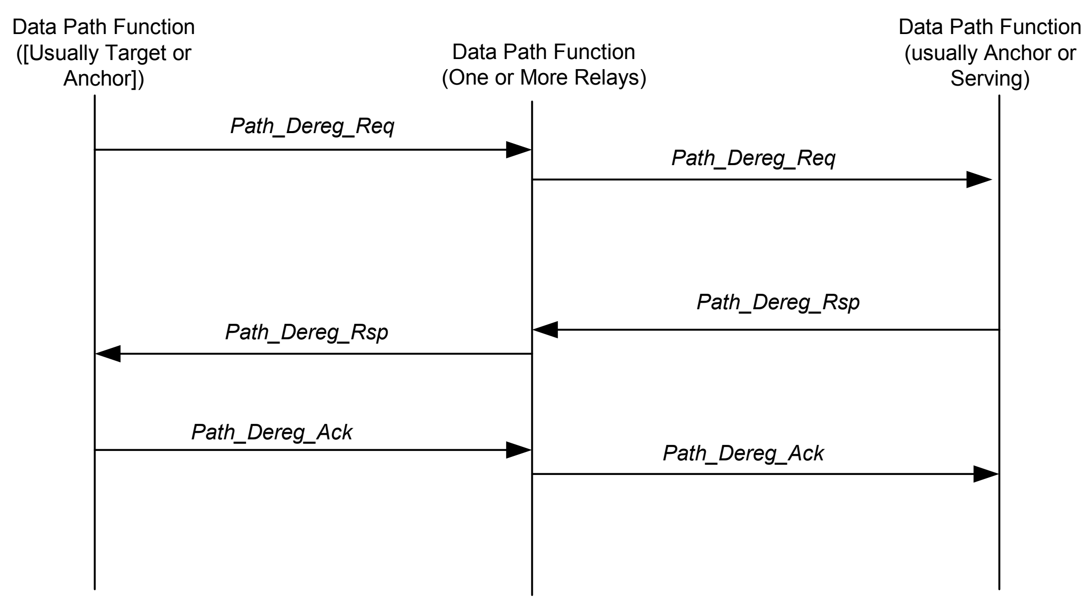


Figure 7-48 - Data Path Function Network Transaction

Data Path Function MAY work in three modes:

a) Target/Anchor Mode. The Data Path Function that initiates a Data Path Network Transaction by sending *Path_Prereg_Req* and *Path_Dereg_Req*. There can be only one Data Path Function in Requesting Mode for any given Data Path Network Transaction.

b) Anchor/Serving Mode. The Data Path Function that responds to the Data Path Network Transaction with *Path_Prereg_Rsp* and *Path_Dereg_Rsp*. There can be only one Terminating Data Path Function for a Data Path Network Transaction.

c) Relaying Mode. The Data Path Function that terminates incoming *Path_Prereg_Req* and *Path_Dereg_Req* messages and generates new *Path_Prereg_Req* and *Path_Dereg_Req* messages related to the same Data Path. The same way it works with *Path_Prereg_Rsp* and *Path_Dereg_Rsp* message as shown in Figure 7-48.

7.7.4.2 Data Path Function Primitives

7.7.4.2.1 Information Elements conveyed with Data Path Primitives

- **Operation ID**. Identifies the operation requested. There four operations: Path Registration, Path De-Registration and Path Pre-Registration, Path Modification.
- **Operation Reason**. Identifies the reason behind the request. The reasons MAY include but are not limited to: Handover, Initial Network Entry, Entering or Exiting Idle Mode, MS loss of carrier, etc.
- **Operation Status**. Success/Failure (used only in Responses).
- **Failure Code** (if Failure)
- **MS ID**. A unique Identifier for the MS (e.g. MAC Address). Data Paths are established to convey data that are either destined to / originated at an MS or an entity behind an MS.
- **Data Path Info.** It describes the Data Path in the direction opposite to that in which the primitive is sent. It potentially includes:
    - **Data Path Type** specifies the type of the Data Path (e.g. GRE, MPLS, VLAN, etc.)
    - **Data Path ID** specifies Data Path ID (e.g. LSP identification for MPLS, GRE Key for GRE, LAN ID for VLAN, etc.).
    - **List of Classifiers** that identify what data SHOULD be classified onto the Data Path and allows optional negotiating Data Path IDs on per microflow (IEEE 802.16 Connection) basis.
    - **Multicast Info**. Specifies relation of the Data Path to the IP Multicast Group.
    - **Endpoint Identifier.** Specifies the addressable subscriber-side endpoint for which the Data Path is being established or maintained.
    - **Data Integrity operation flag:** Indication if data integrity is required for this data path.
- **Data Integrity Info:** It describes the data integrity scheme used during the HO. It potentially includes the following IEs:
    - **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the Originator, Buffering in the Terminator, or Bi/Multi-Casting.
    - **Data delivery synchronization method**: Indication of buffered data delivery synchronization mechanism: sequence number enable, data retrieve with sequence number disable and Ack window with sequence number disable.
    - **Data integrity operation ID:** Specifies the operation which related to particular data integrity mechanisms. There are 3 operations: DP_SYNC-REQ, DP_SYNC-ACK and DP_SYNC-RSP.
    - **First requested Bi-cast SDU SN**: The Sequence Number of the earliest SDU which hasn't been sent or Acked and need to be delivered to target DP Function.
    - **First Bi-cast SDU SN:** Identifies the SN of the first SDU after the datapath has been changed to deal with mobility. This might be used to indicate to the serving DP which is the first SDU bi-cast to the target. Another use of this field is to indicate to the serving DP which is the last SDU sent before the data path changed.

- **Last Packet Indication.** The LPI can be used in the target as an indication that all traffic from the serving has been "synchronized" and normal scheduling of traffic arriving from anchor can be resumed
- **List of lossless session IDs:** Since not all sessions for the MS requires lossless handoff, the list of the lossless session IDs SHALL be included. The session ID is the identifier which can identify a unique service session in the anchor ASN DF.
- **Data retrieve info:** contains the information for data retrieving, such as number of SDU need to be retrieved.

7.7.4.2.2 Path_Reg_Req

Path_Reg_Req is used to handle a registration of a MS, or a MS Flow in the Data Path Function which receives the *Path_Reg_Req*. The registration request is also used for registering the membership of multicast groups corresponding to the MS. It contains the following information:

- **Operation ID**. Set to Path Registration.
- **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info.** Describes Data Path for the direction from the Data Path Function that receives *Path_Reg_Req* to the Data Path Function that sends *Path_Reg_Req*. The content of Data Path info is discussed in 7.7.4.2.1.
- **Anchor DP redirection Indication.** It is used to indicate Anchor DP function relocation when the originating DP function decide to relocate Anchor DP function directly.
- **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this primitives are:
    - **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the Originator, Buffering in the Terminator or, Bi/Multi-Casting.
    - **Data synchronization method**: Indication of buffered data delivery synchronization mechanism: sequence number enable, data retrieve with sequence number disable and Ack window with sequence number disable.
    - **First requested Bi-cast SDU SN**. As described in 7.7.4.2.1.
    - **Data integrity operation ID:** The three following data integrity operation ID can be carried by Path Registration response: DP_SYNC-REQ:
        - DP_SYNC-REQ: It indicates that the indicated sessions SHOULD be lossless handoff. It is sent to the serving ASN DF (from the anchor target DF to the serving ASN DF when there's direct communication between them otherwise is sent from Anchor DF) to establish the a data path for retrieving data synchronization. The primitive conveys at a minimum the following Information Elements.
        - The MS ID and List of lossless session IDs are needed while this operation ID is presented.

For supporting IP multicasts, the primitive is used to indicate that a specific MS is part of the multicast group.

Upon receipt of *Path_Reg_Req*, the Data Path Function which receives *Path_Reg_Req* MAY begin recognizing packets destined for the MS and forward them (using the selected Data Path enforcement mechanism) to the Data Path Function which sends the *Path_Reg_Req* (possibly via Relaying Data Path Functions).

7.7.4.2.3 Path_Prereg_Req

Path_Prereg_Req is used during handovers in order to establish a new Data Path for an MS without destroying the old one. The information the primitive delivers is identical to that of *Path_Reg_Req*, except from the Operation ID which SHALL be set to Path Pre-Registration.

The Data Path Function that receives *Path_Prereg_Req* expects Registration Request to follow in order to complete new DP establishment.

7.7.4.2.4 Path_Dereg_Req

Path_Dereg_Req is used to cancel an existing Data Paths for an MS.

Path_Dereg_Req contains the following information:

- **Operation ID**. Set to Path De-Registration.
- **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info.** Describes Data Path for the direction from the Data Path Function that receives *Path_Reg_Req* to the Data Path Function that sends *Path_Reg_Req*. The content of Data Path info is discussed in 7.7.4.2.1. Data Path Info might be omitted in the *Path_Dereg_Req*. It means that all the Data Paths for the specified MS SHOULD be cancelled.

7.7.4.2.5 Path_Modification_Req

Path_Modification_Req is used to modify attributes of an existing Data Path. It contains the following information:

- **Operation ID**. Set to Path Modification.
- **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info.** Describes Data Path for the direction from the Terminating Data Path Function to the Originating one. The content of Data Path info is discussed in 7.7.4.2.1.

For supporting IP multicasts, the primitive is used to indicate that a specific MS is part of the multicast group. Upon receipt of *Path_Modification_Req*, the Terminating Data Path Function begins modify QoS Info, Data Path Info indicated in the message to the Originating Data Path Function (possibly via Relaying Data Path Functions).

7.7.4.2.6 Path_Reg_Rsp

Path_Req_Rsp is sent in reply to the *Path_Reg_Req*. It contains the following information:

- **Operation ID**. Set to Path Registration.
- **Operation Status**. Success/Failure.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info**. It describes the Data Path in the direction from the Data Path Function that sends *Path_Reg_Req* to the Data Path Function that receives *Path_Reg_Req*. The content of Data Path info is discussed in 7.7.4.2.1.
- **Anchor DP redirection Indication.** It is used to indicate Anchor DP function relocation when the terminating DP function decide to relocate Anchor DP function.
- **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this primitives are:
    - **Data integrity operation ID:** The following data integrity operation ID can be carried by Path Registration response: DP_SYNC-RSP:
        - DP_SYNC_RSP: indicates that the Data Path Sync Request message is received and the corresponding produce is being processed. The received downlink packets for the MS in the serving DF, as well as the un-transmitted downlink packets for the MS in the BS, will be returned to. If the requester was the Anchor DF, where all downlink traffic for this MS is buffered in the anchor DF till the final target DF is identified and the data path is established

between Anchor DF and target DF. It is sent from the serving DF to the anchor DF requester. The MS ID is need while this operation ID is presented.

Upon receipt of Path Registration Response, the Data Path Function that sends *Path_Reg_Req* MAY begins recognizing packets originated from MS and forwards them (using the selected Data Path enforcement mechanism) to the Data Path Function that receives *Path_Reg_Req* MAY (possibly via Relaying Data Path Functions).

7.7.4.2.7 Path_Prereg_Rsp

Path_Prereg_Rsp is sent in reply to the *Path_Prereg_Req*.

It contains the following information:

- **Operation ID**. Set to Path Pre-Registration.
- **Operation Status**. Success/Failure.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info**. It describes the Data Path in the direction from the Originating Data Path Function to the Terminating one). The content of Data Path info is discussed in 7.7.4.2.1.
- **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this primitives are:
    - **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the Originator, Buffering in the Terminator or, Bi/Multi-Casting.
    - **Data synchronization method**: Indication of buffered data delivery synchronization mechanism: sequence number enable, data retrieve with sequence number disable and Ack window with sequence number disable.
    - **First requested Bi-cast SDU SN** As described in 7.7.4.2.1.

7.7.4.2.8 Path_Dereg_Rsp

Path_Dereg_Rsp is sent in reply to *Path_Dereg_Req*. It contains the following information:

- **Operation ID**. Set to Path De-Registration.
- **Operation Status**. Success/Failure.
- **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.9 Path_Modification_Req

Path_Modification_Req is sent in reply to the Path*_Modification_Req*. It contains the following information:

- **Operation ID**. Set to Path Modification.
- **Operation Status**. Success/Failure.
- **MS ID**. As described in 7.7.4.2.1.
- **Data Path Info**. It describes the Data Path in the direction from the Originating Data Path Function to the Terminating one). The content of Data Path info is discussed in 7.7.4.2.1.

Upon receipt of *Path_Reg_Rsp*, the Originating Data Path Function begins recognizing packets destined for the MS and forwards them (using the selected Data Path enforcement mechanism) to the Terminating Data Path Function (possibly via Relaying Data Path Functions).

7.7.4.2.10 Path_Reg_Ack

Path_Reg_Ack acknowledges the completion of a Path Registration Transaction. It contains the following information:

- **Operation ID**. Set to Path Registration.

- **MS ID**. As described in 7.7.4.2.1.
- **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this primitives are:
  - **Data integrity operation ID:** The following data integrity operation ID can be carried by *Path_Reg_Ack*: DP_SYNC-ACK:
    - DP_SYNC-ACK: It indicates that the completion of the retrieve data path establishment. It is sent to the serving DF from the target DF it there's direct communication among them, otherwise it is sent from the anchor DF. The MS ID and Data retrieve IE are need while this operation ID is presented.

Upon receipt of *Path_Reg_Ack* which indicates the completion of final data path registration transaction, the Data Path Function which receives *Path_Reg_Req* MAY begin recognizing packets destined for the MS and forwards them (using the selected Data Path enforcement mechanism) to the Data Path Function which sends the *Path_Reg_Req* (possibly via Relaying Data Path Functions) if this action hasn't been started.

7.7.4.2.11 Path_Dereg_Ack

Path_Dereg_Ack acknowledges the completion of a Path De-Registration Transaction. It contains the following information:

- **Operation ID**. Set to Path De-Registration.
- **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.12 Path_Prereg_Ack

Path_Prereg_Ack acknowledges the completion of a Path Pre-Registration Transaction. It contains the following information:

- **Operation ID**. Set to Pre-Registration.
- **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.13 Path_Modification_Ack

Path_Modification_Ack acknowledges the completion of a Path Modification Transaction. It contains the following information:

- **Operation ID**. Set to Path Modification.
- **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.14 Data-ACK

If the delivery scheme of data integrity uses Ack window, This primitive is sent from serving Data function to Anchor DF to indicate the sequence number of the SDU which has been Acked.

7.7.4.3 Simultaneous Data Path Establishment by Both Peers

The peer Data Path Functions may instigate Data Path Establishment for the same MS simultaneously as shown on the Figure 7-49.

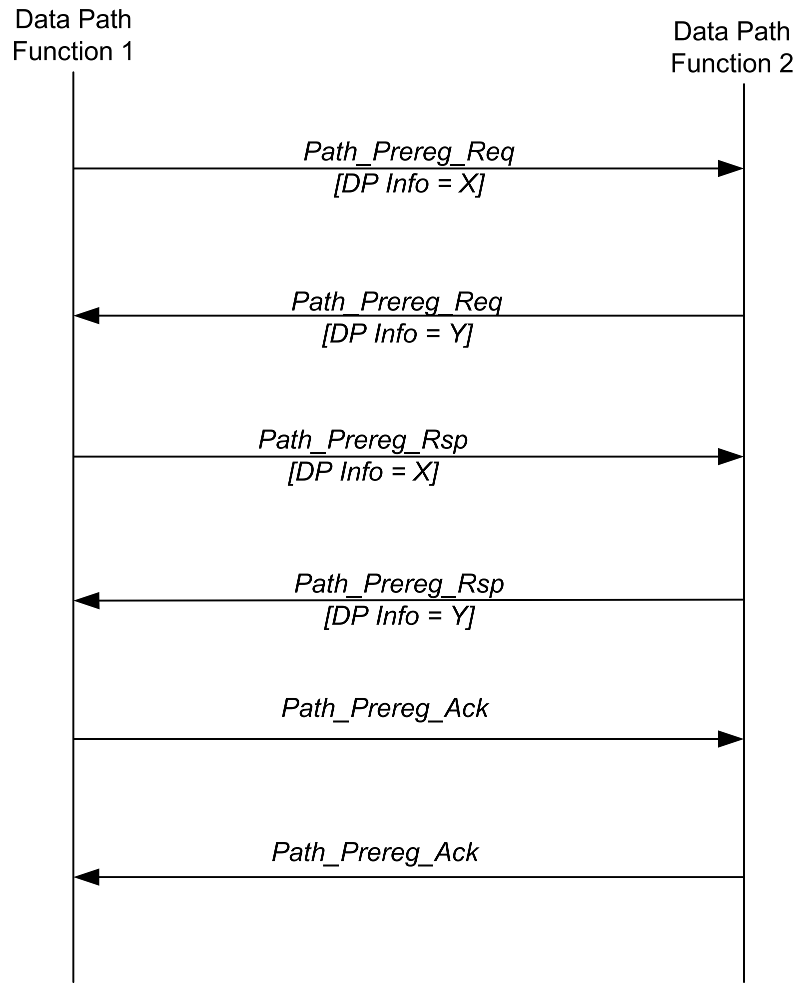


Figure 7-49 - Both Peers Establish Data Path Simultaneously

When such condition take place both peers follow the following rule:

- Both *Path_Prereg_Req* and *Path_Prereg_Rsp* that are sent in the same direction and refer to the same Data Path should convey the same Data Path Info.

This rule utilizes the fact that, in accordance with the definition in 7.7.4.2.1, each peer independently specifies Data Path Info for its respective reception direction and this is why such a collision does not really create a race condition.

In the situation shown on the Figure 7-49, it is enough if only one of the Data Path Establishment transactions succeeds.

7.7.4.4 Target Centric Pre-Registration and Registration during HO

Target Centric refers to an approach according to which the Target DP Function instigates both Pre-Registration and Registration Transactions during HO.

Path Pre-Registration Transaction (*Path_Prereg_Req* and *Path_Prereg_Rsp* and *Path_Prereg_Ack*) is invoked in order to establish a Data Path for an MS between the Anchor DP Function and Target DP Function without destroying the Data Path between the Anchor DP Function and Serving DP Function for the same MS.

It is allowed to pre-register simultaneous Data Paths between the same Anchor DP Function and multiple Target DP Functions.

Pre-establishing Data Paths between the Anchor DP Function and Target DP Functions does not affect forwarding data along the Data Path between the Anchor DP Function and Serving DP Function.

By default when a Data Path between the Anchor DP Function and a Target DP Function is established the data are not forwarded along this Data Path. However other traffic handling options might be negotiated during Path. The data may be forwarded along the pre-established Data Path between the Anchor DP Function and a Target DP Function simultaneously with data forwarding along the Data Path between the Anchor DP Function and the Serving DP Function. Alternatively the data may be buffered for the pre-established Data Path between the Anchor DP Function and a Target DP Function in order to be delivered later upon request. These traffic delivery options are part of the Data Integrity framework.

Path Registration Transaction is invoked when a new Serving Data Path between Anchor DP Function and the DP Function which is a Target DP Function upon beginning of the Transaction and which becomes the new Serving DP Function upon completion of the Transaction. It should not happen earlier than MS arrives to the Target BS/ASN (with which the Target DP Function is associated)

At the moment the Anchor DP Function receives *Path_Reg_Req* from a Target DP Function (which is about to become the new Serving DP Function) it should stop forwarding data along the Data Path to the old Serving DP Function. Shortly after that the Anchor DP Function shall De-Register the Data Path to the old Serving DP Function. The Serving DP Function may also instigate Path De-Registration if it learns from HO Function that the MS has completed HO in the Target BS/ASN.

Path Pre-Registration Transaction may be executed prior to Path Registration Transaction (for the same data path). If Path Pre-Registration Transaction has been completed prior to starting Path Registration Transaction then the purpose of the Path Registration Transaction is only to trigger “data path switch”. In this case *Path_Reg_Req* and *Path_Reg_Rsp* do not have to convey any Informational Elements except from MS ID and, optionally, Data Path ID. The rest of the parameters that are relevant to the data path have to be exchanged during the preceding Path Pre-Registration Transaction. Furthermore in this case Path Registration Transaction is completed with two-way handshake – *Path_Reg_Req* and *Path_Reg_Rsp* exchange without *Path_Reg_Ack*.

As it has been mentioned above, by default the Anchor DP Function does not forward data to a Target DP Function along the corresponding pre-established Data Path (unless a different traffic forwarding option was negotiated upon the Data Path Pre-Registration) In this case the Anchor DP Function may start forwarding data to the Target DP Function immediately after it receives *Path_Reg_Req*. The Target DP Function may start forwarding data to the Anchor DP Function immediately after it receives *Path_Reg_Rsp*.

Figure 7-50 shows the typical sequence for Pre-Registration, Registration and De-Registration Transactions as they likely to occur during HO.

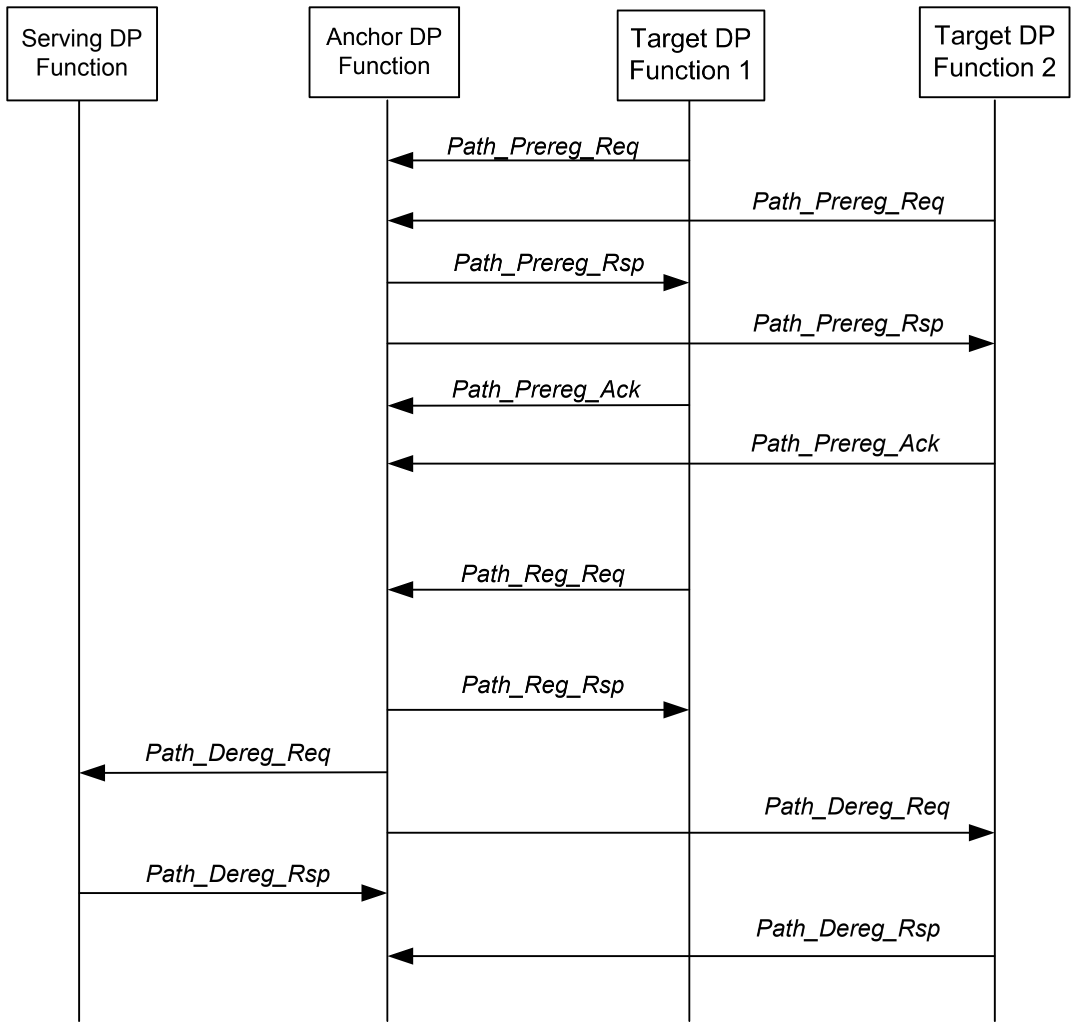


Figure 7-50 - Target Centric DP Control Transactions (with Pre-Registration) during HO

If Path Registration Transaction starts without any preceding Path Pre-Registration Transaction, then Registration Request and Response shall convey all Informational Elements that contain parameters relevant for the data path to be established. In this case *Path_Reg_Ack* shall be sent in response to *Path_Reg_Rsp*. Still, the Anchor DP Function may start forwarding data to the Target DP Function immediately after it receives *Path_Reg_Req*. The Target DP Function may start forwarding data to the Anchor DP Function immediately after it receives *Path_Reg_Rsp*.

Shortly after completing Path Registration Transaction, Anchor DP Function should De-Register the Data Path to the old Serving DP Function. Figure 7-51 shows the transactions involved. The Serving DP Function may also instigate Path De-Registration if it learns from HO Function that the MS has completed HO in the Target BS/ASN.

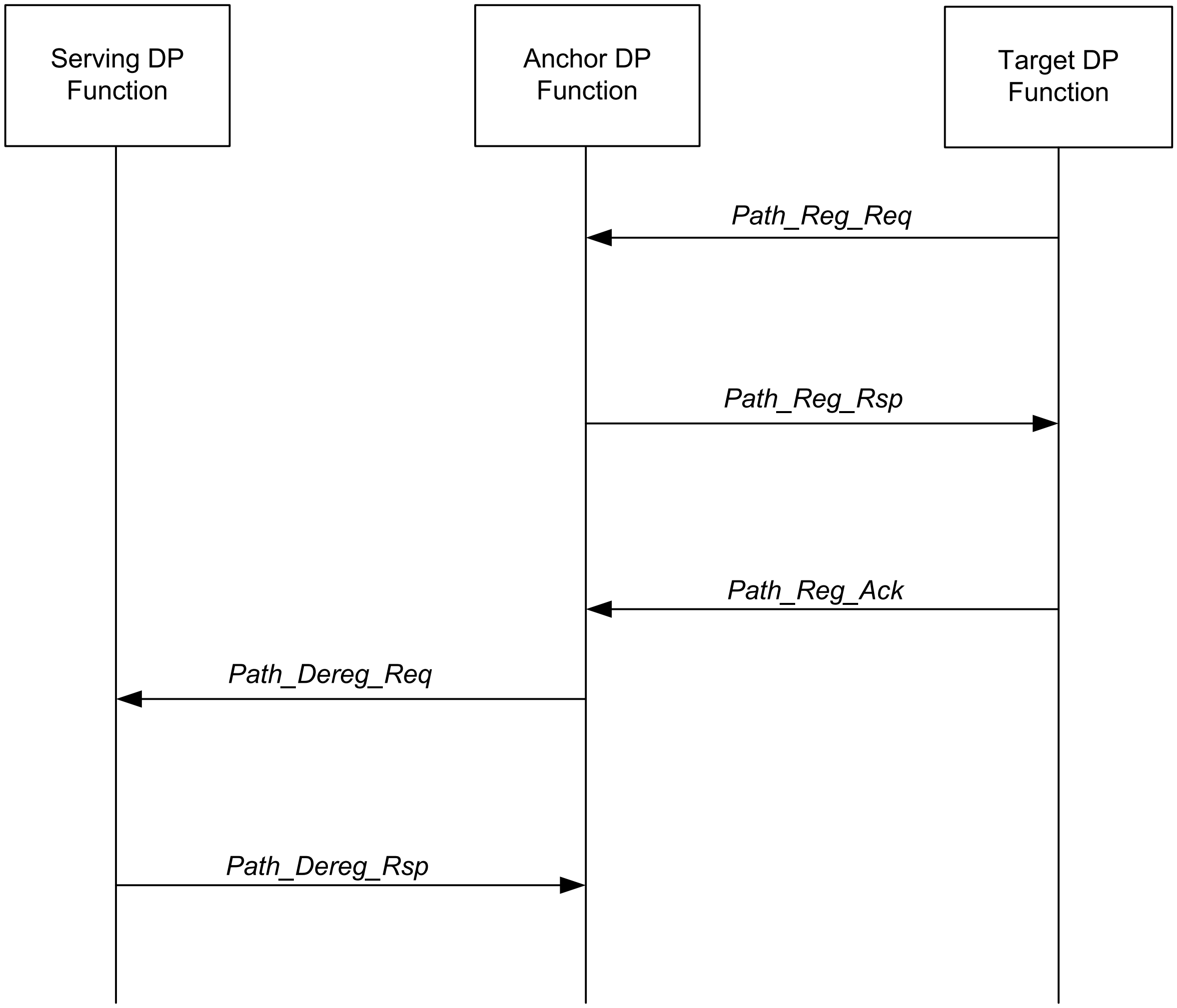


Figure 7-51 - Target Centric DP Control Transactions (without Pre-Registration) during HO

7.7.4.5 Anchor Centric Pre-Registration and Registration during HO

Anchor Centric refers to an approach according to which the Anchor DP Function instigates Pre-Registration Transaction. Registration Transaction however is still instigated by the Target HO Function because the Transaction should not start earlier than MS registers with the Target BS (with which the Target DP Function is associated)

The message processing rules are identical to the rules discussed for the Target Centric approach. Figure 7 52 shows the typical sequence for Pre-Registration, Registration and De-Registration Transactions as they likely to occur during HO.

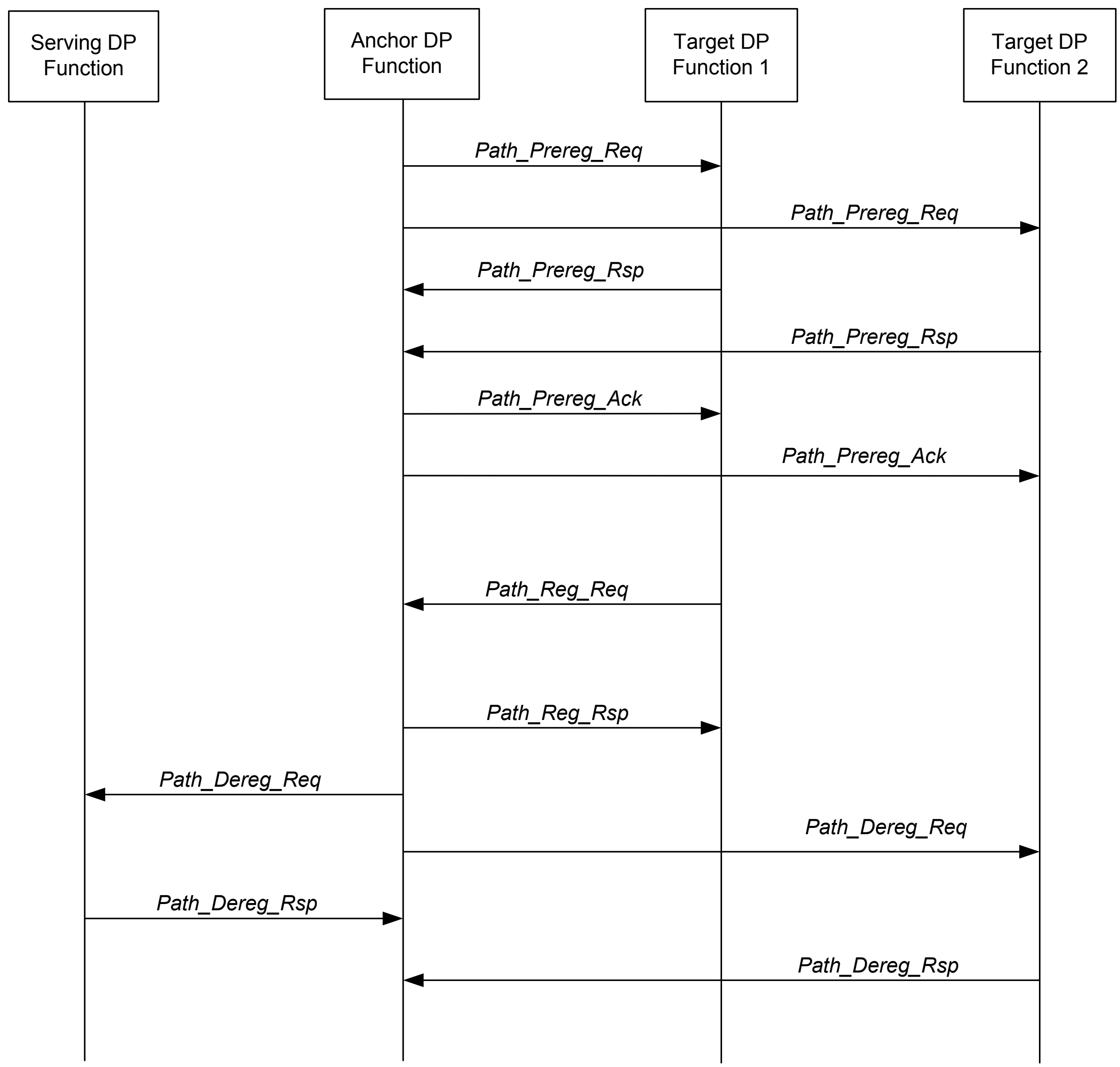


Figure 7-52 - Typical Anchor Centric DP Control Transactions during HO

7.7.5 Context Delivery Function

Context Client MAY request from the Context Server the Session/MS Context (or parts of it).

The Session Info Context MAY include any or all of the following:

- MS NAI
- MS MAC Address
- Anchor ASN GW (profile A&C) or Anchor ASN (profile B) associated with the MS
- List of Service Flow IDs with associated:
    - SF Classifiers
    - SF QoS
    - CID (associated with the SFID)

  - Data Path tagging (ID) Information
  - Etc.
- R3 related information
  - Home Agent IP address
  - CoA
  - DHCP Server
  - AAA Server
  - R3 status Details
- Security Information
  - Security information related to PKMv2 (e.g. SAs and its contexts including TEK, lifetime and PN etc.)
  - Security information related to Proxy MIP (if used)

7.7.5.1 Context Delivery Primitives

7.7.5.1.1 Context_Req

This primitive is used by a network entity to request the session information of a given MS from another network entity.

Context_Req contains type identifiers of the requested Informational Elements belonging to an MS's session context.

The *Context_Req* MAY be used multiple times to derive the set of information required from multiple entities. For example, the security information MAY be delivered via an authenticator.

7.7.5.1.2 Context_Rpt

Context_Rpt might be sent unsolicited or in response to the *Context_Req*.

The entity that received the *Context_Req* SHALL respond with the *Context_Rpt* and include in the response the Informational Elements that have been specified in the *Context_Req*.

The Context Server MAY lack some information requested by the Context Client. Thus the Report does not have to contain all the Informational Elements requested with the *Context_Req*. If the Context Server lacks any requested information it SHALL send an empty Report.

The *Context_Rpt* MAY be unsolicited attached to the HO Control primitives.

7.7.6 Cooperation between the Functions

The Functions described in the sections above trigger each other's operations by issuing internal triggers to one another. With those triggers the information delivered with primitives of one Function might be used in the operations of another Function.

The triggers are out of scope of Stage 2 and are mentioned only to facilitate explanation of the Inter-Function Cooperation. This Cooperation would depend on the actual placement of the Functions. Thus, only examples of Inter-Function Cooperation are given here.

Figure 7-53 and Figure 7-54 shows possible Inter-Function Cooperation in an ASN.

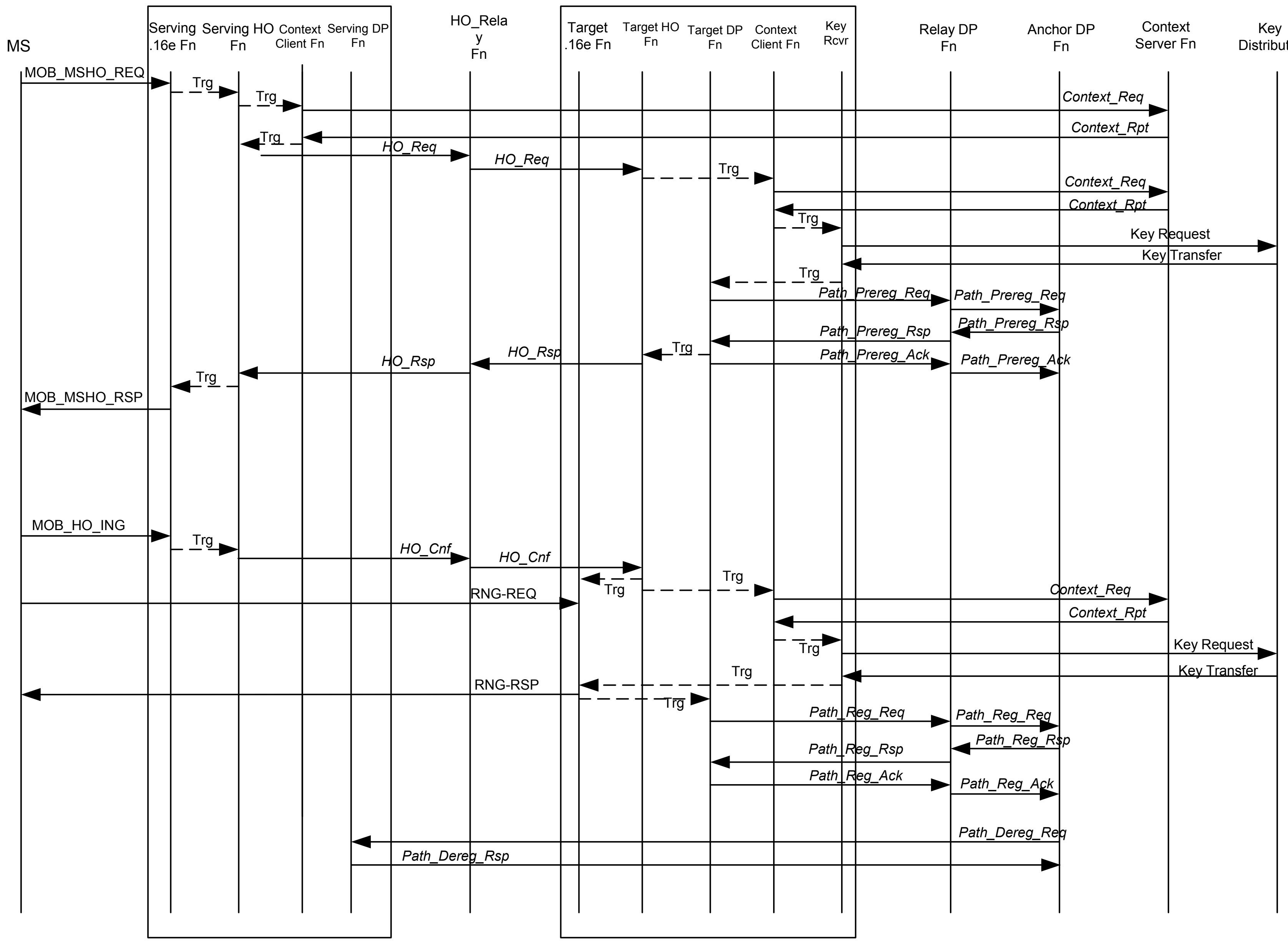

MS
Serving .16e Fn
Serving HO Fn
Context Client Fn
Serving DP Fn
HO_Relay Fn
Target .16e Fn
Target HO Fn
Target DP Fn
Context Client Fn
Key Rcvr
Relay DP Fn
Anchor DP Fn
Context Server Fn
Key Distributor
MOB_MSHO_REQ
Trg
Context_Req
Context_Rpt
HO_Req
Key Request
Key Transfer
Path_Prereg_Req
Path_Prereg_Rsp
Path_Prereg_Ack
HO_Rsp
MOB_MSHO_RSP
MOB_HO_ING
HO_Cnf
RNG-REQ
RNG-RSP
Path_Reg_Req
Path_Reg_Rsp
Path_Reg_Ack
Path_Dereg_Req
Path_Dereg_Rsp

Figure 7-53 - Cooperation between the Functions (Example)

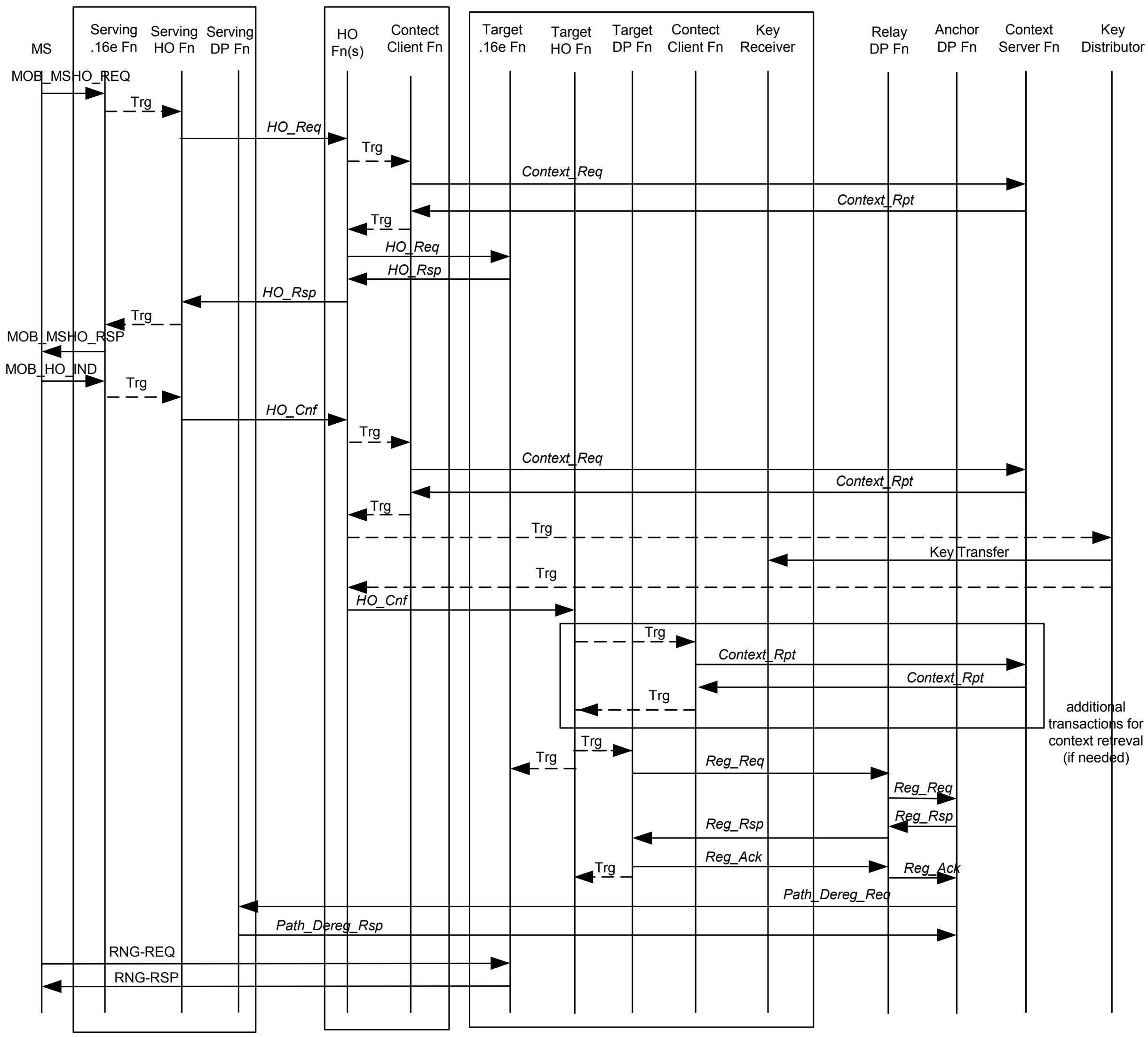


Figure 7-54 - Cooperation between the Functions (Example2)

Figure 7-53 and Figure 7-54 show example scenarios of Mobile Initiated HO:

The MS sends MOB_MSHO-REQ to the Serving .16e Function, which in turn triggers the Serving HO Function to send *HO_Req* to the Target HO Function(s) via the Relay HO Function(s).

The Context retrieval transaction MAY be performed at different points in the HO procedure by different Functional Entity, in different implementations. The three typical points are: before transmitting *HO_Req* to Target HO Function, after receiving *HO_Req* by Target HO Function, and before transmitting *HO_Cnf* to Target HO Function.

In a option, prior to sending the *HO_Req* to the Target HO Function(s), the Serving HO Function (as in the example 1) or the Relay HO Function (as in the example 2) MAY trigger its associated Serving Context Client to request required MS Context (via *Context_Req* and *Context_Rpt* Transaction) which is to be delivered to the Target HO Function with *HO_Req*. It is also possible that a part of the MS Context is delivered here and the other parts are delivered later in time (e.g. when transmitting *HO_Cnf*).

When *HO_Req* arrives to the Target HO Function the latter MAY trigger the associated Context Client Function to send *Context_Req* in order to retrieve the necessary MS Context, if the received *HO_Req* does not have such

Context information (as in the example 1). In this case, the Security Context (e.g. AK, PN associated with AK, etc.) MAY also be retrieved using the Key Distribution Protocol. The MS Context and Key Delivery transactions are optional at this stage. Alternatively these transactions MAY be conducted later when the Serving HO Function or one of Relay HO Functions transmits the *HO_Cnf* to the Target HO Function.

If all necessary MS Context is available in the Target BS(s), then the Data Path Function MAY Pre-Register with the Anchor DP Function via the Relay DP Function(s). This step is optional and is needed only if the Data Path between the Anchor DP Function and the Target DP Function has to be established prior to removing the Data Path between the Anchor DP Function and the Serving DP Function (e.g. for bi-casting). When the optional Pre-Registration is completed the Target DP Function triggers the Target HO Function.

Then the Target HO Function sends *HO_Rsp* to the Serving HO Function.

Upon receiving the *HO_Rsp* the Serving HO function triggers the .16e Function to respond to the MS with MOB_BSHO-RSP.

When the MS is about to leave the Serving .16e Function it sends MOB_HO-IND. The Serving .16e Function in turn triggers the Serving HO Function to send *HO_Cnf* to the Target HO Function via the Relay HO Function(s). Optionally the MS Context and Key Delivery Transactions might be conducted here, and the context and key information are to be delivered to the Target HO Function with *HO_Cnf*.

When *HO_Cnf* arrives to the Target HO Function the latter triggers the Target .16e Function to stand by for MS Network Re-Entry.

And the Target HO Function triggers the Target DP function to Register Data Path with the Anchor DP Function via the Relay DP Function(s), if it receives *HO_Cnf* with MS context and a Data Path has not been made yet. (If needed, the Target HO Function MAY trigger the Context Client to make an additional Context retrieval transaction, before it triggers Target DP Function)

When Registration is completed the Data Path between the Anchor DP Function and the Old Serving DP Function is removed and only the Data Path between the Anchor DP Function and the Target (New Serving) DP Function remains.

7.7.6.1 Data Integrity HO Mechanism

7.7.6.1.1 Anchor DF Buffering with Sequence Number

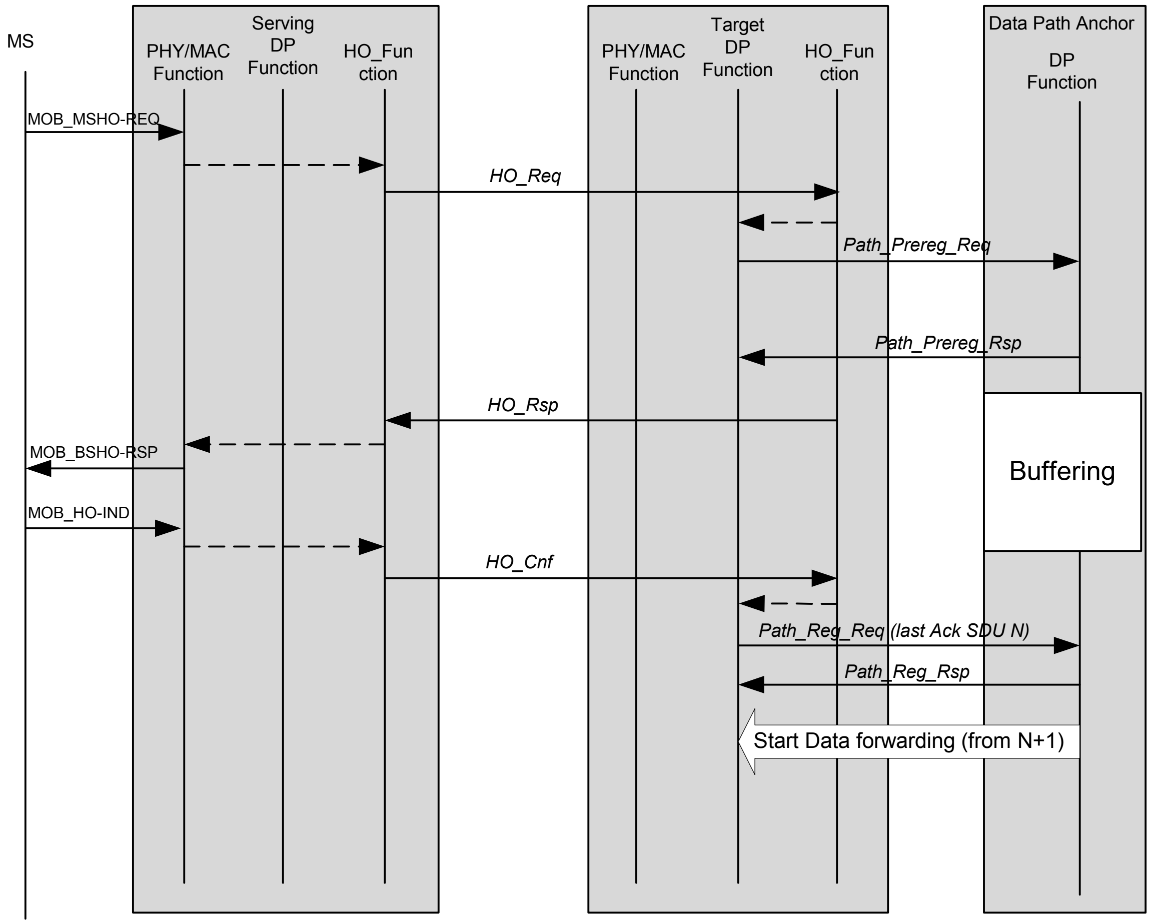
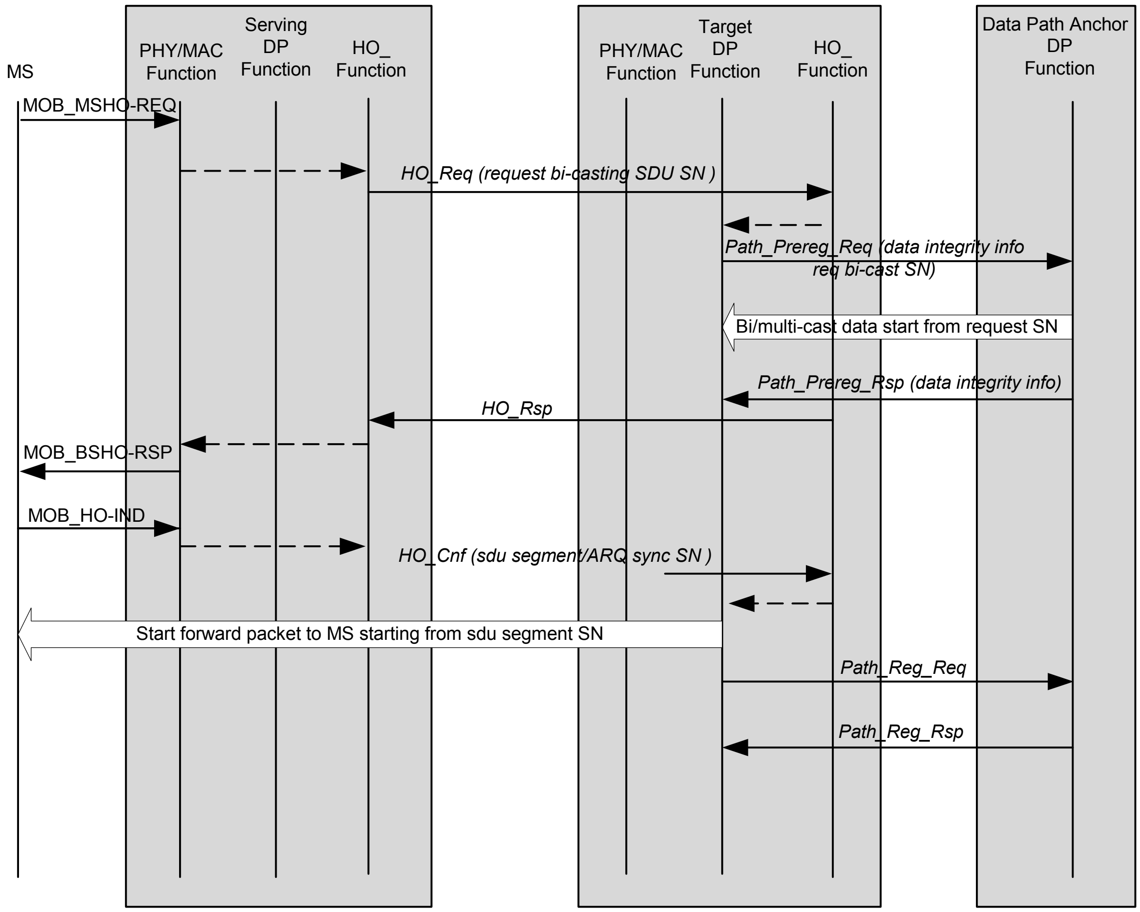


Figure 7-55 - Anchor Data Path Function Buffering with SDU Sequence Numbering

1 **7.7.6.1.2 Anchor DF Bi/Multi-casting with Sequence Number**

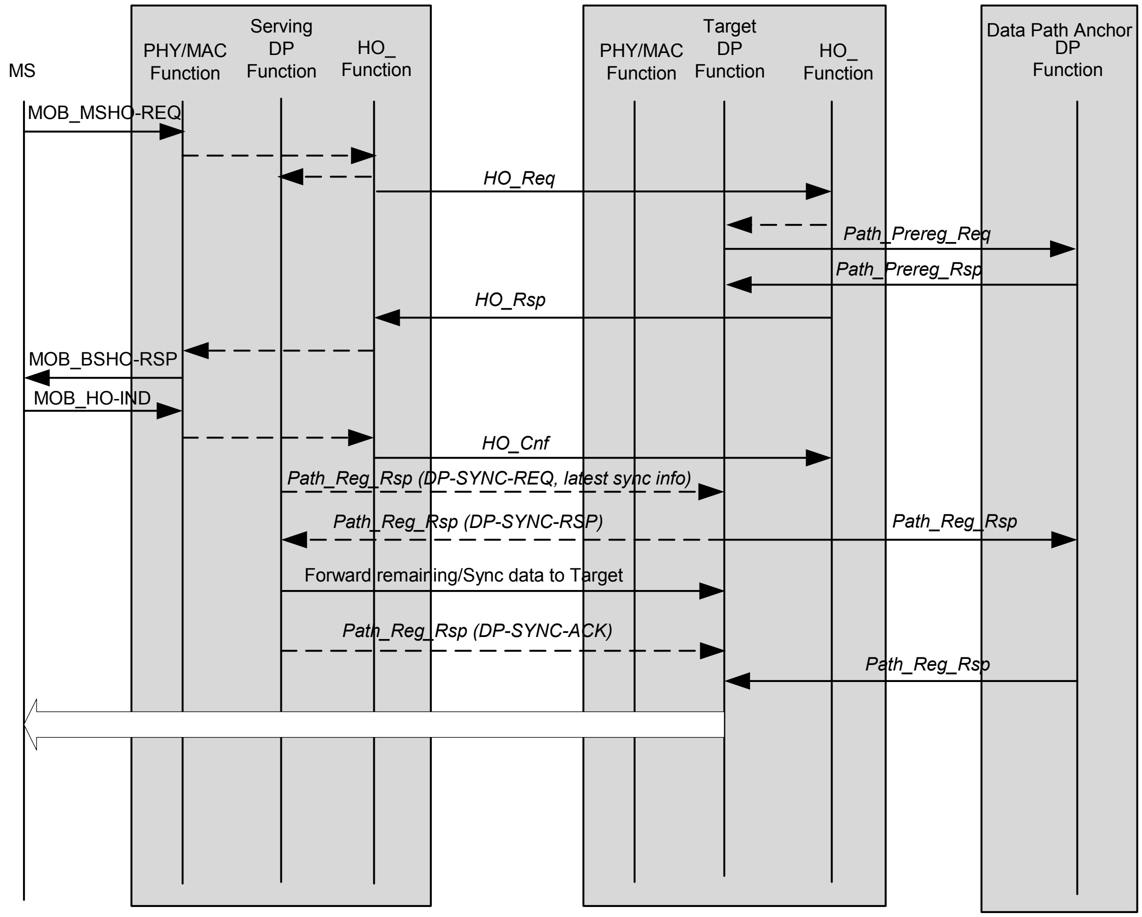


2

3 **Figure 7-56 - Anchor Data Path Function Bi-Cast with SDU Sequence Numbering**[8]

[8] The Target DP Function may be required to buffer the DL packets, once the Anchor DP Function starts bi-casting the traffic

1 #### 7.7.6.1.3 Serving & Target Data Path Function Buffer Transferring

2 

3 **Figure 7-57 - Serving Data Path Function Bi-cast to Target**[9]

---

[9] The Target DP Function may be required to buffer the DL packets, once the Anchor DP Function starts bi-casting the traffic

7.7.6.1.4 Anchor & Target Data Path Function Buffer Transferring

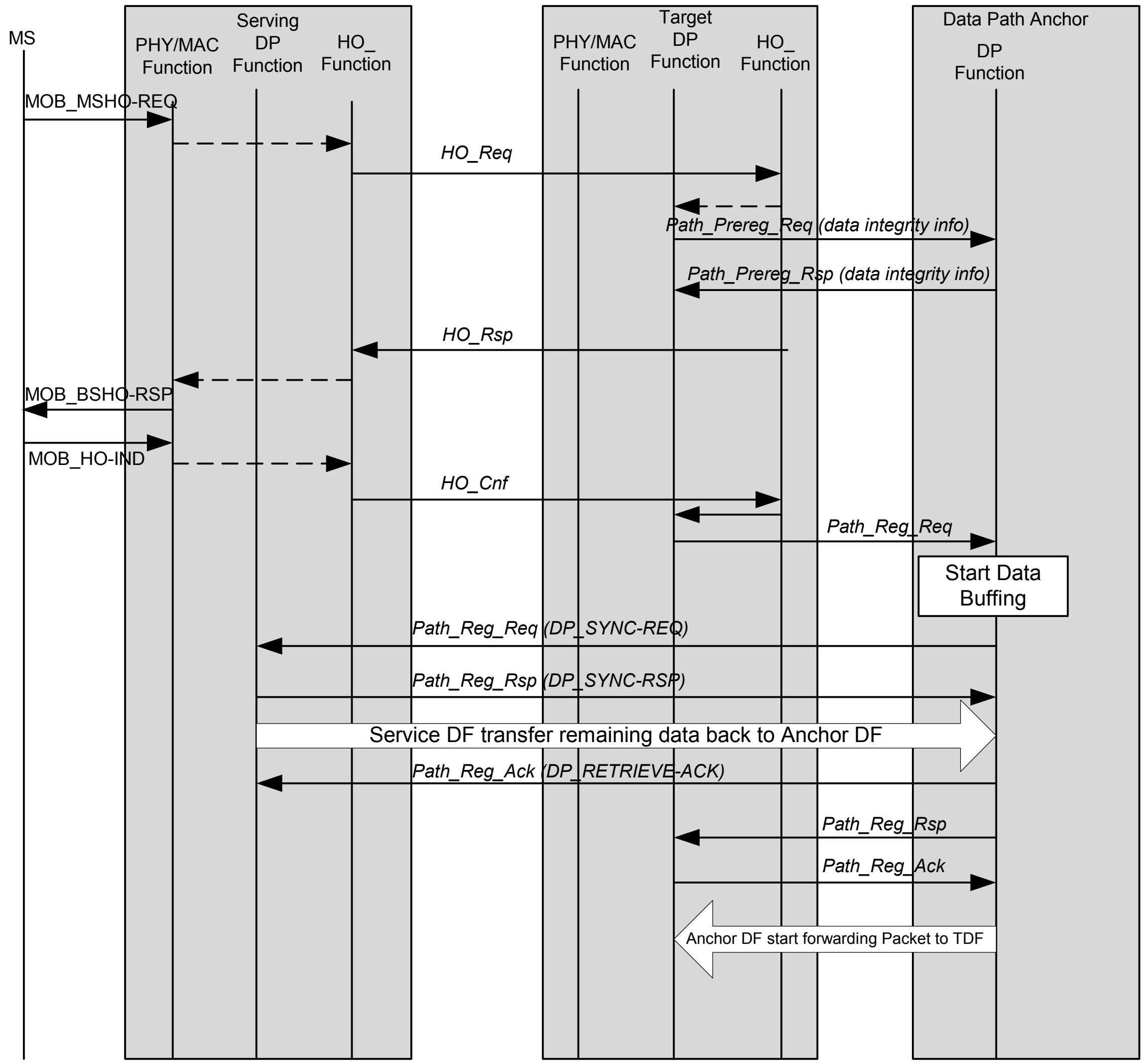


Figure 7-58 - Data Retrieval into Anchored Buffer and Data Forwarding to Target

7.7.6.1.5 Buffering with Ack Window

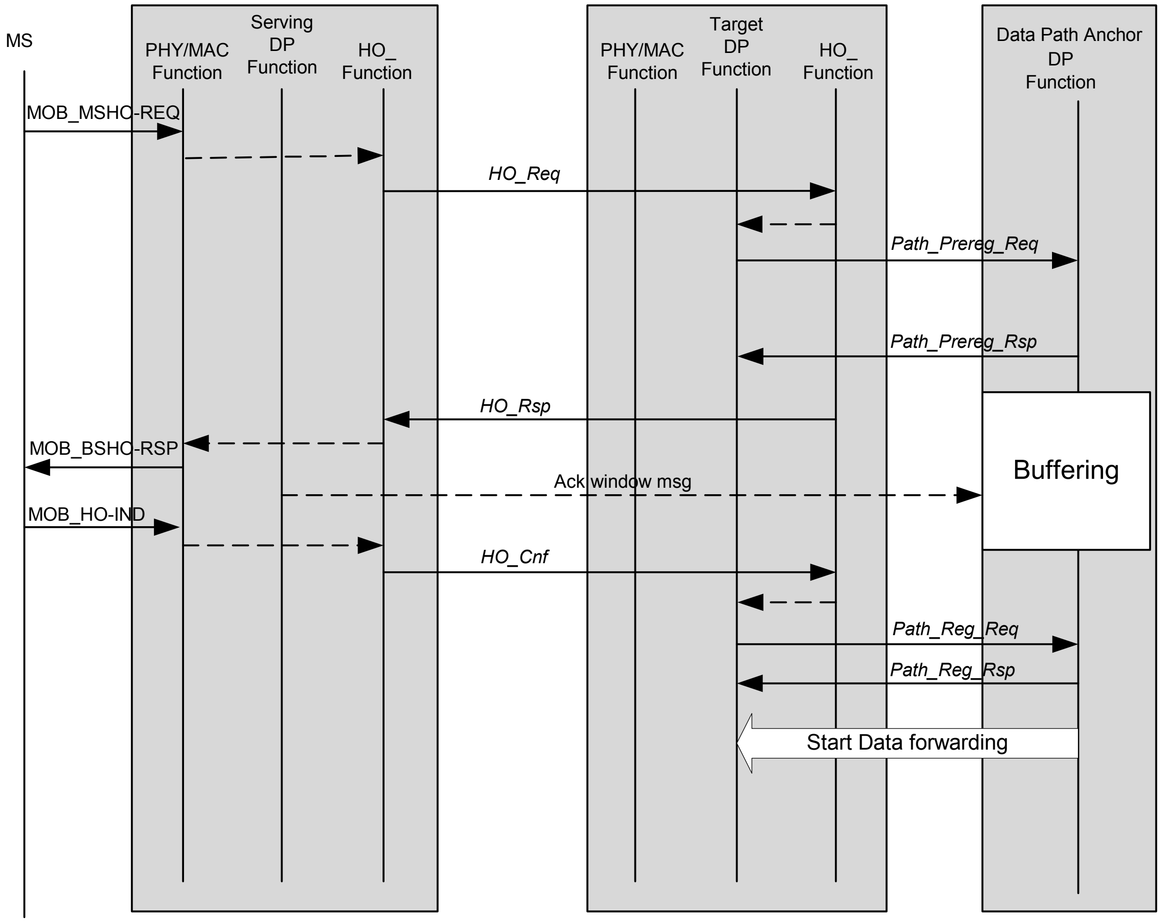


Figure 7-59 - Data Path Anchor Buffering with Sliding Window Forwarding

7.8 CSN Anchored Mobility Management

7.8.1 Scope and Requirements for CSN Anchored Mobility (MIPv4) Management

7.8.1.1 Scope

This section describes mobile IP based macro mobility between the ASN and CSN across the R3 reference point. In the case of IPv4, this implies re-anchoring of the current FA to a new FA and the consequent binding updates (or MIP re-registration) to update the upstream and downstream data forwarding paths. The procedures described in this section complement the procedures outlined in Section 7.7 (where ASN—anchored mobility management procedures are discussed without changes to the anchor FA in the case of IPv4).

The WiMAX mobility solution consists of two mobility levels:

- ASN-anchored mobility or micro mobility is when the MS moves between Data Path Functions while maintaining the same anchor FA sitting at the northbound edge of the ASN network. The data flow between CSN and Data Path Functions pivots at the anchor FA. CSN is unaware of any mobility that occurs between ASN Data Plane Functions. This scenario is covered in Section 7.7.

- CSN 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.[10]. This chapter describes the solution for this type of mobility.

The following additional considerations apply for R3 mobility management:.

- CSN Anchored Mobility Management SHALL be established between ASN and CSN that are in the same or different administrative domains.
- The mobility management MAY extend to handovers across ASNs in the same administrative domain. (See Figure 7-60)
- Inter-technology handovers are outside the scope of Release 1.0.0.

The CSN Anchored Mobility Management procedures MAY not be synchronized with the event of MS changing its point of attachment to the ASN. In other words, the procedures MAY be delayed relative to the completion of link layer handover by the MS.

Figure 7-60 illustrates the CSN Anchored Mobility Management scope for IPv4 based mobile IP. In an intra NAP R3 mobility case, a MS is mobile between FAs within a single NAP domain. As shown, the R3 mobility event results in a handover between two FAs, thereby relocating the ASN R3 reference anchor point in the NAP.

Note that Inter-NAP R3 mobility is not supported in Release1.

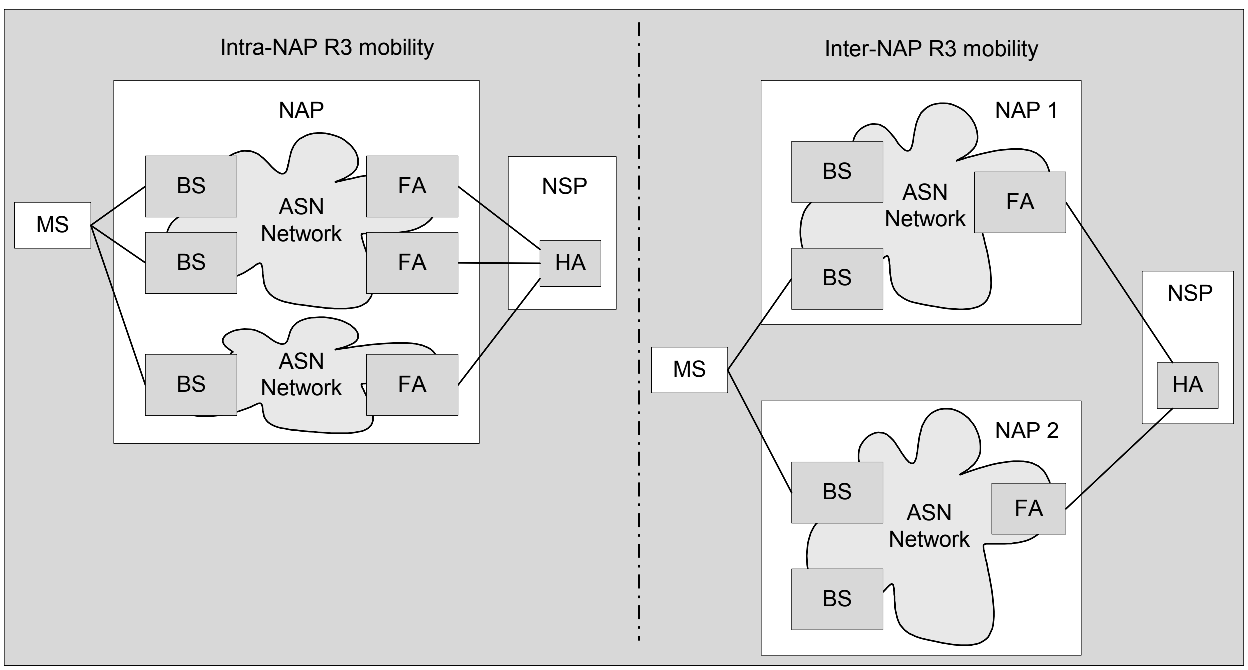


Figure 7-60 - R3 Mobility Scope

7.8.1.2 Functional Requirements

The following functional requirements have been identified for CSN Anchored Mobility Management:

- CSN Anchored Mobility Management for IPv4 SHALL be based on [43] and related RFCs. Proxy-MIP differs from client-based MIP in that the ASN network performs the role of the Mobile Node (MN).

[10] The scope of this version of the document only covers the inter/intra-ASN handover (R3 mobility) between FAs belonging to the same NAP.

- R3 mobility SHALL NOT automatically terminate or otherwise interfere with idle/sleep mode of operation of the MS. CSN Anchored Mobility Management SHALL accommodate the scenario in which MS remains in idle/sleep state until it is ready to send upstream traffic or is notified of downstream traffic from the network and relinquishes the idle/sleep state.
- Reverse tunneling between ASN and CSN SHALL be supported.
- In all non-roaming scenarios, the HA SHALL be located in the CSN of Home-NSP. For roaming scenarios, the HA MAY be located in the CSN of either the Home-NSP or Visited-NSP depending on:
    - Roaming agreement between Home-NSP and Visited-NSP.
    - User subscription profile and policy in Home-NSP
- CSN Anchored Mobility Management within a single NAP administrative domain SHALL introduce minimal latency and packet loss.
- Make-before-break operation (when coupled with ASN-anchored mobility procedures described in Section 7.7) SHOULD be possible within the same NAP administrative domain. To accomplish this, the previous anchor SHOULD be capable of maintaining continuous data flow while signaling to establish the data path to a new anchor FA.
- It SHALL be possible to generate triggers to re-anchor at any time independent of ASN-anchored mobility.
- From a MIP point of view an MS SHALL always operate as if in a foreign network.
- Both the CMIP and PMIP mobility schemes are mandatory.
- Efficient use of wireless link. Extra overhead over the air-interface to accomplish CSN Anchored Mobility Management SHALL be minimized.

7.8.1.2.1 PMIP-Specific Functional Requirements

- PMIP procedures SHALL NOT require additional signaling over the air or additional data headers to complete CSN Anchored Mobility Management.
- MS SHALL be unaware of CSN Anchored Mobility Management activities.
- Use of DHCP by the MS for IP address assignment and host configuration SHALL be supported.

7.8.1.2.2 CMIPv4-Specific Functional Requirements

- MIP [43] specified procedures SHALL be used on MS for IP address assignment and host configuration.

7.8.1.3 R3 Mobility Security Requirements

7.8.1.3.1 Intra-domain Security

- When FA and HA are in the same administrative domain a trust relationship (via established FA-HA security association) is assumed between the FA and HA. The set of the FA-HA security associations is an implementation and/or operational issue that are outside the scope of this specification.

7.8.1.3.2 Inter-domain Security

- FA and HA, which are in different administrative domains, need to set up a trust relationship for mobility signaling.
- Mobility service authorization for MS is needed to set-up data forwarding.
- Signaling between ASN and CSN SHOULD be secure:
    - For PMIP, the H-AAA will derive the PMIP MN-HA key for a particular MS to the ASN during network access authentication process. The PMIP MN-HA key is unique for each MS; key sharing between MS SHALL NOT be allowed.

- Mobility service key is used to set up forwarding path via dynamically established tunnels between FA and HA.
- User Data encryption is out of the scope of this document.
- The choice of authentication methods SHALL comply with [43]. For example, HMAC_SHA1 can be applied to protect the signaling for now. More importantly, authentication mechanism SHALL be extensible to support future cryptography.

7.8.1.4 CSN anchored mobility (R3 Mobility)

This section describes requirements and procedures for Mobile IPv4 based R3 mobility management.

Mobile IP (MIP, RFC 3344 and related RFCs for IPv4) is adopted as the mobility management protocol for all applicable usage/deployment scenarios requiring seamless inter-subnet/inter-prefix layer-3 handovers. Within the Mobile IP framework, an MIP client maintains a persistent Home IP address when handing off between different FAs. The R3 Mobility solution has four functional components— a MIP client, an Foreign Agent (FA) located in the access network, a Home Agent (HA) typically located in the user's home network (but MAY be dynamically assigned/requested from a visited operator's network) and a AAA server.

For CSN Anchored Mobility Management two variants of the MIP protocols are supported:

- Client MIP (CMIP): CMIP is an IETF compliant MIP solution based on a Mobile IP enabled MS. CSN Anchored Mobility Management will cover CMIP based mobility schemes for IPv4 and IPv6.
- Proxy MIP (PMIP): Proxy MIP is an embodiment of the standard Mobile IP framework in which an MN is transparently instanced in the access network on behalf of a client that is not MIP-aware or MIP-capable.

7.8.1.5 CSN Anchored Mobility Management triggers

The following types of event can trigger the procedure:

- *MS mobility:* The MS hands off to a new Base Station under a new FA.
- *Wake-up from idle mode*: The MS wakes up from the idle mode at a different ASN than the one under which it entered the idle mode.
- *Resource optimization:* The network decides for resource optimization purposes to transfer the R3 endpoint for the MS from the serving FA to a new FA, independently of any MS movement.

7.8.1.6 MIP Extensions

The following standards SHALL be used for Mobile IPv4 operations with any limitations or extensions described in this document:

- Mobility support for IPv4 [43]
- Reverse Tunneling [29]
- NAI Extension [22]
- Registration Revocation [45]

The following standards MAY be used for Mobile IPv4 operations with any limitations or extensions described in this document:

- Foreign Agent Challenge [28]
- Mobile IP Vendor/Organization Specific Extensions [33]

7.8.1.7 Addressing Support

7.8.1.7.1 Private HoA Address Support

It is possible that two different MS served by the same FA have the same, overlapping private address because they belong to two different private networks.

7.8.1.7.2 Dynamic Home Agent Assignment

In roaming cases the Home Agent can be assigned by either the Home NSP or the Visited NSP. It's the home operator that will decide based on the roaming agreement with the visited operator and/or the end-user's subscription profile which network is responsible for assigning the MIP Home Agent.

If a Home Agent is assigned in the visited network the MIP authentication will take place between the visited HA and the Home AAA server. Security exchanges are transparent to the visited AAA proxy.

If the HA is to be assigned by the Home CSN both the Home Agent address and optionally the DHCP server address or HoA address are appended to the AAA reply by the Home-AAA server.

For Home Agents in the Visited CSN the AAA proxy can append the Home Agent address and the optional DHCP server address or HoA address to the AAA exchange between the home AAA server and the authenticator.

For static agreements between two operator domains (e.g. HA always in the visited network) the AAA proxy can be configured to add a HA address based on the Home-AAA server domain.

For more dynamic Home Agent location algorithms (e.g. based on subscription profile) the AAA proxy decision to append the HA address will depend on the presence of the HA address container in the AAA reply from the home AAA.

Although not considered very scalable the address of a HA in the visited network can be provided by the home AAA server based on pre-configured information.

The Home Agent can be provided in the form of an IP address or a FQDN (Fully Qualified Domain name).

7.8.1.7.3 Dynamic HA: PMIP Considerations

The PMIP security information is always exchanged between the Home AAA server and the authenticator.

The PMIP client will insert the HA address retrieved during the access authentication step in the MIP Registration Request.

7.8.1.7.4 Dynamic HA: CMIP Considerations

The network SHALL support dynamic HA allocation algorithm. When the FA receives an Registration Request from the MS with an HA IP address value of 0.0.0.0, the HA will be assigned based on the AAA HA attribute downloaded during the access authentication step and its HoA address returned in the Home Address field of the RRP.

7.8.1.7.5 MIP Addressing

The FA SHALL support [22] NAI extension.

If the HA address provided by the CMIP client is different from the HA address downloaded during access authentication the FA MAY decide (depending on operator policies) to forward the Registration Request to the dynamically assigned HA unicast address. The HA MAY accept the Registration Request contrary to [43] or MAY reject it with an error code of 136 in accordance to [43]. The HA SHALL put its own IP address in the Registration Reply. The FA SHALL use a publicly routable and visible address as the CoA address.

7.8.1.8 Proxy MIP R3 Mobility Management

Proxy-MIP R3 mobility is based on MIP signaling between MIP client, FA and the Home Agent. In the proxy-MIP approach the MIP client resides within the ASN network and performs R3 mobility management on behalf of the MS. Co-location between the proxy-MIP instance and the Authenticator functional entity in the ASN is assumed;

i.e. any communication between these two entities is beyond the scope of this document. The R3 mobility FA is located at the northbound boundary of the ASN. The Home agent is located in a CSN network.

Proxy-MIP does not put additional requirements on the MS in order to support R3 mobility and is fully network controlled.

To distinguish between a PMIP instance managing the R3 mobility for a single user and the functional entity combining all these logical instances a new definition is introduced:

1. **PMIP Mobility Manager**: Functional entity managing multiple PMIP clients
2. **PMIP client**: Logical entity managing R3 Mobility for a single user/MS

In other words a ‘PMIP Mobility Manager’ = Σ ‘PMIP clients’

Any R3 mobility session or PMIP client is uniquely identified by the user’s NAI. The NAI used for R3 Mobility can be the same as the one used for access authentication.

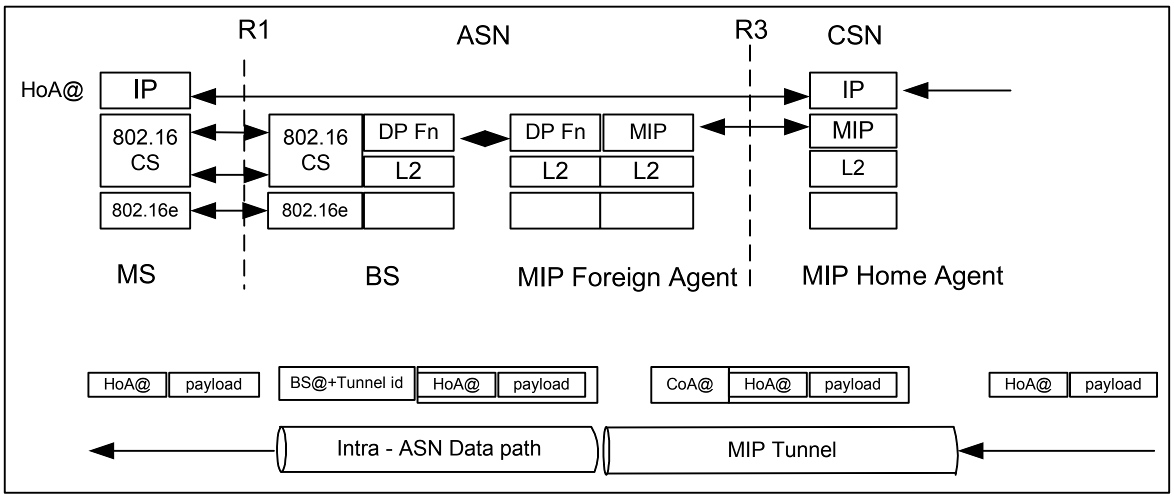


Figure 7-61 - Proxy MIP Data Plane (Example)

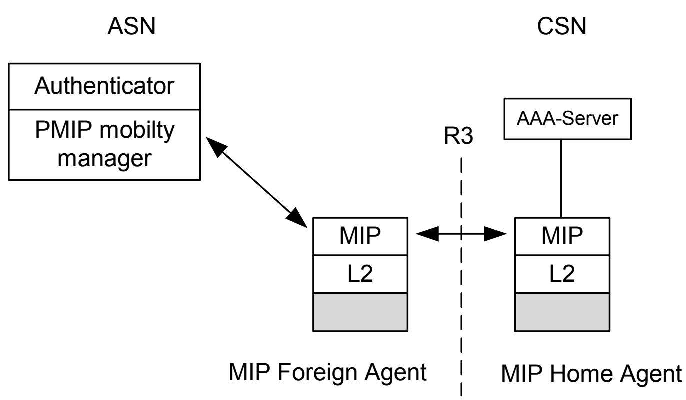


Figure 7-62 - Proxy MIP Control Plane

In the proxy MIP solution, the IP network aspects of the CSN Anchored Mobility Management handovers are transparent to the MS. The MIP registration to set up or update the MS’s forwarding path on the HA is performed by the proxy-MIP client on behalf of the MS. The MIP related information required to perform MIP registrations to the HA are retrieved via the AAA messages exchanged during the authentication phase. This information consists of Home Agent address, and the security information to generate the MN-HA authentication extension and either the DHCP server address or HoA address.

7.8.1.8.1 Proxy-MIP FA Considerations

Additionally, in applicable ASN configurations the alternative PMIP redirection procedure as described in Section 7.8.1.8.7 MAY be used.

As illustrated in Figure 7-62 the Foreign Agent behavior for proxy-MIP differs slightly from RFC3344 in that the destination IP addresses for the control and data plane are different.

In the IETF MIP model the MIP client resides on the host and is the termination point for both the MIP signaling and user traffic. In PMIP approach user data is sent to the MS over the corresponding R6 or R4 data path, MIP signaling needs to be directed to a PMIP client within the PMIP mobility manager.

To achieve this goal, odd-numbered MN-HA SPI is used as an indication of PMIP usage.

Messages originated by the PMIP mobility manager will set the IP packet source address to the address of the PMIP mobility manager.

MIP Registration Reply will be returned to the PMIP mobility manager instead of the MS by FA. The PMIP mobility manager address is not directly linked to an MS's R3 mobility session and can be changed at any time independently of an ongoing R3 mobility session.

7.8.1.8.2 DHCP server/proxy consideration

There are two DHCP server/proxy deployments options for CSN anchored mobility in Release 1.0.0:

2) DHCP proxy: There is DHCP proxy in the ASN acting as DHCP server to manage DHCP exchange with MS. There is no DHCP messages cross R3.

3) DHCP relay: There is DHCP relay in the ASN to forward the DHCP messages between the DHCP server in the CSN and MS. There are DHCP message cross R3.

7.8.1.8.3 Proxy-MIP Connection Setup Phase

After successful access level authentication the R3 mobility connection setup takes place.

During R3 mobility connection-setup following actions are performed:

- Location of the Home-Agent is determined based on inter operator policies.
- MS PoA assignment
- MS IP host configuration
- MIP registration
- R3 mobility authentication between MN and HA

The following signaling flow describes the connection setup phase for the Proxy-MIP solution using DHCP Relay option.

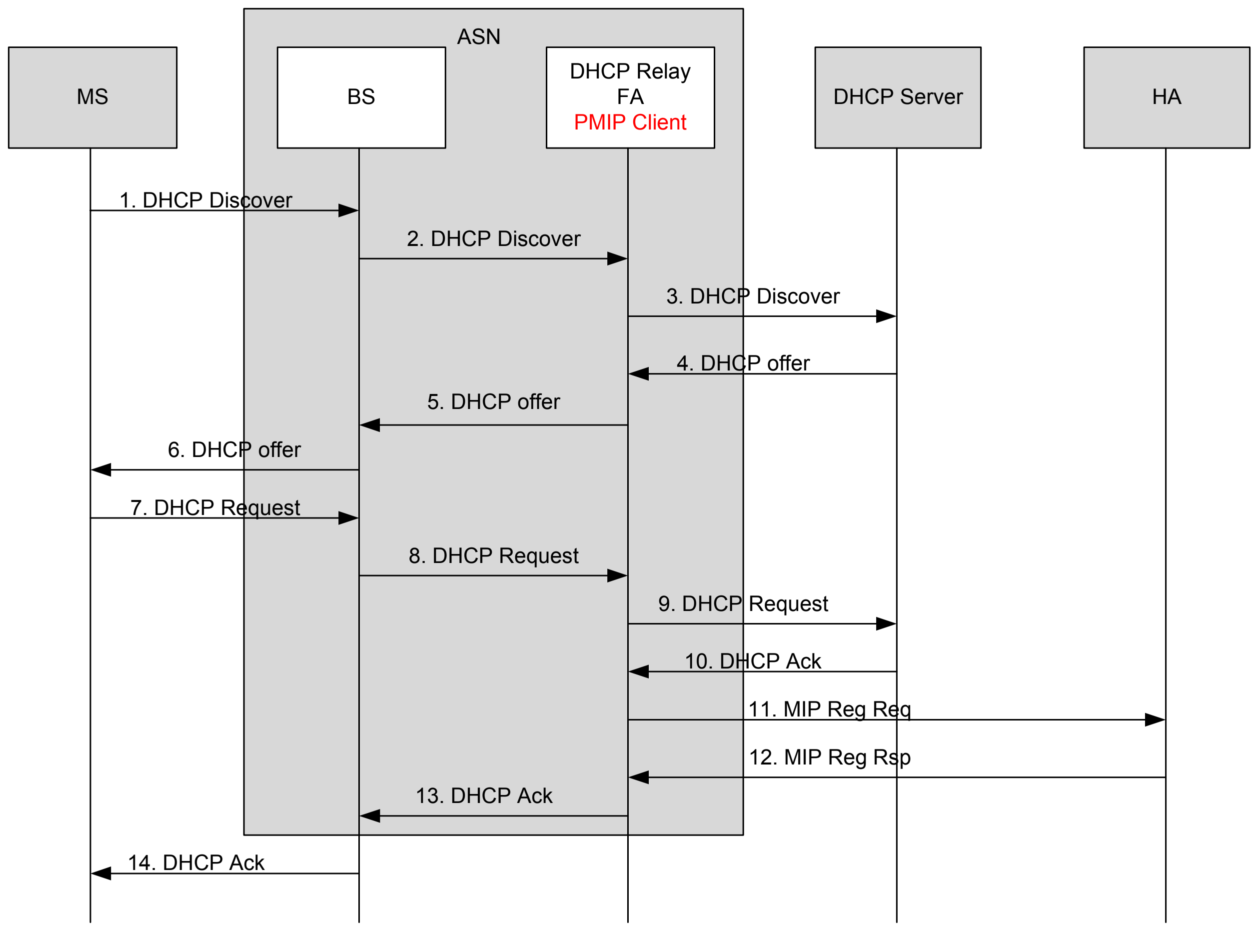


Figure 7-63 - Connection Setup in the Proxy MIP Solution (HA in H-NSP)

The following steps are written based on R3 is already secured, if R3 is not secured the DHCP Relay shall add the authentication sub-option as explained in RFC 4030 to have data integrity and replay protection for relayed DHCP messages.

STEP 1:

The MS sends a **DHCP Discover** as a broadcast message. The DHCP message is sent on the MS's Initial service flow setup over R1 interface to the BS.

STEP 2:

The **DHCP Discover** message is forwarded from BS to DHCP Relay present in ASN through the data path established for the ISF (Initial Service Flow) traffic.

STEP 3:

The DHCP Relay in ASN will intercept and change the destination IP address from broadcast to unicast and configure the giaddr field in the DHCP payload and sends the **DHCP Discover** message to the DHCP server of the MS based on configuration information. The configuration information in the most generic case will be downloaded via AAA but it may also be statically provisioned

If the Datapath is per MS or per SF, the MS context can be found based on the Datapath and not on the MAC address. If the Datapath is per BS the MS context can be found based on the MAC address or MS NAI

STEP 4:

DHCP servers receiving the **DHCP Discover** request reply by sending a **DHCP Offer** message including an offered IP address.

STEP 5:

The DHCP Relay in ASN forwards the DHCP replies to the MS. The **DHCP Offer** message is sent from ASN GW to BS through the Data Path.

The destination IP address of the **DHCP Offer** message sent to MS is a unicast one. Normally DHCP servers or relay agents attempt to deliver the **DHCP Offer** to a MS directly using unicast delivery. Unfortunately some MS's implementations are unable to receive such unicast IP datagram until they know their own IP addresses. To work around with this kind of MS's broadcast address MAY be used in **DHCP Offer** message. ASN need to check the BROADCAST (B) flag in the **DHCP Offer** message. If this flag is set, ASN need to use broadcast address to send **DHCP Offer** message, otherwise unicast address, but the delivery will be over a unicast CID.

STEP 6:

BS sends **DHCP Offer** message to the MS on the MS's Initial Service Flow.

STEP 7:

MS receives **DHCP Offer** message, and sends a **DHCP Request** to the selected DHCP server as a broadcast message confirming its choice of the DHCP Server.

STEP 8:

DHCP Request message is sent from BS to DHCP relay in ASN through the Data Path established.

STEP 9:

The DHCP Relay in ASN will relay the **DHCP Request** to the DHCP server.

STEP 10:

The selected DHCP server receives the **DHCP Request** and replies with a **DHCP Ack** containing the configuration information requested by the MS.

STEP 11:

The DHCP Relay in the ASN triggers a newly instantiated PMIP client to initiate the Mobile IP Registration procedure (not shown in Figure 7-63). The PMIP client uses the HoA information and constructs a Mobile IP Registration Request message. This message contains HoA and CoA for this MS. The source address for this R3 message is CoA, and the destination address is HA address.

STEP 12:

The HA responds with the Mobile IP Registration Response message. The source address for this R3 message is HA, and the destination address is CoA.

STEP 13:

After the establishment of MIP tunnel the PMIP client triggers DHCP Relay to send the **DHCP Ack** to the BS.

STEP 14:

BS sends **DHCP Ack** message to the MS on the MS's provisioned Initial Service Flow.

If MS doesn't receive a **DHCP Ack**, or **DHCP Nak** message when timeout, it will retransmit **DHCP Request**. If neither **DHCP Ack** nor **DHCP Nak** received when the maximum retransmission reached, MS shall restart the IP initialization process.

7.8.1.8.3.1 Backend IP Address Assignment Options

In the proxy-MIP solution a DHCP request is sent to the ASN network to retrieve the HoA address and IP host configuration parameters.

Between the ASN and CSN network following options are available:

- *DHCP relay*: The DHCP relay in the ASN manages the DHCP exchange with the DHCP server in the CSN. The DHCP server address is retrieved during access authentication.
- *AAA based HoA assignment*: IP host information and HoA address can be retrieved from the CSN as part of the access authentication AAA exchange. In this case the ASN will host a DHCP proxy and return the complete IP configuration to the MS.
- *MIP*: MIP exchange can be used by the PMIP client to retrieve the MS HoA address. For the MS host configuration the PMIP client SHALL use normal Vendor/Organization Specific extensions [33] in the MIP registration request. In that case, Mobile IP registration exchanges are triggered by DHCP proxy after DHCP discovery is received, DHCP proxy will not send DHCP offer until MIP registration is complete. After getting HoA from HA through the MIP registration progress, the PMIP client sends the HoA to the DHCP proxy which will act as a server in the forthcoming DHCP exchanges.

In the AAA scheme the IP address of the MS is available in the ASN network prior to the IP connection or radio connection establishment. In case of network-initiated connections, this information can be used to configure the SF classifiers directly with the correct IP address information, avoiding address spoofing or bootstrapping procedures.

7.8.1.8.4 Proxy-MIP Session Renewal

To update session state in the network and allow context release in case of SS/MS or network failure both the MIP context and the DHCP session state have to be renewed.

In a proxy MIP approach the MIP context renewal is handled completely by the network. As MIP re-registrations do not generate overhead over the air interface or interfere with SS/MSs going into sleep mode small refresh timer values can be chosen.

DHCP renewals are initiated by the MS.

7.8.1.8.4.1 DHCP Relay

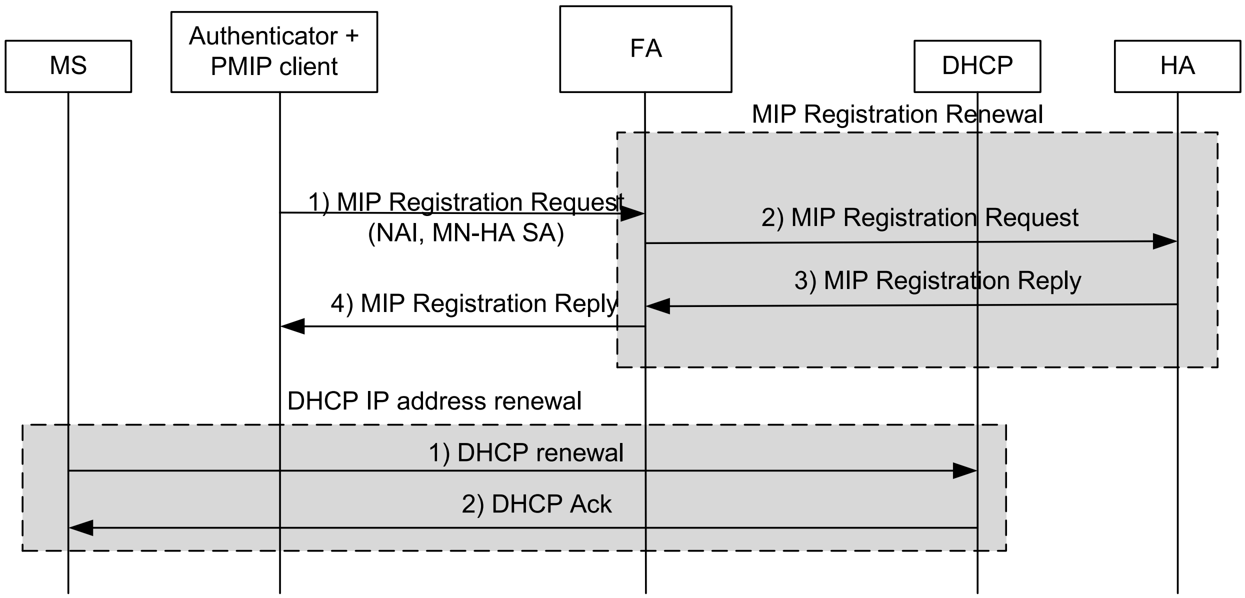


Figure 7-64 - Proxy-MIP, MIP Re-registration + IP Address Renewal

MIP session renewal:

In conformance with the [43] regular MIP registration messages are sent by the PMIP-client to FA to be forwarded to the Home-Agent.

Upon receiving the MIP registration message the Home-Agent will reset the MIP session timer.

Authentication of the source of the MIP registration messages is based on the keys exchanged during access authentication and do not require re-synchronization with the user's authentication server.

DHCP session renewal:

Through DHCP renewal the MS is able to maintain its HoA address.

DHCP renewal messages are initiated by the mobile, using the siaddr field from the initial DHCP ack message during the initial address allocation as the IP address of the DHCP server. The ASN can either act as DHCP relay or DHCP proxy as described in section 7.8.1.8.3.1.

In scenarios where AAA or MIP is used on R3/R5 to assign the HoA address the ASN will host the DHCP server.

7.8.1.8.5 Proxy-MIP CSN Anchored Mobility Management Handovers

The following signaling flow describes the CSN Anchored Mobility Management based on MS mobility event. In the Proxy MIP approach handovers are initiated by the Proxy-MIP client.

7.8.1.8.5.1 CSN Anchored Mobility Management Triggered by MS Mobility

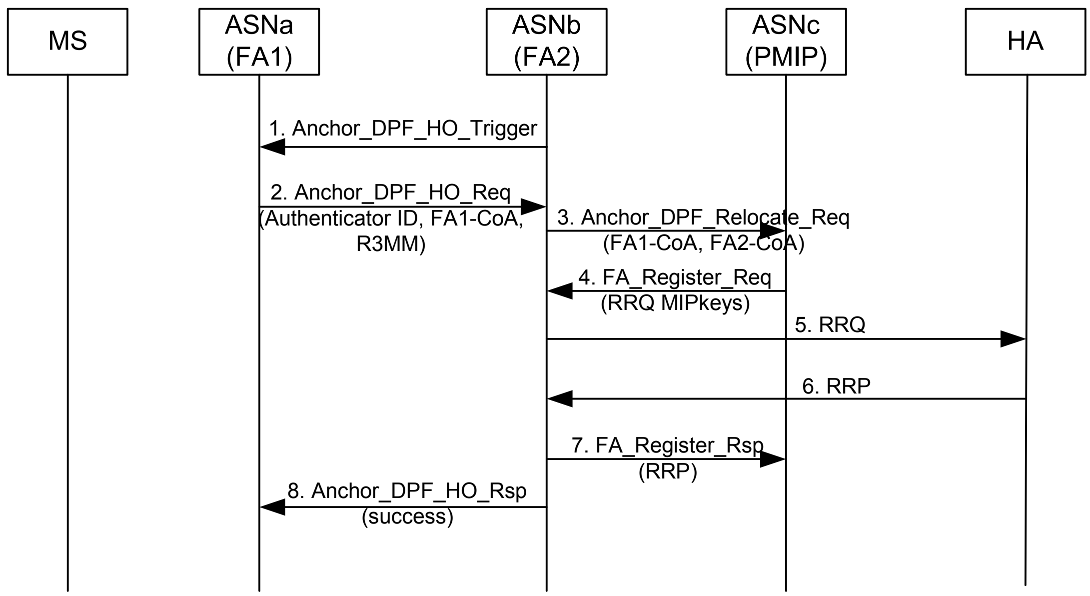


Figure 7-65 - MS Mobility Event Triggering a Network Initiated R3 Re-anchoring (PMIP)

STEP 1

If the target ASNb initiates the FA relocation negotiation, it sends a *Anchor_DPF_HO_Trigger* message to the anchor DPF in ASNa. If ASNa agrees with the FA relocation, it proceeds to Step2.

If the source ASNa initiates the FA relocation procedure, the call flow starts from Step2.

STEP 2

ASNa sends a AnchorDPF*_HO_Req* message to the DPF in ASNb. The message contains Authenticator ID, the current FA-CoA address and the DHCP context information for the MS.

STEP 3

Target ASN for FA relocation sends an *Anchor_DPF_Relocate_Req* message to the PMIP Client. This message relays some information about target ASN that is necessary in order to construct and send the MIP RRQ message in step4. The message contains CoA for the target FA, and target FA address if it is different than the CoA. In addition to target FA-CoA, current FA-CoA is included in the message.

STEP 4

The PMIP Client verifies that the current FA-CoA indeed matches the FA on its record, and starts the MIP registration with the target FA by sending *FA_Register_Req* message. This message contains a fully formed RRQ according to RFC3344, with CoA field in the RRQ set to the CoA of the Target FA which is received in *Anchor_DPF_Relocate_Req* message in step3. The source address of the RRQ is that of the MS and the destination address the CoA or the FA if FA address is different from CoA. In addition, *FA_Register_Req* message contains the FA-HA MIP key if this key is used. This message is sent to the Target ASN, whose address was identified as the source address of the *Anchor_DPF_Relocate_Req* message in step3.

STEP 5

The target FA relays the RRQ to the HA.

STEP 6

The HA responds with the RRP.

STEP 7

The target ASN relays the MIP RRP encapsulated in an *FA_Register_Rsp* message to the PMIP Client. The PMIP Client updates the FA in its record.

STEP 8

The target ASN also replies to the source ASNa with a Anchor_DPF_*HO_Rsp* message indicating a successful FA relocation. The source ASNa can then remove the mobility binding, DHCP context information and the R4 data path towards the ASNb.

7.8.1.8.6 Proxy-MIP Session Termination

In case of MS session termination the corresponding R3 mobility session has to be released.

An MS can either gracefully terminate its ongoing IP connection (e.g. by sending a DHCP release) or a session termination can be caused by an error condition.

Typical error conditions could be, MS out of coverage, low battery, system error, etc.

Criteria for initiating a R3 session release are not covered in this section.

The proxy MIP client will receive a session release trigger from an ASN functional entity, or the MIP Revocation from HA.

The R3 Mobility session is released by sending a MIP registration with a lifetime of zero.

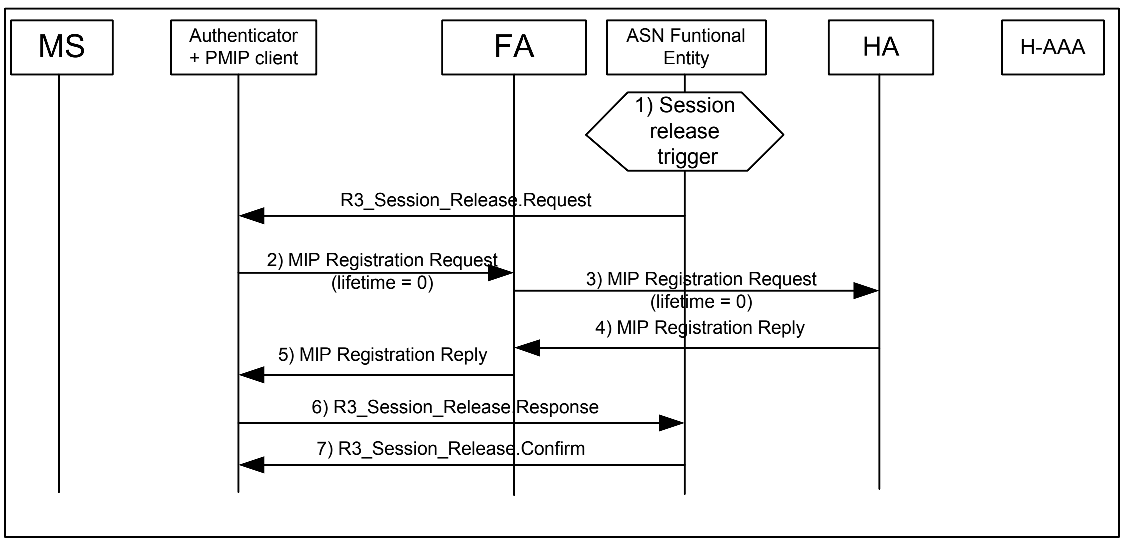


Figure 7-66 - R3 Session Release

For charging and accounting purposes the HA MAY optionally send an AAA Accounting message to the MS's H-AAA server.

Note that R6 or R4 session termination is not covered by the signaling flow illustrated in Figure 7-66.

After receiving the R3_Session_Release.Request message from the ASN Functional Entity, the PMIP client SHALL release the tunnel associated with the MS. In addition, the PMIP client SHALL notify the ASN functional entity to update the MS session context.

If there are more than one session identifiers contained in the R3_Session_Release.Request message, the PMIP client SHALL repeat the same steps for each session contained in the R3_Session_Release.Request.

7.8.1.9 Client MIP R3 Mobility Management

This section describes requirements and procedures for the CMIP R3 mobility management.

Figure 7-67 provides an example of an MS with multiple wireless and wired access options. The depicted stack can support handoff across different access technologies. In the following discussion we only address R3 mobility for IEEE 802.16 access links. For release one, Inter-technology handovers are outside the scope of R3 mobility.

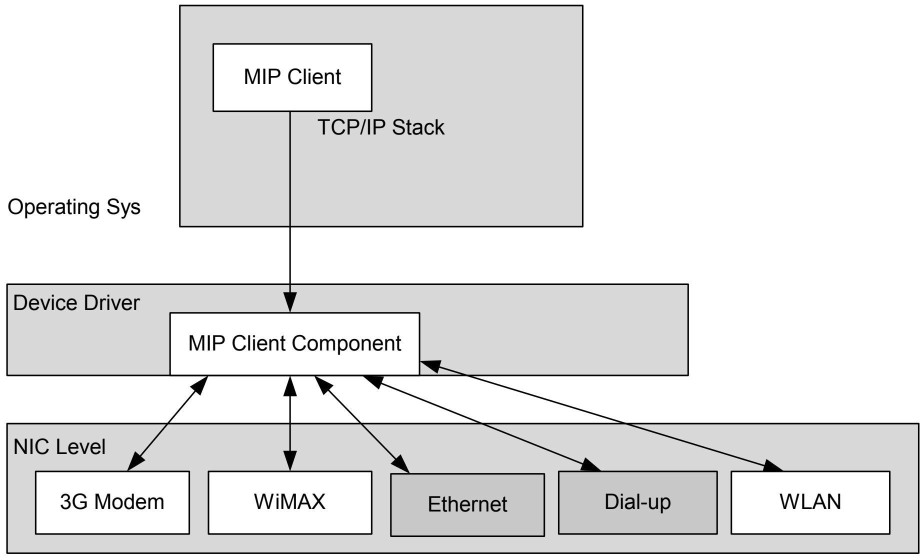


Figure 7-67 - MS with Mobile IP Stack and Multiple Access Options

At the time of the initial MIP session establishment, when new R6 tunnel is established between the Data Path Function at the ASN-GW and the Data Path Function in the new target BS, the MIP client receives a mobility trigger in the form of new MIP advertisement from the FA.

The FA is located at the boundary of the ASN and the CSN and terminates the R3 Reference Point within the ASN. The MIP client is a single entity that supports R3 mobility for a single user and is located above the 802.16 drivers and can be an integral part of the OS stack. Such client typically includes multiple components (modules) that MAY span various stack elements as shown above.

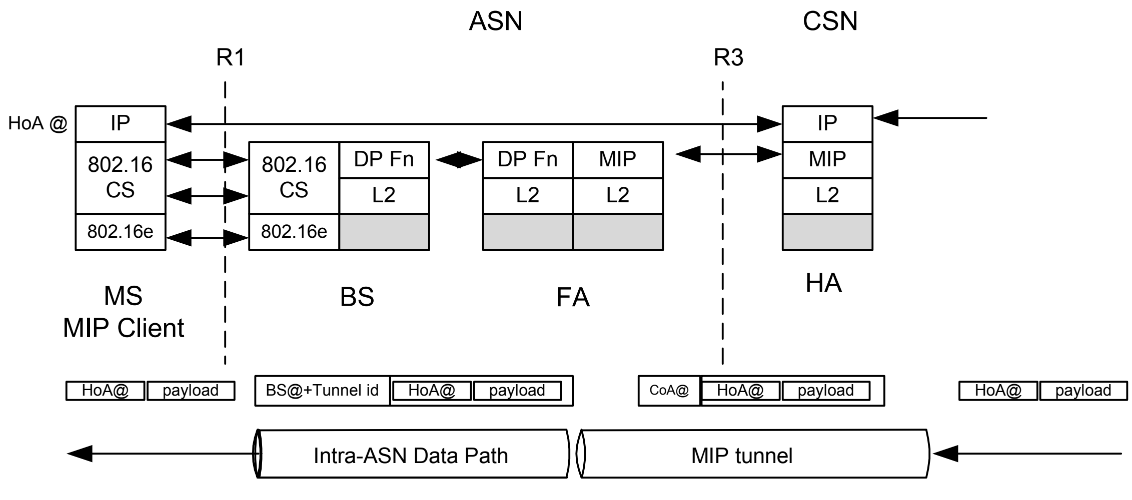


Figure 7-68 - Mobile IP Data Plane (Example)

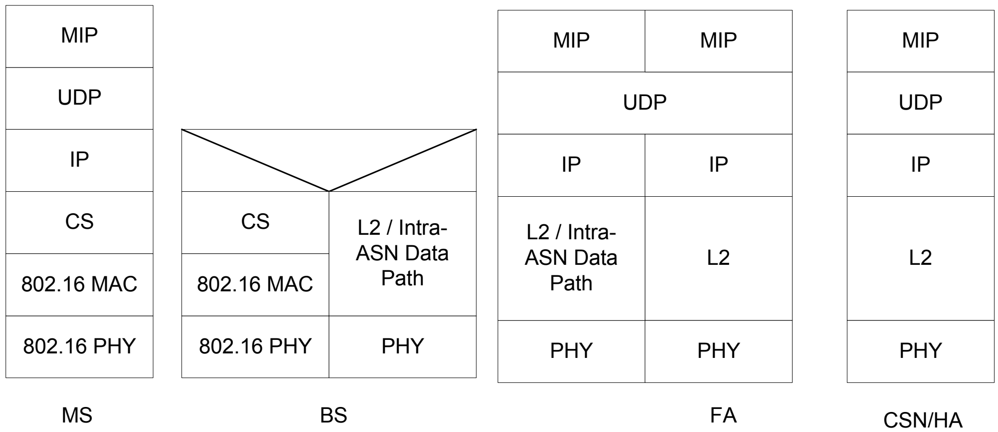


Figure 7-69 - Mobile IP Control Plane

The MIP client in the MS participates in the message exchanges required to perform inter-ASN and inter-NAP mobility. The MIP client supports dynamic address assignment and dynamic HA allocation. To support unambiguous detection of the MS' capabilities and determination of use of CMIP versus PMIP for Ipv4, the use of co-located CoA mode with CMIPv4 (when used only with the WiMAX interface), SHALL NOT be supported in this specification. When the MIP client is involved in inter-technology handoffs, the use of Collocated CoAs (CCoA) is allowed in association with access interfaces different than IEEE 802.16.

7.8.1.9.1 Client-MIP Connection Setup Phase

Upon successful access level authentication, the MS obtains the AAA-Key/MSK and EMSK. When HA address is not assigned, the MS can obtain the HA address as part of the Mobile IP registration messages exchange.

The following signaling flow describes the connection setup phase:

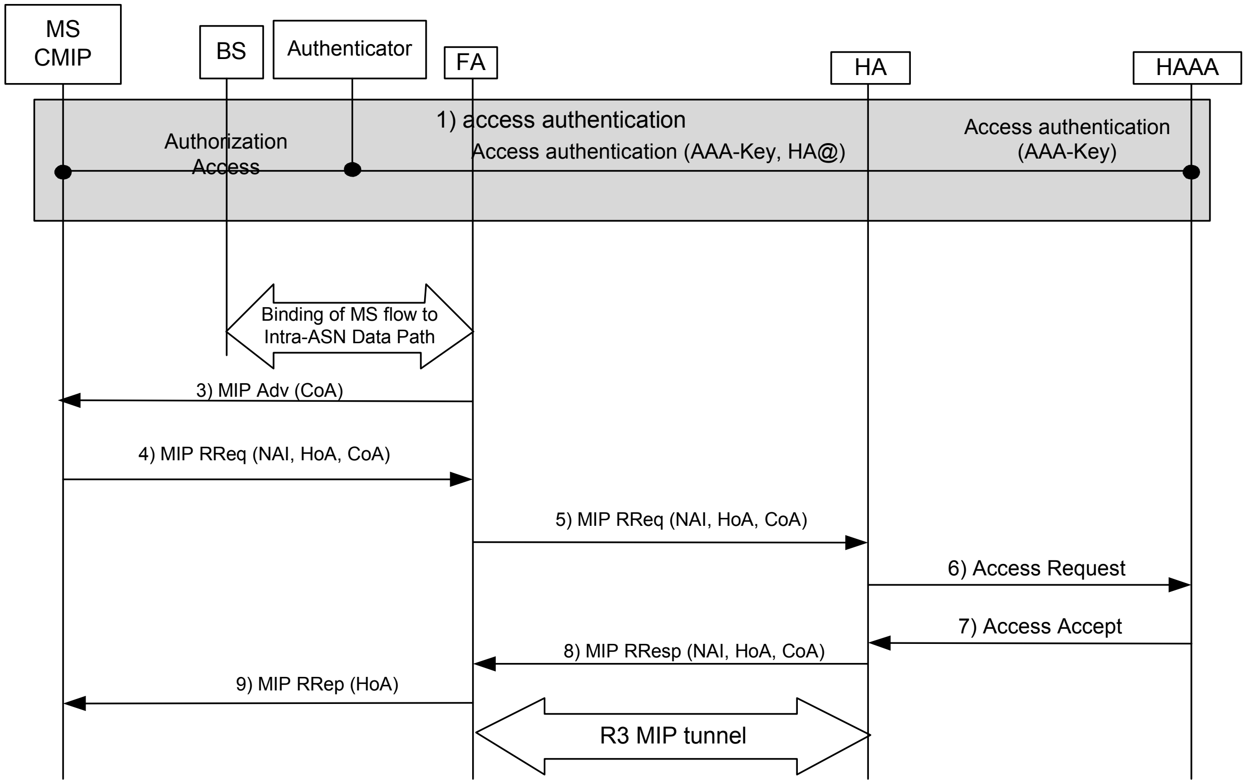


Figure 7-70 - Connection Setup

Step 1) Access Authentication: During access level authentication the AAA authentication key is retrieved from the AAA access authentication message exchanged with the MS home AAA server.

Step 2) A trigger is generated when binding of MS or MS flow with intra-ASN Data Path is established.

Step 3) When new intra-ASN Data Path is established configurable number of advertisements is sent to the MS.

Step 4-5) The MIP registration is performed by the client and forward to the HA. MS using Mobile IP connectivity will not issue DHCP requests and will only use MIP signaling to obtain its home address.

Step 6) HA sends RADIUS Access-Request message to Home AAA.

Step 7) Upon receipt of a RADIUS Access-Request message from a HA containing the MN-HA attribute, the RADIUS server SHALL send a RADIUS Access-Accept message containing the MN-HA shared key encrypted. If registration request included dynamic HA assignment and IP host configuration the HA address and the IP configuration will be respectively returned by the AAA as well.

Step 8) The HA forwards the Registration Reply to the FA.

Step 9) MIP Registration Reply is forwarded to the MS containing the MS home address.

IP Host configuration: The MS MAY use extensions defined in draft-bharatia-mip4-gen-ext-01.txt in the MIP Registration Reply to obtain its IP host configuration.

7.8.1.9.2 Client MIP Session Renewal

To update session state in the network and allow a context release in case of SS/MS or network failure the MIP context SHALL be renewed. The client sends Mobile IP re-registration messages to the FA according to [43]. Upon receiving the re-registration request the HA will reset the MIP session timer. Authentication is based on the prior keys obtained during initial authentication and as such do not require a synchronization with the user authentication server. The following depicts the message flow. If MN-FA is used, the challenge used by the MS for re-registration SHOULD be the one last sent by the prior MIP registration/re-registration response. On re-registration, the FA

MAY communicate user FAC authentication information to the Home AAA Server. The frequency of this re-authentication and re-authorization is configurable.

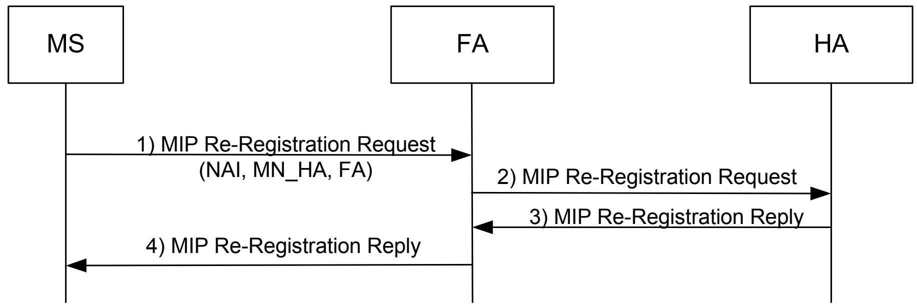


Figure 7-71 - Session Renewal, MIP Re-Registration

7.8.1.9.3 Client MIP CSN Anchored Mobility Management

As previously mentioned, MIP R3 mobility handovers are always network initiated. Even when the mobile initiates the handover to a new BS and FA, the R3 mobility is a result of a network event that strives to minimize impact on real time traffic when migration R3 from anchored to target FA. The R3 mobility trigger is typically a delayed event to the FA re-anchoring procedure described in 7.8.1.10.

7.8.1.9.4 Foreign Agent Advertisement

When a new MS or a service flow within MS is initially bound to an intra-ASN Data Path, the FA begins the transmission of configurable number of Agent Advertisements to the MS. Once the configurable number of Agent Advertisement is sent, the FA will not send more Advertisement. Only when the MS sends Agent Solicitation message the FA will respond with an Agent Advertisement. When the first MIP Registration Request is received by the FA, it SHALL cease sending Agent Advertisements even if the number sent is less than the configurable number of Agent Advertisements.

In order to minimize Agent Advertisement sent over the air, the FA SHOULD not send unsolicited Agent Advertisements to the MS to refresh the advertisement lifetime. The MS MAY send Agent Solicitation when the FA advertisement lifetime expires or about to expire. The advertisement lifetime is a configurable value and can be set to the maximum value of 9000 seconds (the maximum ICMP advertisement lifetime).

7.8.1.9.5 Client-MIP Session Termination

In case an MS active IP session has to be terminated, both the MAC state as well as intra-ASN Data Paths between the FA and the HA has to be gracefully removed.

The four termination scenarios are as follows:

(1) An MS initiated graceful termination: a session is gracefully terminated by sending a MIP Registration Request message with lifetime = 0. This termination is triggered either by the user or MS being in an error conditions such as low battery power, etc.

(2) ASN initiated graceful termination: The conditions for ASN initiated termination MAY be some error conditions with respect to the MS such as the MS being identified as a rogue MS with security violations, planned maintenance, etc. This scenario is depicted in Figure 7-73. A session is gracefully terminated by sending an R3_Session_Release.Request message from an ASN Functional entity like the intra-ASN Handover function. After receiving the R3_Session_Release.Request message from an ASN Functional entity, the FA SHALL trigger registration revocation procedure with HA to terminate binding as per RFC 3543.

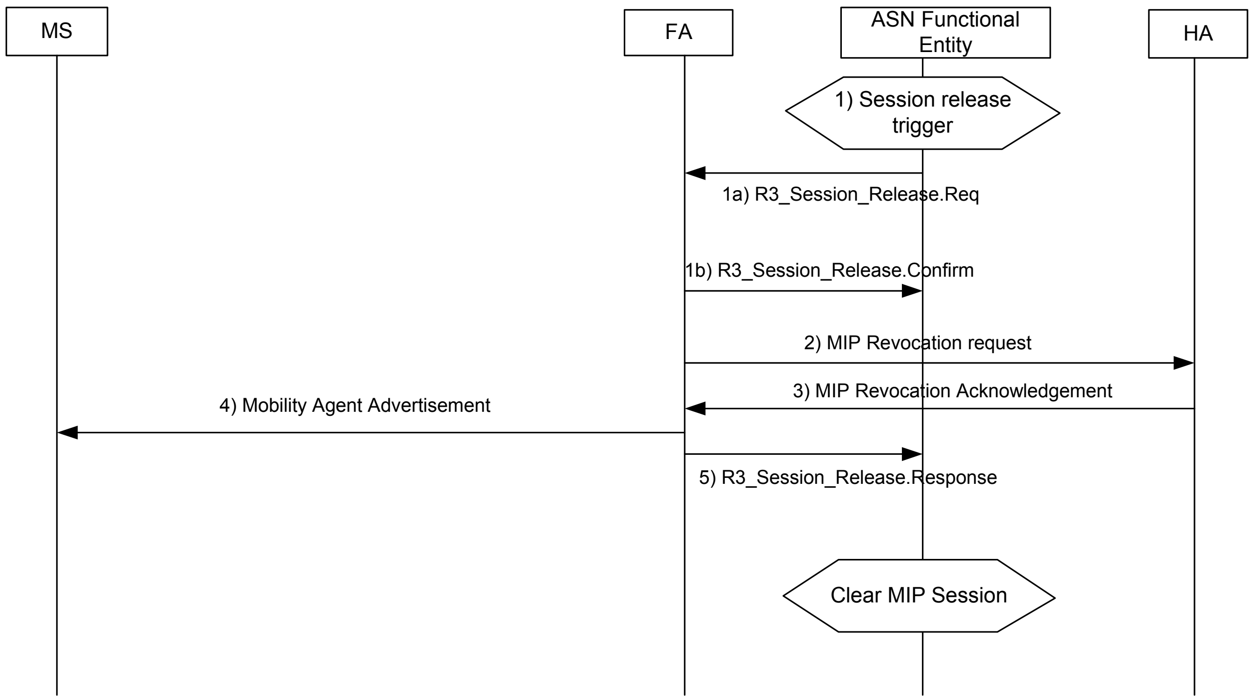


Figure 7-72 - ASN Initiated Graceful Termination

4) HA initiated graceful termination: This scenario is depicted in Figure 7-74. A session is gracefully terminated when HA triggers registration revocation with FA as per RFC 3543. FA sends the R3_Session_Release.Request to ASN Functional to notify termination of mobility binding. MS may be informed depending on if the I bit is set in Revocation message.

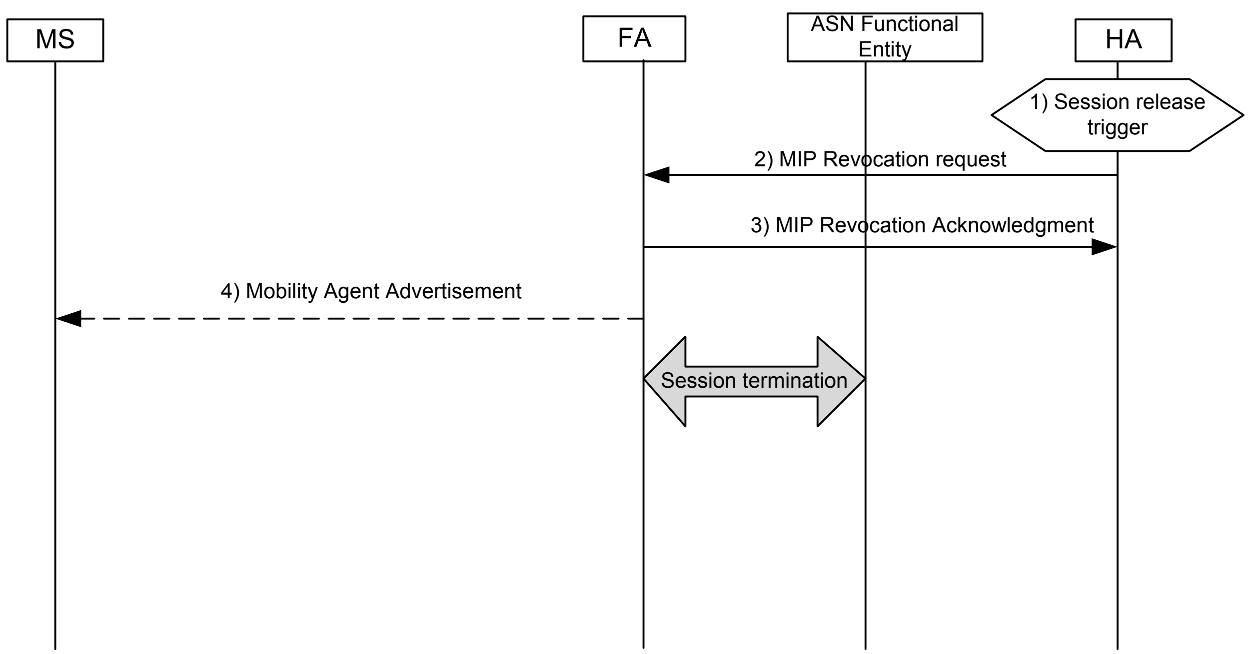


Figure 7-73 - HA Initiated Graceful Termination

5) MS loss of carrier unconventionally termination: the scenario when the BS detects the MS is loss of carrier unconventionally, the BS SHALL inform ASN Function Entity by sending an *Path_Dereg_Req* with operation reason as "MS loss of carrier". Then, if the SFA and Data Path Function of ASN Function Entity make a decision to release R3 and the related R6 or R4 resource, it SHALL inform the FA to release the HA to unbind the PoA address of the MS by sending Path_Dereg_Req, thus the session is terminated. This scenario is depicted in Figure 7-75. At the same time, in this scenario, ASN Function entity can release ASN resource for the MS, such as intra-ASN data path etc.

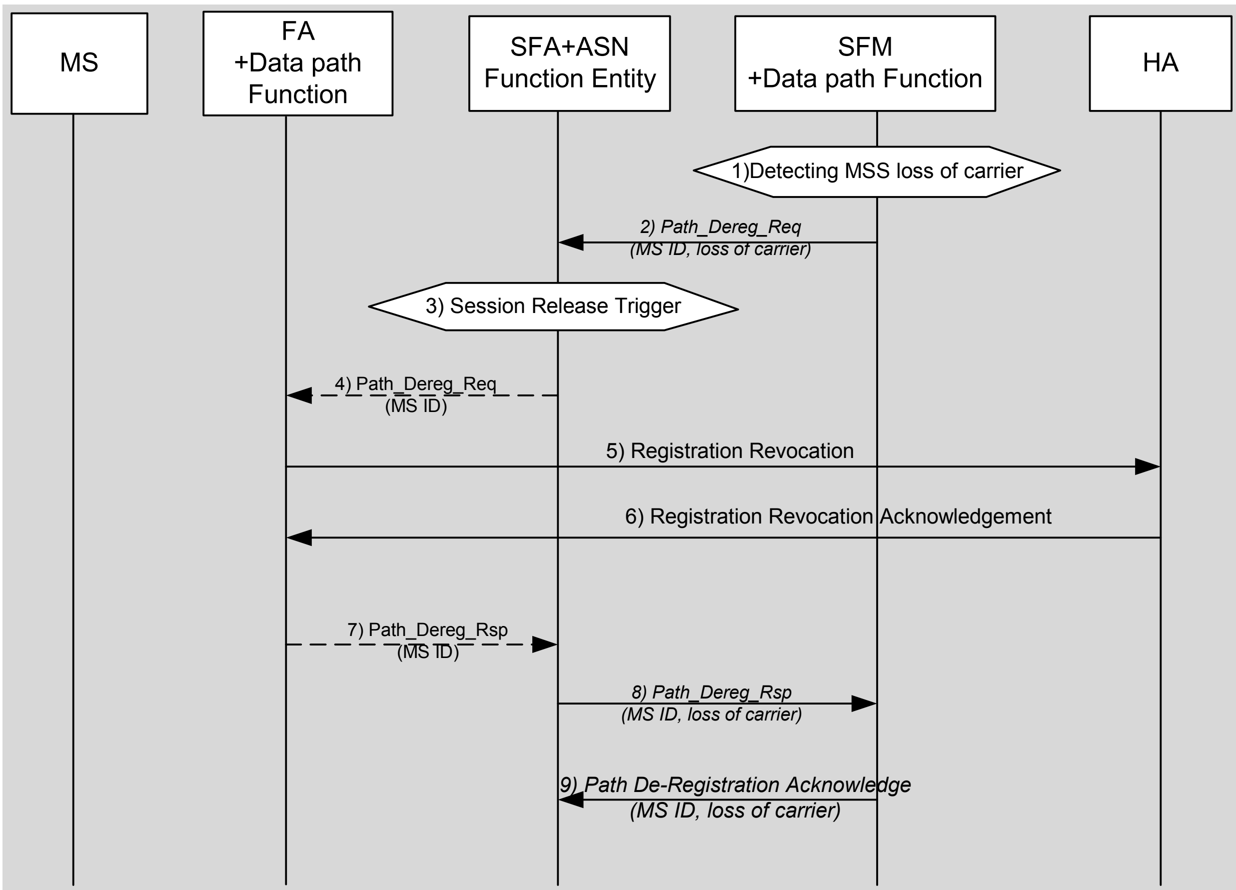


Figure 7-74 - MS Loss of Carrier Unconventionally Termination

7.8.1.10 CSN Anchored Mobility Management to ASN-Anchored Mobility Management Relationship

This section describes a possible link between ASN-anchored mobility and CSN Anchored Mobility Management and is meant as informational. Actual implementations can differ from the option described below.

Figure 7-75 illustrates the two major handover types described above from both an architecture and functional perspective. The top of the Figure shows ASN1 anchoring R3 and forwarding bearer traffic to ASN2 over R4 (labeled before) followed by an R3 relocation message that relocates R3 bearer traffic from ASN1 to ASN2 (labeled after). The bottom part shows a combined CSN -anchored mobility handover events where R3 is relocated from ASN1 to ASN2 without a prior ASN anchoring. Combined CSN/ASN-anchored mobility handovers is normally triggered by an MS mobility event like running into coverage of a new Base Station, although these handover can also be a result of a resource optimization decision. The dotted line represent the initial state before a handover, the solid line depicts the data path after a combined R3/R6 handover.

The top part of Figure 7-75 illustrates a typical RRM based handover that results in both an ASN Anchored Mobility where traffic is forward from ASN1 to ASN2 followed by a CSN-anchored mobility handover where R3 is relocated from ASN1 to ASN2.

In case of an RRM based handovers the R3 handover request is never sent directly from the RRM controller to the mobility manager but will be passed through the ASN Handover Function. This approach facilitates synchronization between the different ASN functional elements. Additionally it makes the R3 mobility transparent to the RRM management.

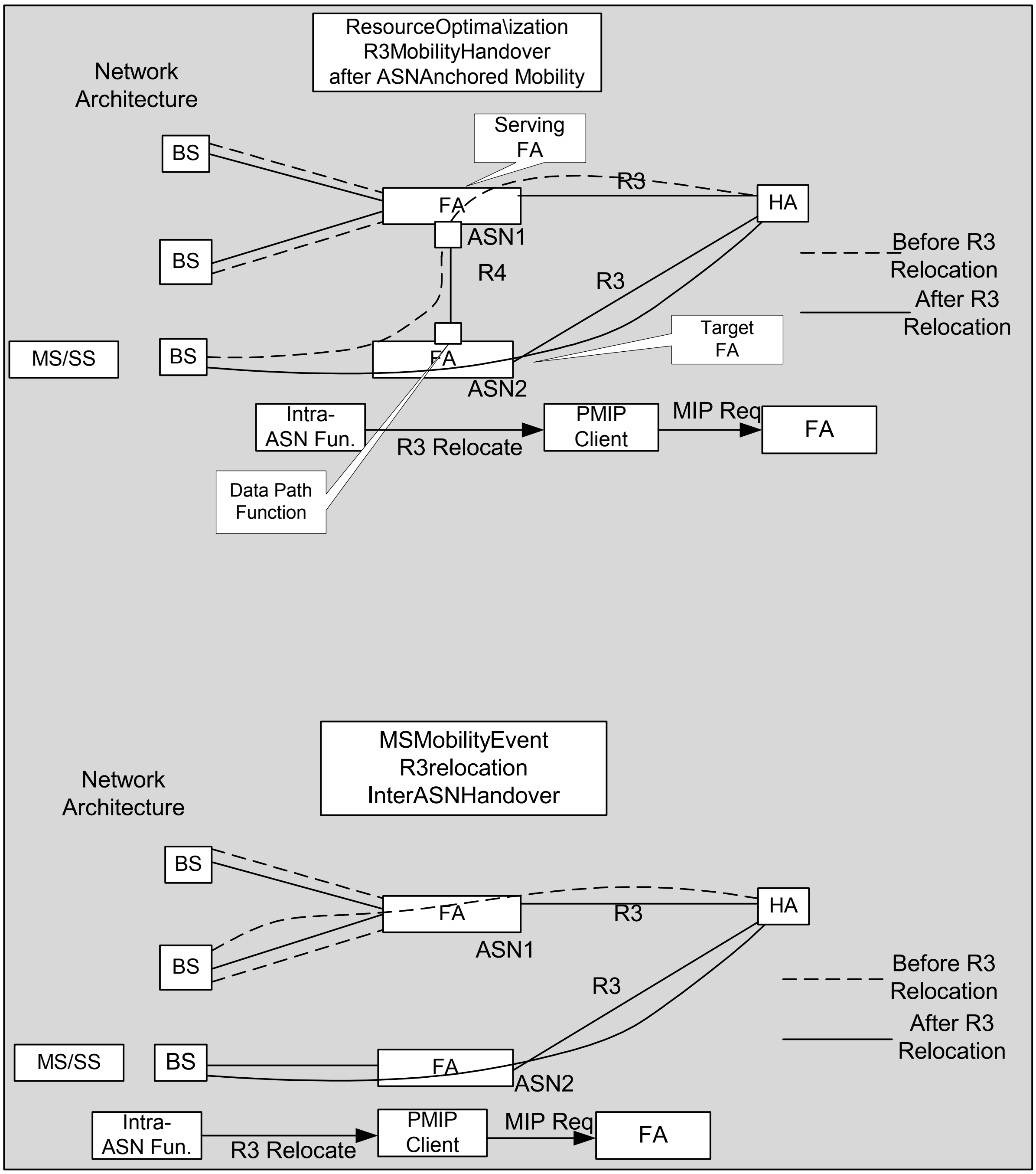


Figure 7-75 - R3MM to Intra-ASN Mobility Relationship

From ASN-anchored mobility management perspective, there are two scenarios exist where an R3 handover can be initiated. The first scenario is during an ASN-anchored mobility handover event, e.g. upon receiving an HO-indication message at the ASN Functional entity. The second scenario (which is preferred) is to initiate an R3 handover after the ASN-anchored mobility handover has been successfully executed, e.g. when the ASN Functional Entity receives a '*Anchor_DPF_Relocate_Req*'. Triggering an R3 handover after the ASN-anchored mobility handover has been fully processed avoids scenarios where an R3 handover needs to be cancelled and the old connection is reestablished due to unsuccessful ASN-anchored mobility.

Applying ASN data forwarding prior and during the time it takes to complete an R3 handover minimizes packet loss and handover interruption time. After the new R3 path has been established the PMIP mobility manager will notify the ASN Functional Entity by sending an '*Anchor_DPF_Relocate_Rsp*' message.

The *Anchor_DPF_Relocate_Rsp* message can be used by the ASN Functional Entity to terminate inter-ASN data forwarding between the old and new ASN.

7.8.1.11 CSN Anchored Mobility Management Trigger Primitives

Table 7-2 lists the messages involved in R3 mobility. Note that these messages MAY be exchanged between functional entities within a single ASN, or between functional entities in different ASNs.

Table 7-2 - R3MM Mobility Management Primitives "for information only, the binding facts are defined in the Stage3 Spec"

Primitives	From => To	Message Content	Applicability CMIP/PMIP
HoA_Address	DHCP Proxy => PMIP Client	MSID, HoA @, Transaction ID	PMIP
HoA.Address.Ack	PMIP Client => DHCP Proxy	MSID, Status, [error code], Transaction ID, Status	PMIP
DHCP_Gating.Release	PMIP Client => DHCP Proxy	MSID, Transaction ID	PMIP
R3_Session_Release.Request	ASN-Fn => PMIP Client ASN-Fn => FA	MSID, list of (status (Successful, Failed), [Error Code]) attributes, Transaction ID	PMIP CMIP
R3_Session_Release.Response	PMIP Client => ASN-Fn FA => ASN-Fn	MSID, list of (MIP session ID, status (Successful, Failed), [Error Code]) attributes, Transaction ID	PMIP CMIP
R3_Mobility_Context	DHCP Proxy => ASN-Fn FA => ASN-Fn	MSID, R3 Mobility Mode, Transaction ID	PMIP CMIP
R3_Mobility_Context.Ack	ASN-Fn => DHCP Proxy ASN-Fn => FA	MSID, Transaction ID, Status (Successful, Failed), [Error Code]	PMIP CMIP
Anchor_DPF_Relocate_Req	ASN-Fn => PMIP Client ASN-Fn => Target FA	MSID, Target FA, Transaction ID	PMIP CMIP
R3_Relocate. Confirm	PMIP Client => ASN-Fn FA => ASN-Fn	MSID, Transaction ID	PMIP CMIP
Anchor_DPF_Relocate_Rsp	PMIP Client => ASN-Fn	MSID, Transaction ID	PMIP

Primitives	From => To	Message Content	Applicability CMIP/PMIP
	Target FA => ASN-Fn		CMIP

7.8.1.11.1 HoA_Address

The HoA_Address message provides the HoA address retrieved from the CSN to the PMIP client.

As described in the session setup paragraph the HoA address can be provided during the access authentication as part of the AAA exchange or can be retrieved for a DHCP server in the CSN network.

- **MSID**: identifies the MS for which an R3 handover is requested.
- **HoA Address**: Home address of the MS.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MS uniquely identifies a request

7.8.1.11.2 HoA_Address.Ack

A HoA_Address.Ack is send by the PMIP Client upon successfully receiving the HoA_Address message.

- **MS ID:** identifies the MS for which an R3 handover is requested.
- **Transaction ID:** Correlates the replies with the correct request. To match Replies with Requests the Transaction ID in the reply SHALL match the Transaction ID in the Request
- **Status:** Indicates whether or not the HoA_Address message was successful received.
    - In case of failure an additional error code identifying the reason of failure can be added (e.g., unknown MS ID).

7.8.1.11.3 R3_Session_Release.Request

An R3_Session_Release.Request will terminate the R3 MIP session for a specific MS.

- **MS ID**: identifies the MS for which an R3 handover is requested.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MS uniquely identifies a request.

7.8.1.11.4 R3_Session_Release.Response

The R3_Session_Release.Response message indicates either a successful or failed R3 handover event in response of an R3_Release.Request.

- **MS ID:** identifies the MS for which an R3 handover is requested.
- List of (Status (Successful, Failed), [Error Code]) attributes: Optionally list the MIP session to be released event result.
- **Status:** Indicates whether or not the R3 handover was successful.
    - In case of failure an additional error code identifying the reason of failure can be added.
- **Transaction ID**: Correlates the replies with the correct request. To match Replies with Requests the Transaction ID in the response SHALL match the Transaction ID in the Request

7.8.1.11.5 R3_Mobility_Context

The R3_Mobility_Context is used to inform the ASN Functional Entity whether the MS is in Proxy-MIP or CMIP mode. Additionally some R3 context information can be added. This information is used by the ASN Function Entities to determine the correct moment in time to trigger an R3 handover request plus the correct destination of the message (e.g. FA or PMIP mobility manager).

- **MSID**: identifies the MS for which an R3 handover is requested.
- **R3 Mobility Mode**: Indicates the R3 mobility the MS is using. The field can take two values, either CMIPv4, CMIPv6 or PMIPv4.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MSID uniquely identifies a request.

7.8.1.11.6 R3_Mobility_Context.Ack

An R3_Mobility_Context.Ack is send by the ASN Functional Entity upon successfully receiving the R3_Mobility_Context message.

- **MSID**: identifies the MS for which an R3 handover is requested.
- **Transaction ID**: Correlates the replies with the correct request. To match Replies with Requests the Transaction ID in the response SHALL match the Transaction ID in the Request
- **Status**: Indicates whether or not the R3_Mobility_Context message was successful received. In case of failure an additional error code identifying the reason of failure can be added (e.g. unknown MSID).

7.8.1.11.7 Anchor_DPF_Relocate_Req

R3 *Anchor_DPF_Relocate_Req*s are used to trigger an R3 handover. R3 *Anchor_DPF_Relocate_Req*s can be triggered by the resource management function or other network entities.—Upon receiving an R3 *Anchor_DPF_Relocate_Req*, the ASN Functional Entity will send a R3_Relocation.Request to the ASN Functional Entity and start R3 handover procedure.

- **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In PMIP the MS identifies a specific PMIP client in the PMIP client.
- **Target FA**: Identifies the new R3 anchor point for the MS. In MIP terminology the Target FA address corresponds to the FA's CoA address.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MSID uniquely identifies a request.

7.8.1.11.8 R3_Relocate.Confirm

R3_Relocate Confirm is used to acknowledge successful receipt of the R3 *Anchor_DPF_Relocate_Req* message. The confirmation does not give any feedback on the actual processing or state of the R3 relocation.

- **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In PMIP the MS identifies a specific PMIP client in the PMIP client.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MSID uniquely identifies a request.

7.8.1.11.9 Anchor_DPF_Relocate_Rsp

The R3 *Anchor_DPF_Relocate_Rsp* message indicates either a successful or failed R3 relocate event in response of an R3 *Anchor_DPF_Relocate_Req*.

- **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In PMIP the MS identifies a specific PMIP client in the PMIP mobility manager.
- **Target FA**: Identifies the new R3 anchor point for the MS. In MIP terminology the Target FA address corresponds to the FA's CoA address.
- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MSID uniquely identifies a request.

7.8.1.12 Proxy-MIP and Client MIP Coexistence

R3 mobility can be provided based on two mechanisms:

- Client MIP solution based on a MIP client in the MS.
- Proxy MIP solution based on MIP client in the network.

Both solutions are based on a different network and SS/MS behavior and therefore require special consideration to support both on the same network. Which R3 mobility scheme is used depends on a number of factors like SS/MS type, MIP client availability, inter-technology handovers support, type of operator, roaming considerations, etc.

In order to be able to accommodate for any type of SS/MS and inbound roamer a network SHOULD ideally be able to support both the CMIP and PMIP R3 mobility schemes.

With both PMIP and CMIP being mandatory from network point of view several scenarios can be identified, the table below gives a short overview of the different possibilities. Table 7-3 only covers R3 mobility, fallback options to nomadic access based on network capabilities or operator policies are not covered.

Table 7-3 - R3MM coexistence scenarios

MS support	Network Support	Decision
MIP	CMIP	CMIP
Simple-IP	PMIP	PMIP
MIP	CMIP + PMIP	CMIP
Simple IP	CMIP + PMIP	PMIP
MIP	PMIP	Not Applicable
Simple-IP	CMIP	Not Applicable

The Coexistence solution focuses on the following points:

- **MS capability discovery**. A MS can be categorized as either a simple IP SS/MS or a MIP enabled MS. A simple IP SS/MS can be any IP SS/MS using DHCP for IP address assignment.
- **Supported network mobility schemes discovery**. Based on some of the arguments listed above an operator might decide to only support PMIP or CMIP or both schemes.
- **R3 mobility scheme selection**. Once both the SS/MS and network capabilities are known the correct R3 mobility scheme needs to be activated.

7.8.1.13 Coexistence for Networks Supporting Both CMIP and PMIP

This specific coexistence scenario deals with networks that are able to support both simple IP SS/MSs as well as Mobile-IP enabled MSs.

Which scheme the network applies will depend on the SS/MS capabilities and can additionally be imposed by the Home-NSP based on the knowledge of both the SS/MS capabilities and NAP mobility support.

If the Home NSP is unable to determine the SS/MS capabilities or the network supported R3 mobility schemes the home AAA-server will provide both the necessary PMIP and CMIP information to the ASN during the Access Authentication phase.

Prior to an intra-ASN data path establishment the network is unaware of the MS capabilities, so immediately after the data path between ASN-located FA and MS is established, the FA entity will send an FA advertisement to the SS/MS over this newly established data path. If the SS/MS is MIP enabled it will perform a MIP registration using the CoA advertised in the FA advertisement.

The MIP registration originated from the MS will force the network into CMIP mode.

A MS without MIP functionality (simple IP SS/MS) will discard the FA advertisement and send a DHCP request to get an IP address. The DHCP request will trigger the PMIP Mobility Manager – HoA_Address message – to setup an R3 session on behalf of the MS.

So for networks supporting both CMIP and PMIP the selection is straightforward and driven by the SS/MS. Network capability discovery is based on MIP agent advertisement messages send just after connection setup. The mobility scheme selection is determined by the ASN, based on the type of message received from the SS/MS and can be either a DHCP request or a MIP registration request.

To avoid situations where due to loss of the FA advertisement message or unexpected delays a MIP client would go into collocated CoA mode the MIP client needs to be configured such that collocated CoA mode is prevented for the WiMAX interface. In collocated CoA mode, the MIP client will send a DHCP request to retrieve the co-located care of address, this message will be wrongly interpreted by the network as a request to establish a PMIP session.

After initial R3 session setup the ASN network stores the current R3 Mobility mode the SS/MS is in.

The R3 mobility mode needs to be stored at the ASN Functional Entity. Based on this information the ASN Functional entity can determine the right moment and destination to send an R3 *Relocation_Req* to. Knowledge of the R3 mobility mode will also prevent unnecessary air-overhead by suppressing FA advertisements after every handover in case of PMIP users.

For MIP enabled SS/MSs the R3 mobility trigger will be send directly to the FA, for PMIP user the R3 mobility trigger will be sent to the PMIP mobility manager.

7.8.1.14 R3 Mobility Session Authentication and Authorization

7.8.1.14.1 Proxy-MIP Security

The following section describes the elements of the PMIP security framework and their interaction to dynamically establish a PMIP key to enable a Proxy Mobile IP client and Home Agent (HA) exchange authenticated registration requests and response messages.

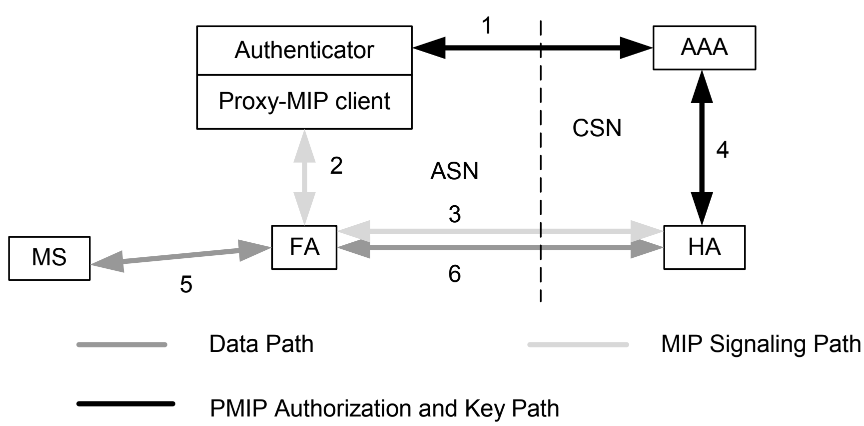


Figure 7-76 - PMIP Functional Elements

Figure 7-76 shows the function elements related to PMIP. During network entry the mobile node (MS) authenticates to the AAA via an authenticator, using an EAP authentication process. At the end of the exchange, if the authentication is successful, the AAA server sends an EAP success and a notification of authorization for PMIP process to the authenticator. At this point the Authenticator obtains the PMIP Key. The AAA server SHALL send the SPI, lifetime and any other PMIP related information (such as HoA, HA IP address, and so on, if desired) along with the authorization notification for PMIP. The lifetime of this key SHALL be the same as that of the MSK that is generated as a result of successful authenticator. The Authenticator SHALL share the PMIP key and related information with the Proxy-MIP client. The Proxy Mobile Node (PMN) MAY use this key for the lifetime of the key, i.e. additional registration requests MAY be generated using the same Proxy-MIP Client when the lifetime of the registration expires or when the MS moves to a new subnet requiring a new registration.

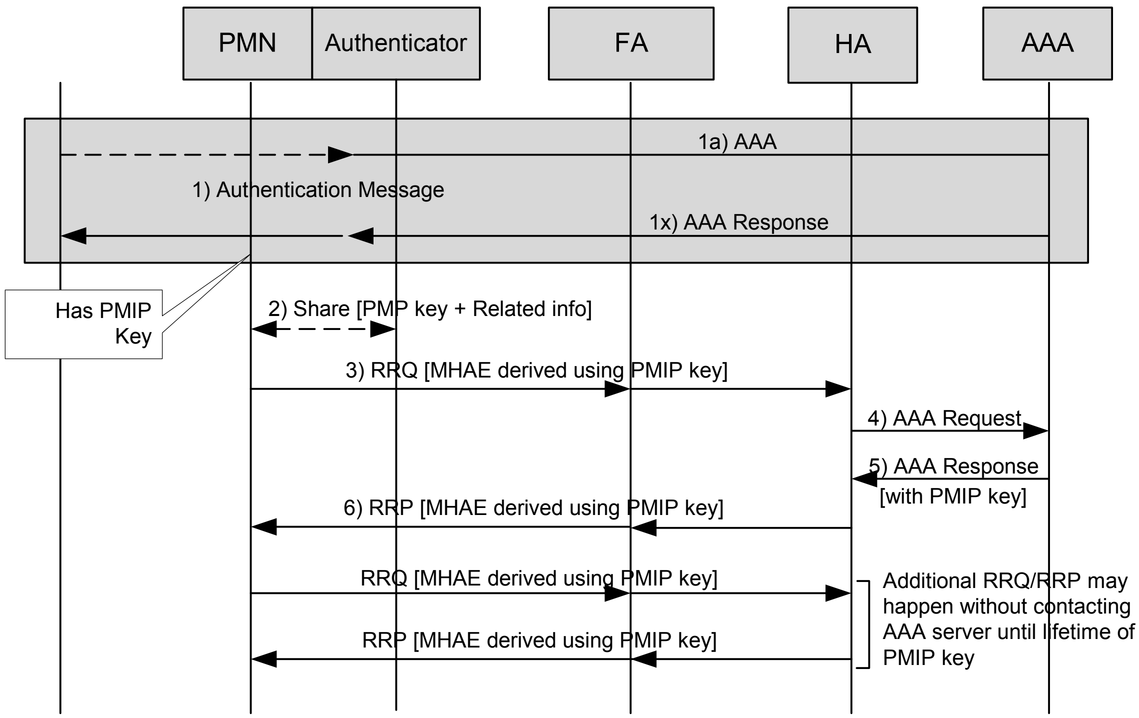


Figure 7-77 - PMIP Key Generation and Transfer – Message Sequence

a) During network entry the mobile node (MS) authenticates to the AAA via the authenticator, using an EAP authentication process. This MAY take multiple steps and at the end of successful authentication the authenticator obtains the PMIP Key. Note that the PMIP key that is obtained by the authenticator is in addition to the MSK that is provided by the AAA server as a result of EAP.

b) The PMN function obtains the key and related information from the authenticator function.

c) When the PMN generates a registration request (Registration Request) it uses the PMIP key to create the Mobile-Home Authentication Extension (MHAE) to authenticate the registration request to the HA. The PMN MAY include the NAI extension in the Registration Request

d) When a HA receives a registration request, if it does not have the SPI/keys corresponding to the MN, it queries the AAA server via an AAA Request.

e) The AAA server validates the request and sends an AAA Response with the MN-HA key (PMIP key) corresponding to the Proxy-MIP Client that is identified in the Request. After receiving the PMIP key, the HA validates the MHAE in Registration Request, and processes the Registration Request and generates a registration response with a valid authentication extension using the same MN-HA key.

Further exchanges of Registration Request and Registration Reply can happen without contacting the AAA server until the expiration of the MN-HA key.

7.8.1.14.2 Client-MIP Security

7.8.1.14.2.1 Client MIP Authentication

For Mobile Ipv4 authentication MN-HA and FA-HA authentication are mandatory, MN-FA authentication is optional. MN-HA and MN-FA keys are derived from EAP EMSK

7.8.1.14.2.2 AAA Support

7.8.1.14.2.2.1 RADIUS Support

If using MN-FA challenge extension according to [28], the FA SHALL act as a RADIUS client in accordance with [23]. Upon initial MS access, the FA SHALL communicate user MN-FA Challenge extension information to a RADIUS Server, via the broker RADIUS servers if required, in a RADIUS Access-Request message. Upon receipt of the Registration Request from the MS, and if the SPI in the MN-AAA Authentication Extension is set to CHAP-SPI, the FA SHALL create a RADIUS Access-Request message.

If the SPI in the MN-AAA Authentication Extension is set to CHAP-SPI as per [28], the FA SHALL use MD5 when computing the CHAP challenge. If the authentication succeeds, the RADIUS server SHALL send a RADIUS Access-Accept message to the FA. If the authentication fails, the RADIUS server SHALL send a RADIUS Access-Reject message to the FA.

7.8.2 R3 Mobility Management with CMIPv6

This subsection describes requirements and procedures for Mobile IP operation with Ipv6 (CMIPv6) [53]. Within the Mobile IP framework, an MS with Mobile IP stack maintains a persistent IP address when handing off between different subnets. Mobile Ipv6 provides the user IP routing service to a NSP's network.

CMIPv6 is different from CMIPv4 ([43]) in many ways. The most obvious differences are the lack of a foreign agent (FA) in CMIPv6, and the support for route optimization (RO) in CMIPv6. Instead of a FA, CMIPv6 uses a co-located care-of-address (CoA) that is in the mobile node, which is then communicated with the HA using a binding update message. The CoA can be derived by the mobile node using several methods; the most common methods are stateless autoconfiguration [16] and stateful configuration using DHCPv6 [42]. Route optimization is another advantage that CMIPv6 has over CMIPv4. It will allow the correspondent node to communicate directly to the mobile node without having to transverse the home network. The mobile node registers its bindings with the correspondent node and then the correspondent node will check its binding cache and can route traffic directly to the mobile node. If the correspondent node cannot support the binding cache, then it will simply route the IP packets to the mobile node's home address and the HA will forward to the CoA.

CMIPv6) is adopted as the preferred mobility management protocol for all applicable usage/deployment scenarios requiring seamless inter-subnet/inter-prefix layer-3 handovers for Ipv6 based SS/MSs. The R3 Mobility solution has four functional components— a MIP client, a Home Agent (HA) typically located in the user's home network (but MAY be dynamically assigned/requested from a visited operator's network), a correspondent node, and a AAA server.

A WiMAX mobile node cannot be connected to its MIPv6 home network. In other words, the MN never directly connects to its Home Link. To ensure macro mobility between ASNs a subnet cannot span multiple ASNs. To work within these restrictions several assumptions need to be made and enforced. They are as follows.

- Each ASN SHOULD be a unique subnet to the Visited CSN
- A MS SHOULD have no more then one (1) MIP "home" network.
- The MIP "Home" network SHALL belong to a CSN domain.

7.8.2.1 CMIPv6 Specific Functional Requirements

- Efficient use of wireless link. Extra overhead over the air-interface to accomplish R3 mobility SHALL be minimized.
- IP address assignment and host configuration SHALL be performed per Section 7.2.2.2 of this document.
- The MIP client SHOULD be located above all physical adaptors and can be integrated into the OS stack.
- To support DAD on the MS's CoA, the ASN-GW which acts as access router SHALL perform proxy DAD function, that maintain all the assigned CoA information and responses to Neighbor Solicitation from MS for DAD,

7.8.2.2 Network Initiated Mobility

R3 Mobility handover procedure is always initiated by the network. The following types of event can trigger the procedure:

1) MS mobility: The MS hands off to a new Base Station under a new Access Router.

2) Wake-up from idle mode: The MS wakes up from the idle mode under a different Access Router than the one under which it entered the idle mode.

3) Resource optimization: The network decides for resource optimization purposes to transfer the R3 endpoint for the MS from the serving Access Router to a new Access Router, independently of any MS movement.

7.8.2.3 CMIPv6 Extensions

The MIPv6 Client SHALL include the NAI Option [59], in all CMIPv6 message.

7.8.2.4 Mobile IPv6 Operations

The following standards SHALL be used for Mobile Ipv6 operation with any limitations or extensions described in this document:

- Mobility Support in Ipv6 [RFC 3775]
- Mobile Node Identifier Option for Mobile IPv6 [RFC 4285]
- Authentication Protocol for Mobile IPv6 [RFC 4283]
- draft-ietf-mip6-ikev2-ipsec-08.txt
- draft-ietf-mip6-hiopt-02.txt

7.8.2.4.1 Dynamic Home Agent assignment

In roaming cases the Home Agent can be assigned by either the Home NSP or the Visited NSP. It's the home operator that will decide based on the roaming agreement with the visited operator and/or the end-user's subscription profile which network is responsible for assigning the MIPv6 Home Agent.

If a Home Agent is assigned in the visited network the MIPv6 authentication will take place between the visited HA and the Home AAA server. The visited AAA proxy is not involved in the MIPv6 security part.

If the HA is to be assigned by the Home CSN both the Home Agent address is appended to the AAA reply by the Home-AAA server. For Home Agents in the Visited CSN the AAA proxy can append the Home Agent address to the AAA exchange between the home AAA server and the authenticator.

For static agreements between two operator domains (e.g. HA always in the visited network) the AAA proxy can be configured to add a HA address based on the Home-AAA server domain.

For more dynamic Home Agent location algorithms (e.g. based on subscription profile) the AAA proxy decision to append to HA address will depend on the presence of the HA address container in the AAA reply from the home AAA.

Although not considered very scalable the address of a HA in the visited network can be provided by the home AAA server based on pre-configured information.

The Home Agent information can be provided in the form of an IP address or a FQDN. The Home Agent information received from the AAA system is conveyed to the MS via DHCPv6.

7.8.2.5 CMIPv6 R3 Mobility Management

This section describes requirements and procedures for the MIPv6 R3 mobility management.

At the time of the initial MIPv6 session establishment, when a new intra ASN Data Path tunnel is established between the Access Router and the new target BS, the MIPv6 client receives new mobile router advertisement messages as defined in section 7.5 of [53] to trigger the MS to perform a new CCoA update and binding update to the HA

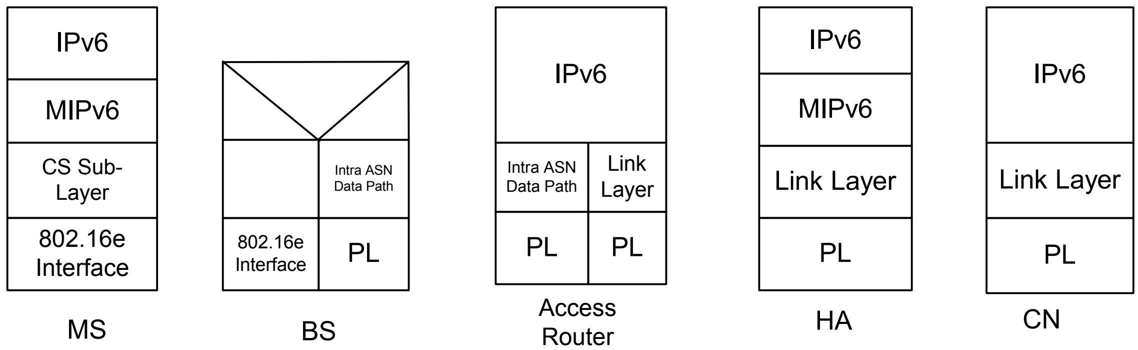


Figure 7-78 - CMIPv6 Data Plane with Tunneling

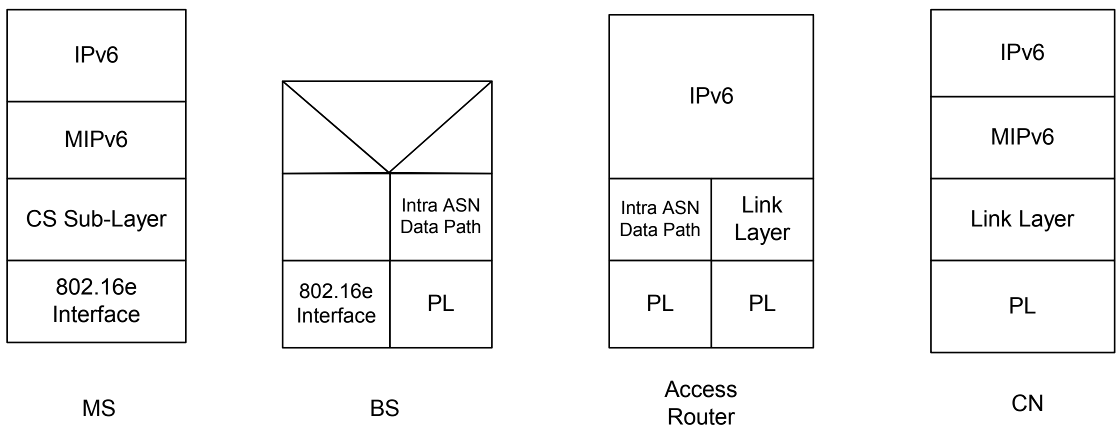


Figure 7-79 - CMIPv6 Data Plane with RO

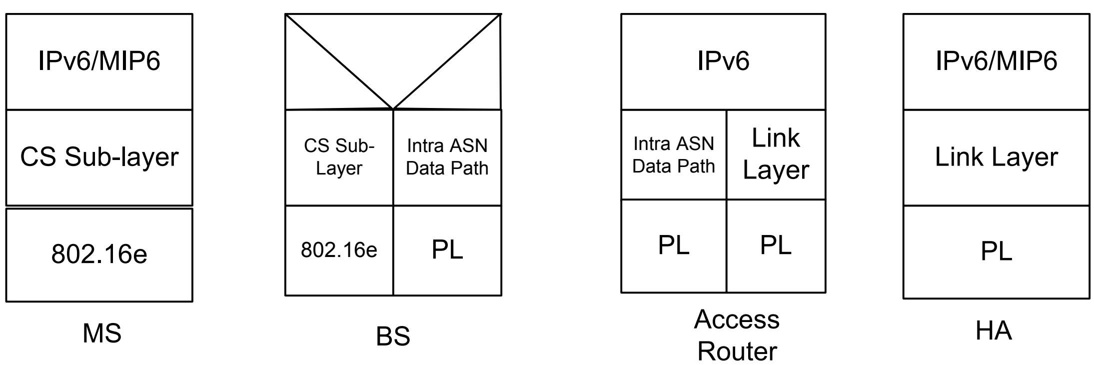


Figure 7-80 - CMIPv6 Control Plane

The MIPv6 client in the MS participates in the message exchanges required to perform anchor CSN mobility. The MIPv6 client supports dynamic address assignment and dynamic HA allocation.

7.8.2.5.1 CMIPv6 Connection Setup and Authentication Phase

In order for the MS to authenticate and authorize with the home network, the MS includes the mobility options carrying the authentication protocol [58]. This type of authentication and authorization allows the MS to perform Home Registration without IPsec. The HA can authenticate and authorize the MS based on other identity credentials that are included in the BU such as the MN-HA authentication mobility option or the MN-AAA authentication mobility options [59].

For an initial home registration, the MN uses the MN-AAA authentication mobility option.

Upon successful access level authentication, the MS obtains the AAA-Key/MSK and possibly the HA address allocated to the user. When HA address is not assigned, the MS can obtain the HA address as part of the Mobile IP registration messages exchange.

The following signaling flow describes the connection setup phase:

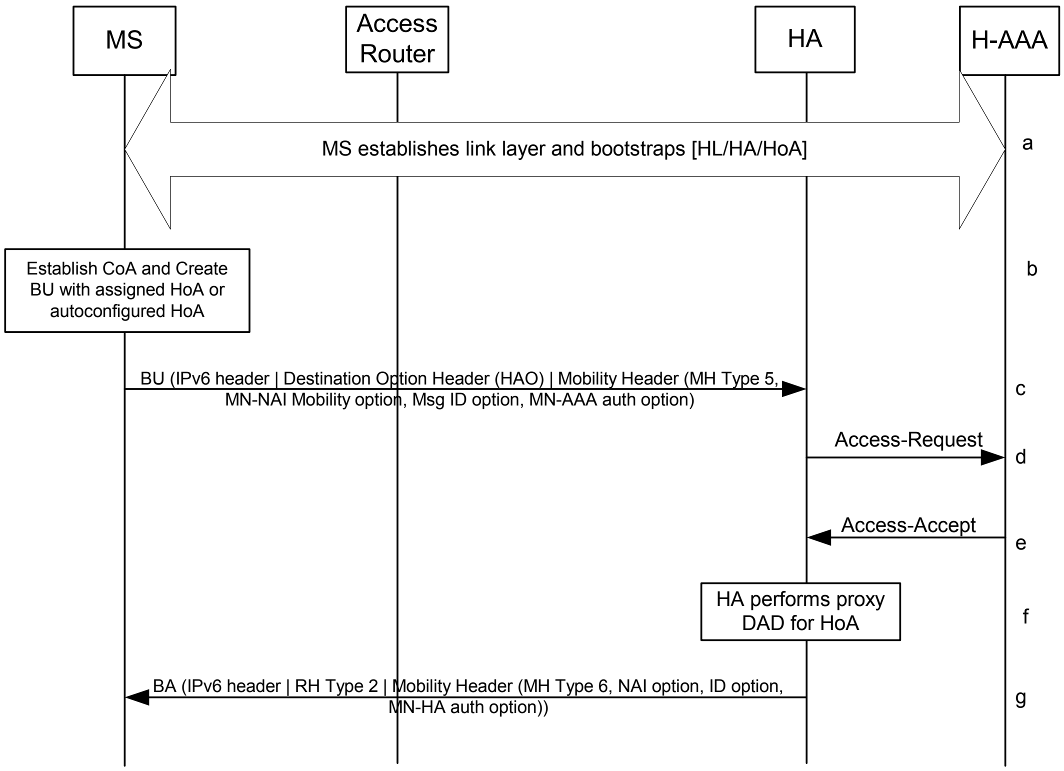


Figure 7-81 - CMIPv6 Connection Setup

a) The MS performs Link Layer establishment. Optionally, the MS acquires bootstrap information from the Home AAA server (via the Access Router). The MS uses stateless DHCPv6 [51] to obtain the bootstrap information.

b) If the MS is assigned a new HoA in step a, the MS begins to use it. If no HoA was assigned in step a, the MN generates (auto-configure) an Ipv6 global unicast address. It MAY be based on Home Link Prefix information if it was received in step a. MS generates a CoA address based on subnet-id received in router advertisement messages

c) At this step the MS sends a Binding Update (Mobility Header type 5) to the selected Home Agent. The MS sets L to 1 if the MS wants the HA to defend (through proxy DAD) its link-local and global addresses created with the same IID. The fields in this BU are set as per [53], [58], and [59]. In the BU, the MS includes the MN-AAA authentication mobility option.

d) The HA extracts the NAI, authenticator etc. from the BU and sends a AAA Access Request message to the Home AAA server. This step always occurs for the initial registration regardless of whether the MS is using an auto-configured HoA.

3. The Home AAA server authenticates and authorizes the user and sends back an AAA Access-Accept to the HA indicating successful authentication and authorization. At this step the Home AAA server also distributes the MN-HA Key to the HA for subsequent MN-HA processing.

e) At this step the HA performs replay check with the ID field in the received BU. The HA MAY optionally performs proxy Duplicate Address Detection (DAD) on the MS's home address (global) using proxy Neighbor Solicitation as specified in [15].

f) Assuming that proxy DAD is successful, the HA sends back a Binding Acknowledgment (Mobility Header type 6) to the MS. In this BA message the HA includes a Type 2 Routing Header (RH) destined to the MS's home address, the MN-HA authentication mobility option, MN-NAI mobility option and the ID mobility option. The MN-HA authenticator is calculated based on the Integrity Key that was derived in the Home RADIUS server and sent to the HA at step e).

7.8.2.5.2 CMIPv6 Session Renewal

To update session state in the network and allow a context release in case of SS/MS or network failure the MIPv6 context SHALL be renewed. The client sends Mobile Ipv6 binding update messages to the HA according to [53]. Upon receiving the binding update the HA will reset the MIPv6 session timer. Authentication is based on the prior keys obtained during initial authentication and as such do not require a synchronization with the user authentication server. The following depicts the message flow.

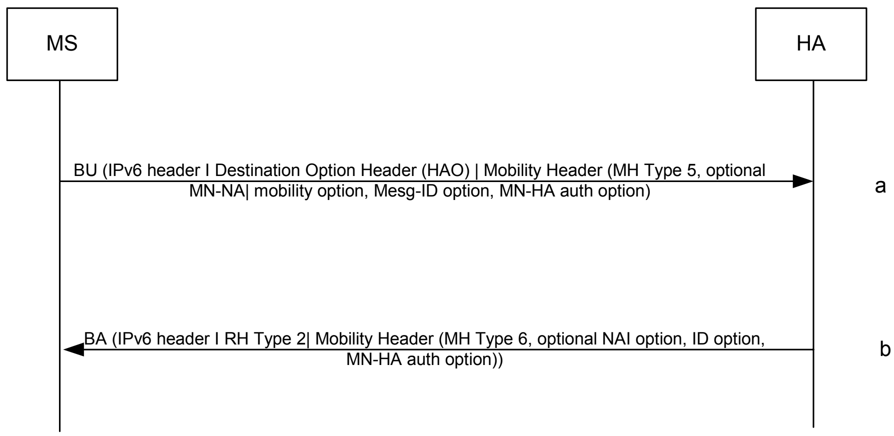


Figure 7-82 - CMIPv6 Session Renewal, MIP Re-Registration

a) The MS sends a BU to the HA. The BU includes ID and the MN-HA authentication mobility options. The BU MAY also include the MN-NAI mobility option. The MN-HA authenticator is computed with the CMIPv6-MN-HA key.

b) The HA authenticates the BU by verifying the MN-HA authenticator using the stored MN-HA Key. The HA performs replay check. If both authentication and replay check succeeds, the HA sends a BA back to the MS. The BA contains the MN-HA authentication mobility option. The BA contains the MN-NAI mobility option.

Replay protection is provided using the Mobility message identification option as specified in [58]. Timestamp based replay protection is used in this document for the both MN-AAA and MN-HA authentication mobility options.

7.8.2.5.3 MIPv6 Inter Access Router Handovers

As previously mentioned, CMIPv6 R3 mobility handovers are always network initiated. Even when the mobile initiates the handover to a new BS and Access Router, the R3 mobility is a result of a network event that strives to minimize impact on real time traffic when migration R3 from anchored to serving Access Router.

7.8.2.5.3.1 Inter Access Router Handover

The following flow diagram describes the inter Access Router handover.

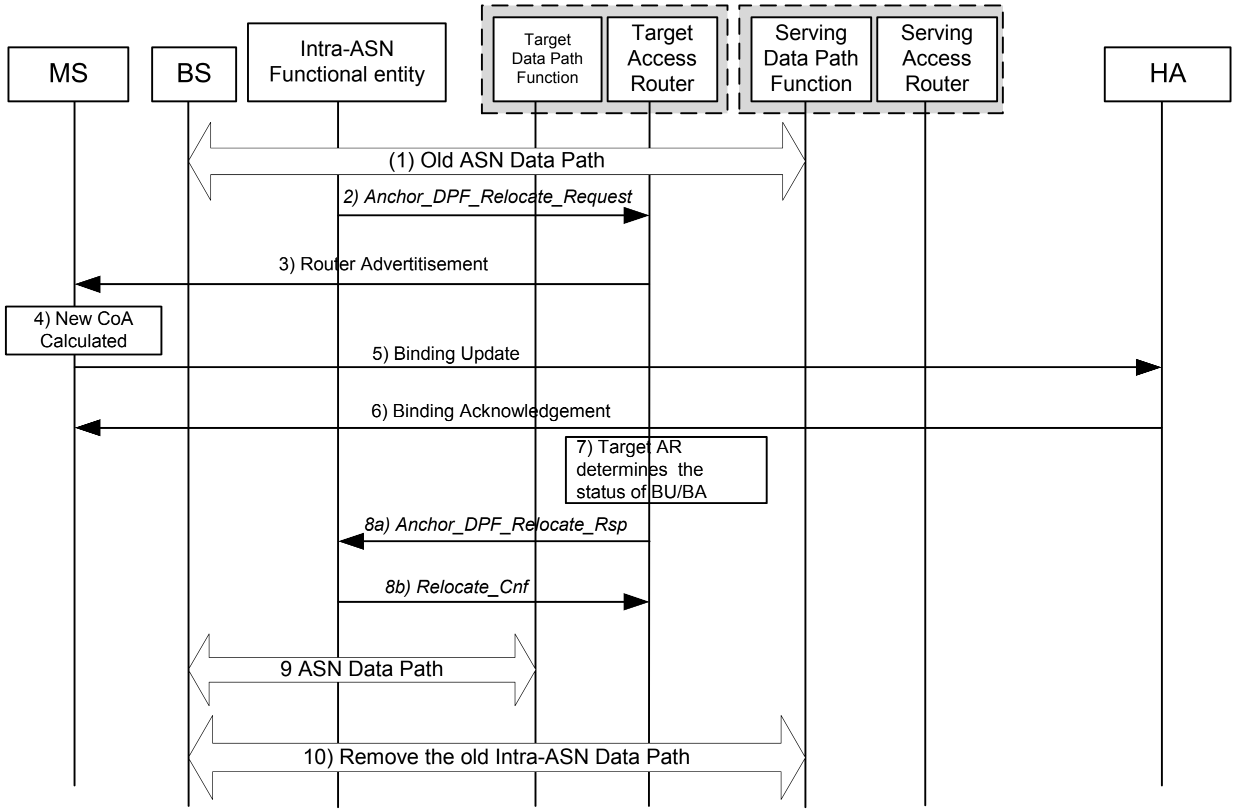


Figure 7-83 - CMIPv6 Mobility Event Triggering a Network Initiated R3 Re-Anchoring (CMIPv6)

1-2) *Old Access Router:* Arrows 1 represent the old intra-ASN data path prior to handover.

2) *Inter/Intra-ASN mobility trigger*: R3 handovers is initiated by an ASN Functional Entity.

After successful R3 Handover the Intra-ASN Functional entity is notified by an R3 *Anchor_DPF_Relocate_Rsp*. This message is acknowledged by sending the R3 relocation.Confirm. This completes the establishment of the new MIP context.

3) Upon receiving R3 mobility relocation trigger, target Access Router sends router advertisement to MS.

5-6) *MIP context update*: New binding with the HA is created

7) The Target AR determines the state of the MIPv6 registration process by parsing the BU/BA in a passive mode

8) *Inter-ASN context update*: After successful R3 Handover the Intra-ASN Functional entity is notified by an R3 *Relocation_Rsp*. In case of an unsuccessful handover the Intra-ASN Functional Entity is also informed so that the old states can be restored.

9) *Establishment of new Intra-ASN tunnel*: Together with an R3 re-anchoring also new intra-ASN Data Paths need to be established.

10) Upon successful R3 relocation the old ASN Data Path between serving and target Access Routers can be released

7.8.2.5.4 Router Advertisements

The router advertisements are sent as per IPv6 address configuration procedures.

7.8.2.5.5 MIPv6 Session Termination

In the case where a MS's IPv6 session has to be terminated, the MIP6 binding state between the MS and the HA has to be gracefully removed.

The two termination scenarios are:

- An MS initiated graceful termination: a session is gracefully terminated by sending a MIPv6 binding update message with lifetime = 0. This termination is triggered either by the user or MS being in an error conditions such as low battery power, etc.
- Network initiated graceful termination: a session is gracefully terminated by sending an R3_Session_Release.Request message from the ASN-Functional Entity to the Serving Access Router. The AR can in turn send a RA to the MS with Router Lifetime set to 0. This will force the MS to terminate it's IPv6 session with the AR. This should also prompt the MS to send a binding update with the lifetime=0 to the HA. For transport of the BU/BA, the AT needs to keep the IPv6 session alive until the MS is able to de-regiester successfully with the HA. This will require the AR to inspect the BU/BA in a passive mode so that it can determine when to remove the IPv6 session state with the MS and initiate R6 teardown. The conditions for network initiated termination MAY be some error conditions with respect to the MS such as the MS being identified as a rogue MS with security violations, planned maintenance, etc. This scenario is depicted in Figure 7-84.

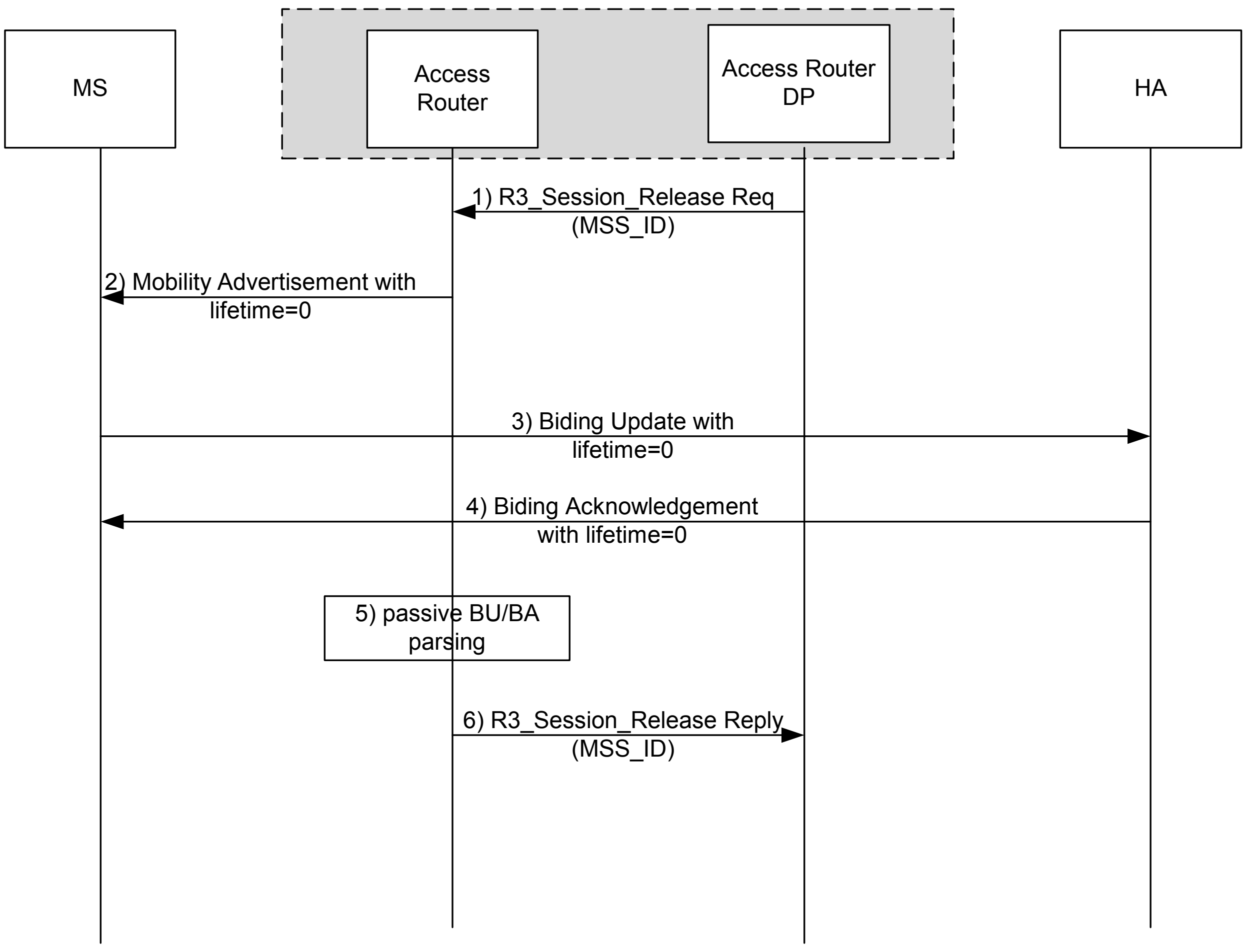


Figure 7-84 - CMIPv6 Network Initiated Graceful Termination

7.8.2.5.6 Dynamic Home Agent Assignment via CMIPv6 Bootstrap

The Home AAA server allocates the Home Agent and the Home Link Prefix to an MS during access authentication using MIP6 Home Agent VSA and MIP6 Home Link Prefix VSA. The MS obtains the assigned HA information using stateless DHCPv6 procedures as described in Figure 7-85.

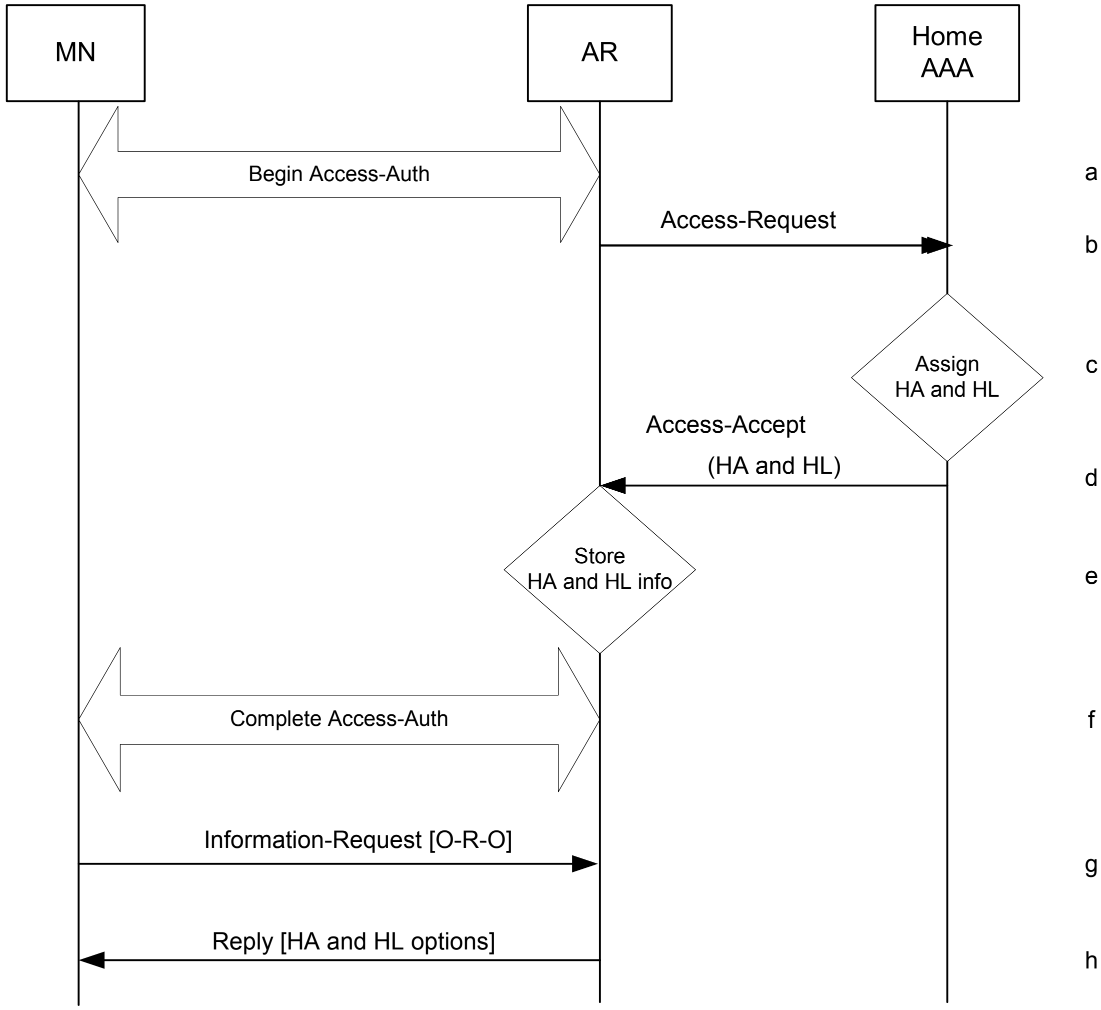


Figure 7-85 - Flow Diagram for Dynamic Home Agent Assignment

a) The MS begins the Access Authentication procedure.

b) The AR sends Access-Request to the Home AAA server.

c) The Home AAA server verifies the user's profile and detects that the user is a MIP6 subscriber. The Home AAA server assigns an HA and a Home Link Prefix for the MS.

d) The Home AAA server includes a Home Agent address in the MIP6 Home Agent VSA. The Home AAA server also includes a Home Link Prefix in the MIP6 Home Link Prefix VSA.

e) The AR receives the HA and HL information VSAs from the Home AAA server and stores them.

f) The Access Authentication procedure completes at this step.

g) The MS requests MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent to the AR. The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-hiopt-00.txt.

h) The ASN looks up the appropriate record based on the Client Identifier and replies back to the MS [51] with the options that were requested, attaching the HA information in a DHCP WiMAX Vendor Option with a Vendor-Specific Option-Code=1. It also attaches the HL information in a DHCPv6 opcode as defined in draft-jang-mip6-hiopt-00.txt.

7.8.2.5.7 Dynamic Home Link Prefix Discovery via CMIPv6 Bootstrap

The Home Link Prefix information is delivered the AR during the authentication setup phase. The Home RADIUS server selects the Home Link Prefix and includes it in a MIP6 Home Link Prefix VSA in the Access-Accept message. The Home Link Prefix information is delivered to the MS when the MS sends a DHCPv6 Information-Request message.

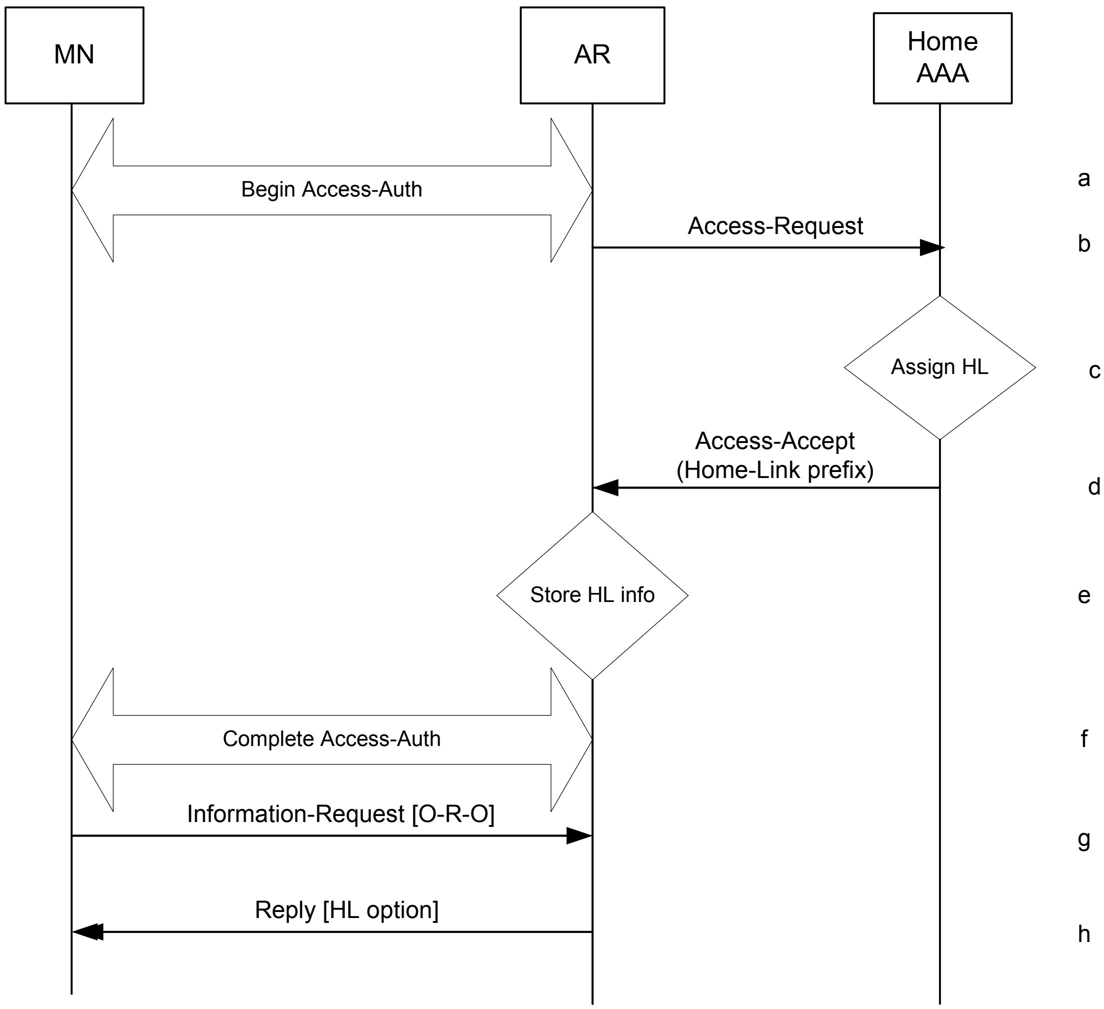


Figure 7-86 - Bootstrap of Home Link Prefix

a) The MS begins the Access Authentication procedure.

b) The AR sends Access-Request to the Home AAA server.

c) The Home AAA server detects that the user is a MIP6 subscriber by verifying with the user's AAA profile.

d) The Home AAA server assigns a HL prefix for the MS.

e) The Home AAA server includes the assigned Home Link Prefix in an AAA MIP6-Home Link Prefix VSA.

f) The AR receives the HL information from the Home AAA server. The AR stores the HL information. The Access Authentication procedure completes at this step.

g) The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent to the AR. The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-hiopt-00.txt.

h) The AR looks up the appropriate record based on the Client Identifier and replies back to the MS [51] with the options that were requested and attaches the HL information in a DHCP option as specified in draft-ietf-mip6-hiopt-00.txt

With the assigned Home Link Prefix, the MS performs dynamic Home Agent Address discovery by using the procedure defined in [53] Section 5.3. The MS also auto-configures a Home Address with the assigned Home Link Prefix.

7.8.2.5.8 Dynamic Home Address Configuration

The MS is allowed to perform stateless auto-configuration of its Home Address based on the Home Link Prefix. Alternatively, the MS MAY be assigned a Home Address by DHCPv6 [42]. In either case, the Binding Cache Entry (BCE) Lifetime is limited by the home-link prefix lifetime at the HA. This is controlled by the HA via the lifetime field in the Binding Acknowledgement message sent to the MS. The MS can request an extension to the HoA/BCE lifetime by sending a Binding Update to the Home Agent.

Once the BCE expires, the MS SHALL NOT use the HoA from the expired session. The MS SHALL initiate the bootstrapping procedure when starting a new MIP6 session if the MS does not have the registration information (i.e., HL Prefix, HoA, HA) provisioned.

If the Binding Refresh Advice mobility option is present in the BA message [53], the Refresh Interval field in the option SHALL be set to a value less than the lifetime value being returned in the Binding Acknowledgement. This indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval. The HA SHALL still retain the registration for the BCE lifetime period, even if the mobile node does not refresh its registration within the refresh period. However, if the mobile node does not refresh the binding by sending a new BU to the HA before the BCE lifetime expires, the HA SHALL delete the BCE.

7.8.2.5.9 Home Address Assignment by DHCPv6

7.8.2.5.10 Home Address Auto-Configuration by the Mobile Station

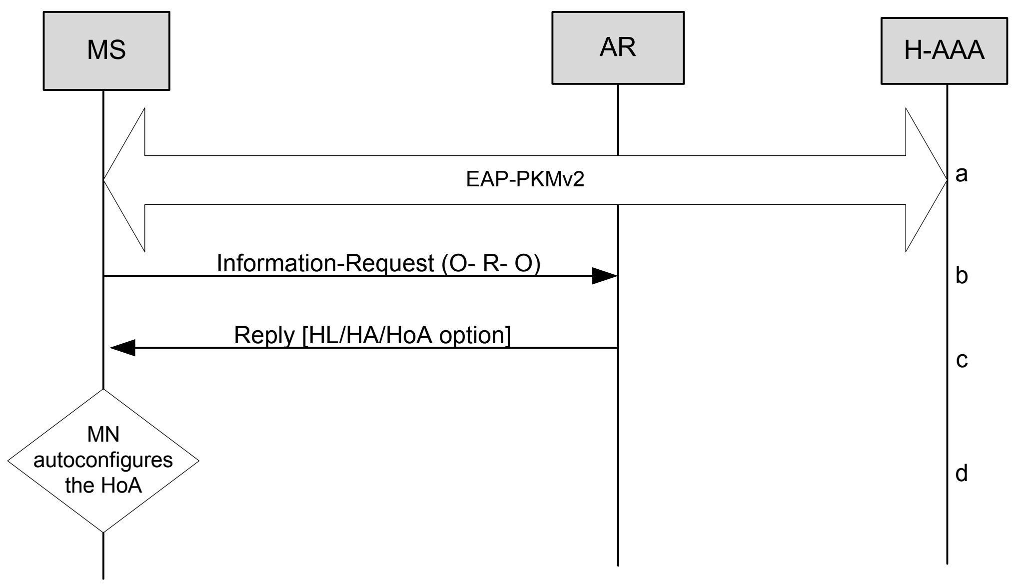


Figure 7-87 - Home Address Auto-Configuration

a) The MS performs Device Authentication using EAP-PKMv2.

b) The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent to the AR The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-hiopt-00.txt.

c) The AR looks up the appropriate record based on the Client Identifier and replies back to the MS [51] with the MIP6 bootstrap options.

d) Upon receiving the MIP6 bootstrap information from the AR, the mobile station checks whether a HoA is included or not. If HoA is not included, the MN uses the Home Link Prefix. The MN auto-configures the Home Address in a stateless manner as described in [16].

7.8.2.6 Home Agent Requirements to Support Dynamic Home Agent Assignment

The HA SHALL support Dynamic Home Agent Address Discovery as defined in [53].

The HA SHALL process Binding Updates that contain Mobility message authentication options (MN-HA or MN-AAA), Mobility message Identification (ID) option and MN-NAI mobility option.

7.8.2.7 Home Agent Requirements to Support Dynamic Home Address Configuration

The Home Agent SHALL support Home Addresses that are either assigned by the Home AAA server or auto-configured by the Mobile Station as long as the use of the Home Address by the user (NAI) is authorized by the Home AAA server and the proxy Duplicate Address Detection procedure on the Home Link passes. In the case where the MS uses an auto-configured HoA, no authorization check against the HoA is performed by the Home AAA server. The HA does not include the HoA information in the AAA Access Request message.

Upon receiving a Binding Update containing Mobility Message Authentication Mobility Options (MN-HA or MN-AAA), Mobility Message Mobility Message replay protection option, MN-NAI mobility option and a Home Address Option (HAO) with a unicast Ipv6 address in the Home Address field, the HA SHALL process the Binding Update. The HA SHALL perform proxy Duplicate Address Detection for the requested Home Address as per RFC 3775. The lifetime in the Binding Acknowledgement is controlled by local configuration at the Home Agent or it is set to the valid-lifetime remaining for the home-link prefix ([15], Section 4.6.2).

7.8.2.8 Multiple Registrations

The HA SHALL support multiple home registrations with the same NAI but different Home Addresses. The Binding Cache Entry (BCE) in the HA SHALL be indexed with the NAI and the Home Address of the MS at a minimum. The HA SHALL rely on the Home AAA server to authorize a user to perform multiple simultaneous home registrations on the same home link.

The MS is allowed to send more than one Binding Update for home registration with different HoA and with same or different CoA. Whether these home registrations will be allowed or disallowed depends on the Home Network provider's policy. If multiple registrations are not authorized, the HA will receive an AAA Access-Reject message for subsequent home registration authorization.

7.8.2.9 Home Registration Support

The HA SHALL support the Authentication Protocol [58] and IPsec/IKEv2 [ref draft-ietf-mip6-ikev2-ipsec-06.txt] based Home Registration.

The following sub-sections describe the detailed HA requirement.

7.8.2.10 Authentication Protocol Based Home Registration Support

The HA SHALL support Mobile Ipv6 authentication protocol as defined in [58] and the MN-NAI mobility option as defined in [59]. Upon receiving the BU, the HA SHALL perform authentication of the BU based on the Mobility authentication option contained in the BU and the MN-NAI mobility option.

7.8.2.11 Authentication with MN-AAA Authentication Mobility Option

The authentication protocol operation is as per RFC 4285. The MS and the HA uses CMIPv6 specific keys that are derived and distributed by the HAAA server.

7.8.2.12 Authentication with MN-HA Authentication Mobility Option

The authentication protocol operation for MN-HA Mobility Option processing is as per RFC 4285.

7.8.2.13 IPsec/IKEv2 based CMIPv6

The MS can perform IPsec/IKEv2 based Mobile IPv6 home registration. The detailed procedure for this type of Mobile IPv6 access is described in draft-ietf-mip6-ikev2-ipsec-06.txt.

7.8.2.14 Return Routability Support for Route Optimization

The Home Agent SHALL support Return Routability (RR) for Route Optimization as specified in [53] with the exception that IPsec is not used to protect (ESP encrypted) the RR messages when auth protocol is in use. These messages MAY be protected on a hop-by-hop basis through the operator's network. When IPsec/IKEv2 is used, the messages (HoT/HoTi) can be protected using ESP to meet the RR requirement

7.9 Radio Resource Management

7.9.1 Functional Requirements

The functional requirements for Radio Resource Management are:

a) RRM specification SHALL be based on a generic architecture that enables efficient radio resource utilization in a WiMAX network.

b) Generic architecture implies that while RRM implementations MAY assist several other WiMAX network functions that impact available radio resources at any given time (QoS, Service Flow Admission Control, mobility management, network management, etc.), the RRM functionality itself MAY be specified independent of any such functions that RRM assists as long as inter-vendor interoperability is not affected.

c) RRM specification SHALL define mechanisms and procedures to share radio resource related information between ASN network entities (e.g. BS or ASN-GW). Examples of such information include wireless link capability or available spare capacity in a BS.

d) RRM procedures SHALL allow for different BSs to communicate, in a standardized manner, with each other or with a centralized RRM entity residing in the same or a different ASN to exchange information related to measurement and management of radio resources.

e) Each BS SHALL perform radio resource measurement locally between itself and the population of MS served by it, as per IEEE 802.16 specifications. Procedures for such measurements SHALL remain out of the scope of NWG specifications, even though such measurements MAY be used as a basis for radio resource allocation and reconfiguration decisions by ASN network entities (e.g. BS or ASN-GW).

f) It SHALL be possible to deploy RRM in an ASN using Base Stations that have no direct communication between them.

g) It SHALL be possible to deploy RRM in an ASN using Base Stations that support direct communication between them.

h) It SHALL be possible to deploy RRM in an ASN using Base Stations with RRM function as well as a centralized RRM entity that does not reside in the BS, and that collects and updates radio resource indicators from several BSs in a standardized way. These indicators SHOULD be sufficient to provide the required information for making such decisions as choice of Target BS, admission or rejection of Service Flows, etc. The frequency of such collections MAY be dependent on a vendor/operator's specific requirements. The content of such collections, however, SHALL be specified.

i) The architecture SHALL NOT require a BS to dynamically collect Radio Resource indicators from other BSs. However, the architecture SHALL allow a BS to learn about neighboring BSs using

   - Static configuration data (e.g., existence of neighboring BSs)
   - Another RRM entity in the ASN that is aware of dynamic load situation of neighboring BSs

RRM procedures MAY provide decision support for one or more of the following WiMAX network functions. However, RRM specification SHALL NOT be tied to any one of the following functions as long as inter-vendor interoperability is not affected:

a) MS Admission Control and Connection Admission Control— i.e., ascertaining a priori that required radio resources are available at a potential target BS before handover.

b) Service Flow Admission Control— i.e., creation or modification of existing/additional service flows for an existing MS in the network. Selection of values for Admitted and Active QoS parameter sets for Service Flows.

c) Load Control—manages situation where system load exceeds the threshold and some counter-measures have to be taken to get the system back to feasible load.

d) Handover preparation and Control—for improvement/maintenance of overall performance indicators (for example, RRM MAY assist in system load balancing by facilitating selection of the most suitable BS during a handover.)

e) RRM procedures SHALL only specify the interfaces (i.e., protocols and procedures) between functional RRM entities residing in BS or outside BS (e.g., a centralized RRM entity in ASN-GW or elsewhere). Any interfaces between these RRM entities and other control entities in ASN (e.g., QoS, session management, etc.), while feasible, SHALL be outside the scope of RRM specification.

In some ASN function split profiles, an RRM entity and the said other control entities that MAY benefit from RRM data are collocated in the same logical component (e.g. BS or ASN-GW), so the information exchange between them is internal communication.

a) RRM communication procedures SHALL be interoperable and compliant with IEEE standards.

b) RRM communication procedures SHALL provide for interoperability between BS, ASN-GW, or other ASN network elements from different vendors.

There MAY be a need for an additional function in the ASN which takes care of network resources measurement and might be labeled Network Resource Measurement and Sampling (NRMS). It SHOULD monitor the transport channel resources, collecting measurements about R6 reference point resources, R4 reference point resources and R3 reference point resources. The NRMS might be located in the ASN-GW or in a BS, depending on ASN Profile. This function is not considered part of RRM, however a close cooperation of RRA, RRC and NRMS will be recommended.

7.9.2 Functional Decomposition

7.9.2.1 Functional Entities

RRM is composed of RRA and RRC from signaling transaction perspective as follows:

a) **Radio Resource Agent (RRA)—** This functional entity resides in BS and each BS shall have an RRA. It maintains a database of collected radio resource indicators. An RRA is responsible for assisting local Radio Resource Management (RRM) as well as communicating to the RRC, if present, including for example:

- Collection/Measurement of radio resource indicators from the BS.
- Collection/Measurement of radio resource indicators from the population of MS registered to the BS, using MAC management procedures as per IEEE 802.16 specifications and other measurement reporting for upper layers (e.g. derived bit error rate, MAC PDU error rate).
- Communicating RRM control information over the air interface to MS, as per IEEE 802.16 specifications. An example of such RRM control information is set of neighbor BSs and their parameters.
- Signaling procedure exchange with RRC for radio resource management function.
- Controlling the radio resources of the respective BS, based on the measurements performed and measurement reports received by the BS and based on information received from the RRC functional entity if available. This local resource control includes power control, supervising the MAC and PHY functions, modifying the contents of the MOB_NBR-ADV broadcast message (by help of information from RRC or from management system), assisting the local Service Flow Management (SFM) function and policy management for Service Flow admission control, making determinations

and conducting actions based on radio resource policy, assisting the local HO functions for initiating HO etc.

b) **Radio Resource Controller (RRC) —** This optional functional entity MAY reside in BS (one per BS), in ASN-GW, or, as a standalone server in an ASN. The RRC MAY be collocated with RRA in the BS, or separate. In the former case, the interface between RRC and RRA is out of the scope of this specification. Such RRC MAY also communicate with RRCs in neighboring BSs which may be in the same or different ASN. In the latter case, RRC MAY reside in the ASN-GW (or as a standalone server) communicating to RRAs across R6 reference point. When RRCs are present in ASN, each RRA shall be associated with exactly one RRC. On the other hand an RRC may be associated with zero, one or more RRAs in the same ASN. An RRC is responsible for:

- o Collection of radio resource indicators from associated RRA(s): When RRA is collocated with RRC in the same BS, the interface between RRA and RRC is outside the scope of this specification. When RRA(s) and RRC are separated across R6 reference point, the collection of radio resource indicators SHALL be as per primitives and information reporting procedures defined in this specification.
- o Communication between/across RRCs: An RRC MAY communicate with other RRCs across NWG-specified interfaces.

c) **RRC Relay** — This functional entity MAY reside in ASN-GW for the purpose of relaying RRM messages. RRC Relay cannot terminate RRM messages but it only relays these to the final destination RRC

When RRC is collocated with the BS, RRCs in different BSs SHALL communicate through the RRC Relays located in the ASN-GWs when there is no R8 interface. If the R8 is exist, RRCs in different BSs may communicate through the R8 interface.
When RRC resides in ASN as a standalone server or in ASN-GW, RRCs MAY communicate across R4 reference point.

Standardized RRM procedures are required between RRA and RRC, and between RRCs across NWG-specified interfaces. These procedures are classified into two types:

- **Information Reporting Procedures** for delivery of BS radio resource indicators from RRA to RRC, and between RRCs.
- **Decision Support Procedures** from RRC to RRA for communicating suggestions or hints of aggregated RRM status (e.g., in neighboring BSs) for various purposes.

7.9.2.2 RRM Generic Reference Models

RRM reference model MAY take one of the following two forms as follows:

Generic Reference Model #1 is shown in Figure 7-88.

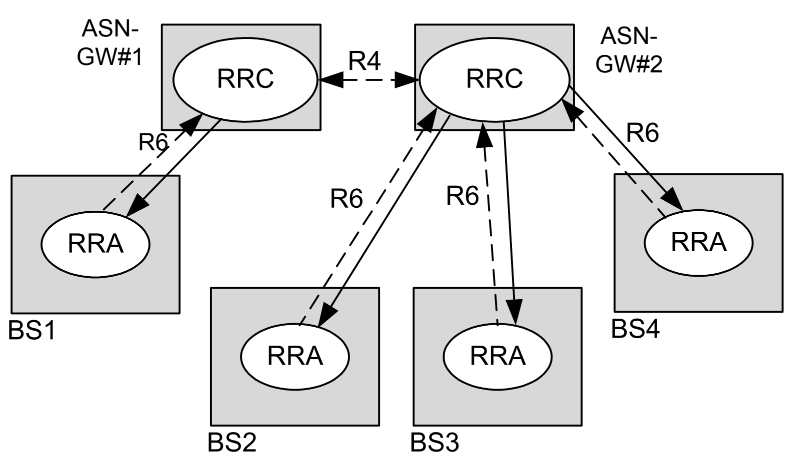


Figure 7-88 - RRAs Resident in BS and RRC Resident in ASN

The above reference model is based on RRA in each BS and RRC resident outside BS in the ASN. RRAs and RRC interact across R6 reference point, using two types of procedures visible at NWG-specified open interfaces—information reporting procedures (dashed lines) and decision support procedures (solid lines). RRCs MAY communicate with each other using R4 reference point.

Generic Reference Model #2 is shown in Figure 7-89.

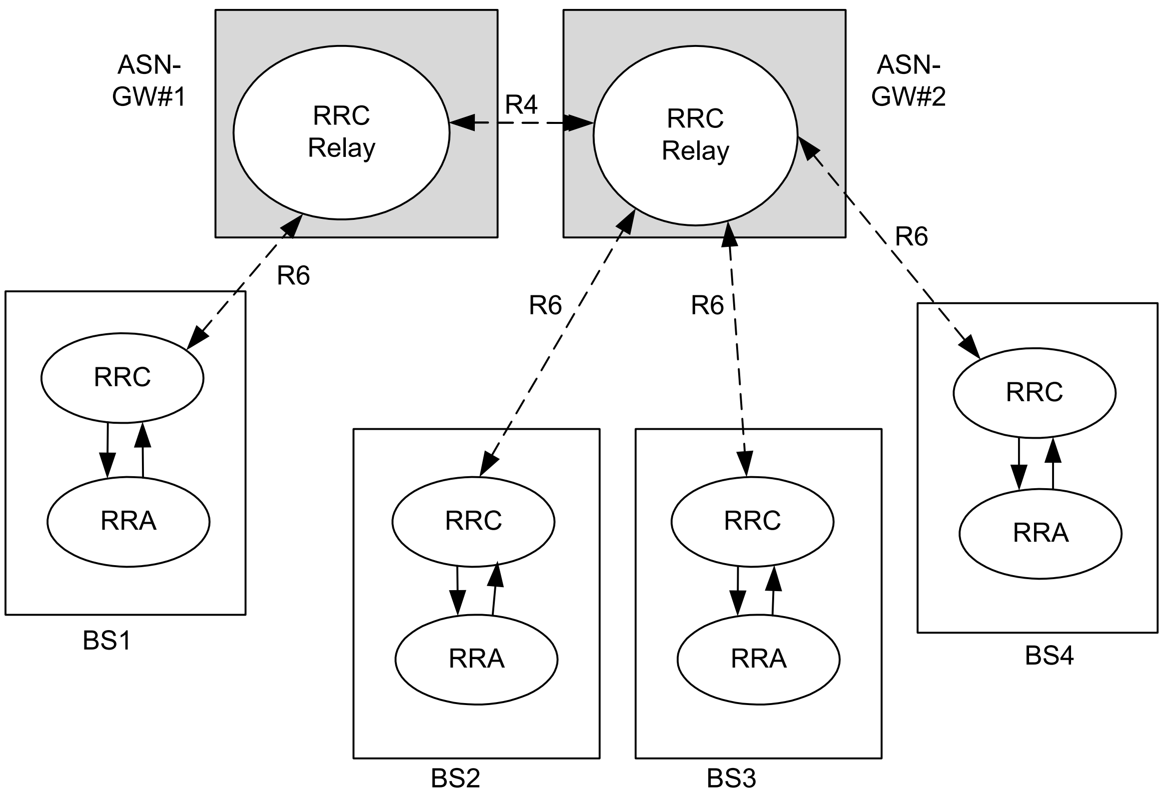


Figure 7-89 - RRA and RRC Collocated in BS

The above reference model is based on collocated RRA and RRC in each BS. The interface between RRA and RRC is outside the scope of this specification. We introduce the "RRC Relay" in the ASN to enable the RRC-RRC communication within and between ASNs over the standard reference interfaces. RRC Relay resides in the ASN GW and acts as a relay for the RRM messages.

Note: this reference model is based on the assumption that there is no R8 reference point, which may be used for direct communication between BSes.

The above two generic reference models can be mapped to the ASN reference model and ASN entities.

7.9.3 Primitives

RRM primitives MAY be used either to report radio resource indicators (i.e., from RRA to RRC, or, between RRCs) or, to communicate decision support information (i.e., from RRC to RRA). The former type of primitive is called information reporting primitive and the latter is called decision support primitive.

The following information reporting procedures SHALL be supported:

a) **Per-BS Spare Capacity Reporting procedure** — These reports are indexed by BS ID and indicate the radio resources available at the BS (BS-ID refers to a sector with a single frequency assignment), e.g. as a hint for Base Station selection during network entry or handover. Such reporting MAY be solicited or unsolicited. Such reports SHALL be sent from RRA to RRC as well as between RRCs such that all interested RRCs MAY have available information on current spare capacity of the BS for which they are responsible, or, of neighboring BSs. – Note that this report does not refer to the service requirements of a specific MS and hence is not a replacement of the "*HO_Req* and *HO_Rsp*" specified for the Intra-ASN Handover preparation phase.

b) **Per MS PHY Service Level Reporting procedure** — These reports are indexed by MS. Such reporting is always solicited by RRC. Such reports SHALL be sent from RRA to RRC to update the per-MS databases in the RRC. These reports SHALL be generated for MS registered with the BS that is associated with the RRC. (See section 7.9.4.3 - Per-MS PHY Measurement Solicitation and Report)

The following decision support procedures SHALL be supported:

c) **Neighbor BS radio resource status update** — These reports are delivered from RRC to RRA to propose a change of the broadcasted advertising message. (See section 7.9.4.4 - Neighbor BS Radio Resource Status Update)

Corresponding to these information reporting and decision support procedures, the corresponding RRM primitives are listed in Table 7-4.

Table 7-4 - Primitives for RRM

Name	Source	Destination	Purpose	Reporting or Decision support
RRM *PHY_Parameters_Req*	RRC	RRA	Request for *PHY_Parameters_Rpt*, per MS.	Request reports from RRA
RRM *PHY_Parameters_Rpt*	RRA	RRC	Assessment of link level quality per MS.	Reporting from RRA to RRC
RRM *Spare_Capacity_Req*	RRC	RRA/RRC	Request for *Spare_Capacity_Rpt* per BS.	Request reports from RRA; Request reports from RRC
RRM-Spare-capacity-report	RRA/RRC	RRC	Available Radio Resource report per BS.	Reporting from RRA to RRC; Reporting between RRCs
RRM-Neighbor-BS radio resource status update	RRC	RRA	Update the broadcasted Neighbor BS list	Decision support
RRM-Radio-configuration-request	RRC	RRA/RRC	Request for *Spare_Capacity_Rpt* per BS.	Request reports from RRA; Request reports from RRC
RRM-Radio-configuration-report	RRA/RRC	RRC	Available Radio Resource report per BS.	Reporting from RRA to RRC; Reporting between RRCs

Note: The final set of RRM procedures is defined in the Stage-3 Specification.

7.9.4 Procedures

This subsection describes the protocol primitives at a functional level.

- Request for per-BS *Spare_Capacity_Rpt*
- Per-BS *Spare_Capacity_Rpt*

- Request for per-MS PHY measurement report
- Per-MS PHY measurement report
- Neighbor BS radio resource status update

Note: The final set of RRM procedures is defined in the Stage-3 Specification.

7.9.4.1 Request for *Spare_Capacity_Rpt*

This primitive can be applied by an RRC to request a Per-BS *Spare_Capacity_Rpt* from an RRA or from another RRC.

An RRC SHALL send this request whenever to query spare capacity in a BS.

The RRC MAY send this request periodically or at any time. The RRC MAY also send this request based on a network event trigger.

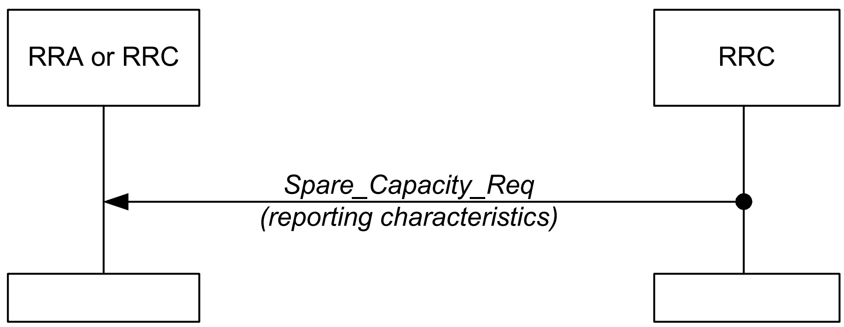


Figure 7-90 - Request for *Spare_Capacity_Rpt*, per BS

Reporting characteristics: Indicates whether report SHOULD be sent periodically, or event-driven etc. The detailed list of events is given in the Stage-3 Specification:

7.9.4.2 Per-BS *Spare_Capacity_Rpt*

RRA (RRC) SHALL send the following type of report to RRC:

Spare_Capacity_Rpt which includes the “Available Radio Resource” indicator (percentage of reported average available sub-channels and symbols resources per frame. The average is over a configurable interval with a default value of 200 frames).

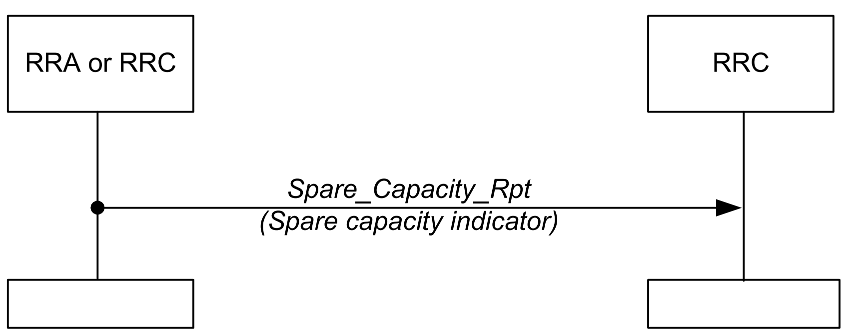


Figure 7-91 - *Spare_Capacity_Rpt*, per BS (Unsolicited or Solicited)

The report MAY be sent periodically or event-driven. The detailed list of events is given in the Stage-3 Specification.

A tabular representation of the Spare Capacity Reporting primitive reporting the “Available Radio Resource” indicator is given in the Stage-3 Specification.

DL (UL) Available Radio Resource:

Available Radio Resource indicator SHALL indicate the average percentage of available physical radio resources for DL (or UL, respectively) where averaging SHALL take place over a configurable time interval with a default value of 200 frame. Available physical radio resources SHALL be defined as the set of subchannels and symbols within a radio frame, which are not used by any non-best-effort service flow class.

7.9.4.2.1 Usage Scenarios

The “Available radio resource” measurements provided by the RRAs to RRC MAY be used by RRC for load balancing: A potential strategy of RRC MAY be to interact with the HO controller with the objective to have approximately equal load, as expressed by the “available resource indicator”, in all BSs controlled by RRC – subject to the availability of suitably radio path conditions between a MS and the potential HO target BSs.

The “available radio resource” indicator SHALL be determined by the BSs as specified above.

Possible ways of RRM interaction with the HO decisions have been described in NWG Stage-2 specification; Section 7.7 - ASN Anchored Mobility Management and 7.8 - CSN Anchored Mobility Management. In Network Initiated Handoff as well as in MS Initiated Handoff, the ASN uses Handover Request primitive to communicate with a number of candidate BSs for permission to handoff a MS or MS’. The candidate BS list MAY be recommended or modified by the external module such as RRC.

7.9.4.3 Per-MS PHY Measurement Solicitation and Report

This primitive can be applied by an RRA to report to an RRC, or by an RRC to report to another RRC.

RRC MAY use this primitive exchange once it has received a *HO_Req* from Serving BS to learn (or recollect a more updated set of parameters) regarding the MS PHY service levels for the Serving BS and each candidate BS. In addition, RRC MAY check the latest “Spare capacity report” whether capacity is available for adding the MS, and RRC will return the updated list of candidate BSs to Serving BS.

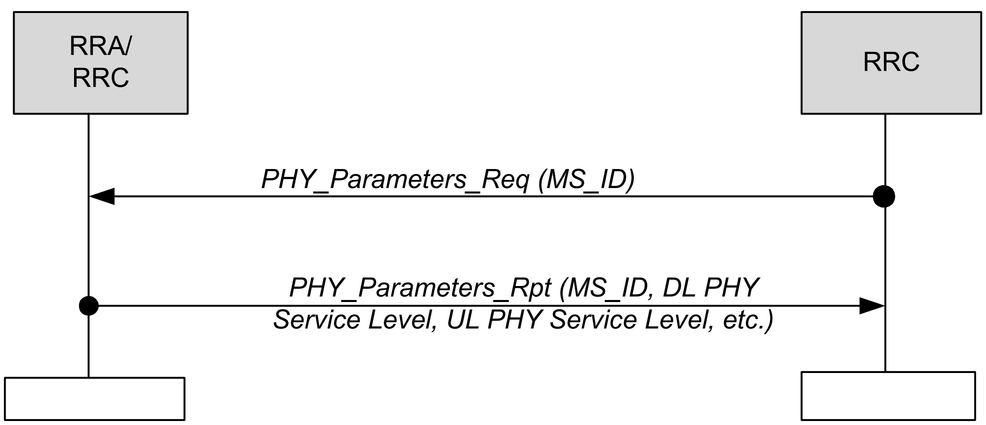


Figure 7-92 - PHY Report (Solicited)

As per this primitive exchange, the BS SHALL send the following types of reports to RRC:

PHY reports for DL & UL per MS. These reports include the set of parameters described in Section 8.4.11 of [1]. Additionally, these reports include the PHY feedback parameters (on a per-MS basis). All parameters are encoded in TLVs.

DL parameters are measured by MS and reported by BS to RRC. UL parameters are measured and reported by BS to RRC. Same parameters MAY be reported from one RRC to another.

A tabular representation of the PHY Report primitive is given in the Stage-3 Specification

In case the RRC is collocated with Target HO Function, it MAY be possible to include these measurement reports into the Handover-Request messages or *HO_Rsp* messages sent from BS to the HO Control. This is FFS.

In order to meet a Stage-1 Requirement for channel quality monitoring, this message might be augmented to include measurements related to QoS parameters, e.g. "burst error rate". – To be checked during work at Stage-3.

7.9.4.4 Neighbor BS Radio Resource Status Update

This procedure can be used by RRC to inform a Serving BS about the list of Neighbor BSs which are potential HO Target Base Stations for any MS being served by the SBS, including information about their radio resource status. It is important consideration for the serving RRC to synchronize the radio resource information that are received from the RRAs of the neighbor BSs as well as from other RRCs to provide the accurate and up-to-date information to the RRA of the Serving BS in order to allow the MS to make appropriate HO decision. The policy on the information processing at the RRC and the frequency of the status update is outside the scope of this specification.

RRA (in SBS) MAY use this hint from RRC as a basis for updating the Neighbor BS Advertisement: SBS would ask the MS to trigger the scanning of the respective neighbor BSs, by means of MOB_NBR_ADV.

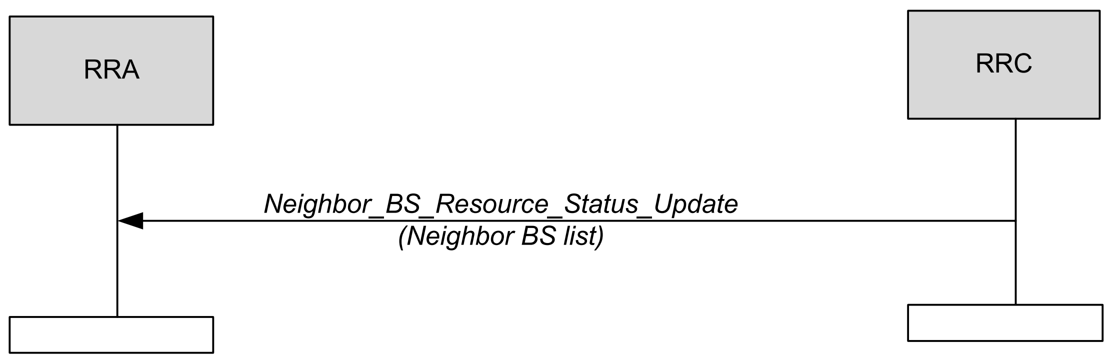


Figure 7-93 - Neighbor BS Radio Resource Status Update Procedure

A tabular representation of the RRM-Neighbor-BS-Radio-Resource-Status-Update primitive is given in the Stage-3 Specification. The primitive has been suitably adopted from MOB_NBR-ADV message format, as defined in [2] and amended by [80].

7.9.5 Power Management and Interference Control

In Release 1.0.0, power management and interference control is primarily a task performed by each BS. In addition there is an RRM primitive "RRM *PHY_Parameters_Rpt*", see above, for interference measurement report from RRA to RRC to allow RRC to get involved in interference control.

Power management during idle mode and sleep mode is handled elsewhere in the Stage-2 document.

Potential enhancements of power management and interference control, as well as of RRM in general, are for further study.

Future enhancements of RRM MAY include adding RRM primitives for the following applications that in Release 1.0.0 are considered to be solved locally by the BS Site, or to be left to BS configuration or Network Management:

- Reconfiguration of sub-channel space to be used in a BS (sector).
- Reconfiguration of maximum transmit power of a BS
- Reconfiguration of burst selection rules.
- Reconfiguration of radio resource allocation and scheduling policies in a BS.
- Reconfiguration of UL/DL switching point for TDD
- Reconfiguration of broadcast information (e.g. supported burst profiles)
- Forwarding of DCD and UCD information between neighboring base stations

7.10 Paging and Idle-mode MS Operation

7.10.1 Functional requirements

The following functional requirements SHALL be supported in the WiMAX network:

a) Paging features should be supported in Nomadicity and Portability usage models whereas they are mandatory for Full Mobility usage scenario (see Stage 1 document). These features shall be compliant with IEEE 802.16e.

b) Paging Groups, as defined in IEEE 802.16e, shall comprise a set of Base Stations. An access network (i.e., NAP) may be provisioned to consist of one or more Paging Groups. A NAP may comprise one or more Paging Controllers. Each Idle MS in the NAP is assigned a single Paging Controller, called Anchor PC.

c) An MS in idle mode must be accessible in the network during Paging Intervals for Paging and Location Updates. This covers cases where the MS:

   (1) stays in the coverage area of same BS in the access network or

   (2) moves to the coverage area of a new BS (in the same or different Paging Group) in the access network.

7.10.2 Functional Decomposition

The Paging operation shall comprise the following functional entities:

Paging Controller (PC) — Paging controller is a functional entity that administers the activity of idle mode MS in the network. It is identified by PC ID (6 bytes) in IEEE 802.16e, which could map to the address of a functional entity in NWG. The PC MAY be either co-located with BS or separated from BS across R6 reference point. There are two types of PCs:

- Anchor PC: For each idle mode MS, there shall be a single Anchor PC that contains the updated location information of the MS.
- Relay PC: There may also be one or more other PCs in the network (called Relay PC) that participate in relaying Paging and Location Management messages between PA and the Anchor PC

Paging Agent (PA) – Paging Agent is a functional entity that handles the interaction between PC and IEEE 802.16e specified Paging related functionality implemented in the Base Station. A Paging Agent is co-located with BS. The interaction between PA and Base Station is out of scope of NWG. When the PA is located across R6 reference point from the PC, its interaction with PC is within the scope of NWG specification. However, when PC is also co-located with BS, the interaction between the co-located PA and PC is outside the scope of NWG.

Paging Group (PG), defined in IEEE 802.16e, may be interpreted as comprising one or more Paging Agents. A Paging Group resides entirely within a NAP boundary. Paging Groups are managed by the network management system and provisioned per the access network operator's provisioning requirements. Paging Group management and its provisioning requirements are not in scope of this document.

Location Register (LR) — An LR is a distributed database with each instance corresponding to an Anchor PC. Location registers contain information about Idle mode MSs. The information for each MS includes, but is not limited to:

a) Contains MS Paging Information for each MS that has registered with the network earlier but currently in Idle mode.

   Current paging group ID (PGID)

   PAGING_CYCLE

   PAGING_OFFSET

   Last reported BSID

   Last reported Relay PCID

b) MS Service Flow Information comprising

   (1) Idle Mode retention information for each MS in idle-mode

   (2) Service Flow Information for each MS

An instance of a Location Register is associated with every Anchor PC. Specifying communication between LR and PC is outside the scope of this specification.

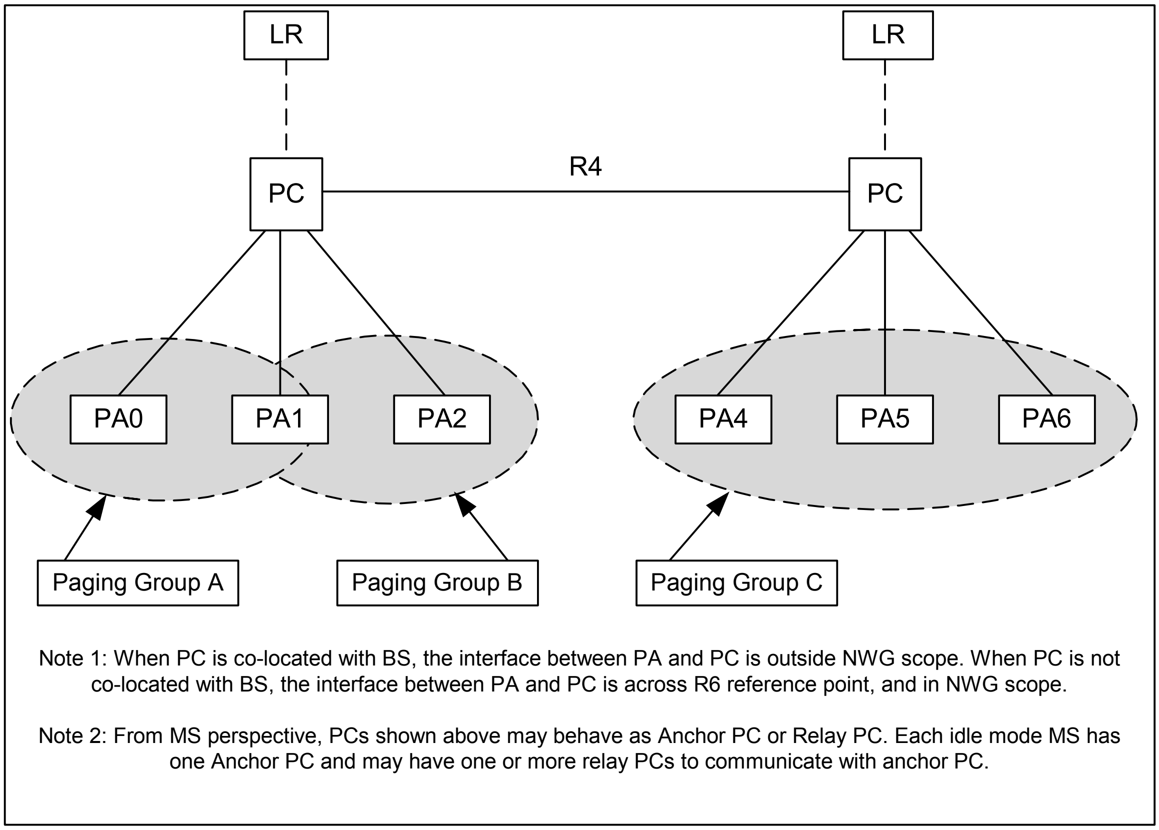


Figure 7-94 - Paging Network Reference Model

The following points are noteworthy regarding this reference model:

a) There MAY be multiple PGs inside an operator's (i.e., NAP) network domain. To keep Paging functionality optimally implemented (i.e., prevent Paging Groups from becoming too large), multiple Paging Groups shall be allowed in the network. Figure 7-94 specifies Paging Groups in reference to WiMAX network reference model. A BS (and its corresponding, co-located PA) may be part of more than one Paging Group.

b) IEEE 802.16e standard specifies PC to be co-located with either BS or a separate entity in the network. This specification describes Paging related control protocol and messages between PA and PC. For the former deployment scenario (where PC is co-located with BS), the messages between these co-located entities (PA and PC) are not exposed over an NWG specified reference point, and therefore not a consideration for interoperability. For the latter deployment scenario (where PC is not co-located with BS), Paging control protocol (messages) are exchanged over R6 reference point between PA and PC. In both deployment scenarios, Paging Control messages between PCs are exchanged across R4 reference point.

   The Location Register (LR) comprises a location database in the network. This database, accessible by/through PC, tracks the current Paging Group (identified by Paging Group Id, PGID) of each idle-mode MS in the network. It also stores the context information required for Paging. In the event of MS movement across Paging Groups, location update occurs across PCs via R6 and/or R4 interfaces and information is updated in the LR that is associated with the Anchor PC assigned for the MS.

When MS enters IDLE mode, the LR entry for this MS is created. The LR will be updated with MS idle-mode retain information. For this idle-mode MS, its Anchor PC shall be either static or may change until MS becomes active and performs a full network entry.

As MS travels in IDLE mode and crosses the boundary of it current PG, it is enforced to perform Location Update. Location Update messaging between PA and Anchor PC occurs over R6 and in some cases over R4 reference interfaces. R4 reference interface is involved when PA has no direct connectivity with Anchor PC over R6 and, therefore, needs to reach it via intermediate routing nodes (i.e. Relay PCs).

NOTE 1- For CMIP/PMIP based services, MS movements while in idle mode may not result in FA change (wakeup, MIP registration etc.)

NOTE 2- For Simple IP based services, when an idle mode MS location update results in full network entry (e.g., unsecured location update, re-authentication), the MS PoA IP address refresh may be performed.

7.10.3 Paging and Idle-Mode MS Operation Procedures

This section describes the protocols and procedures as per the above reference model.

The following is a generic case that depicts an MS about to enter IDLE mode as it is served by Foreign Agent (FA) and Authenticator in the network.

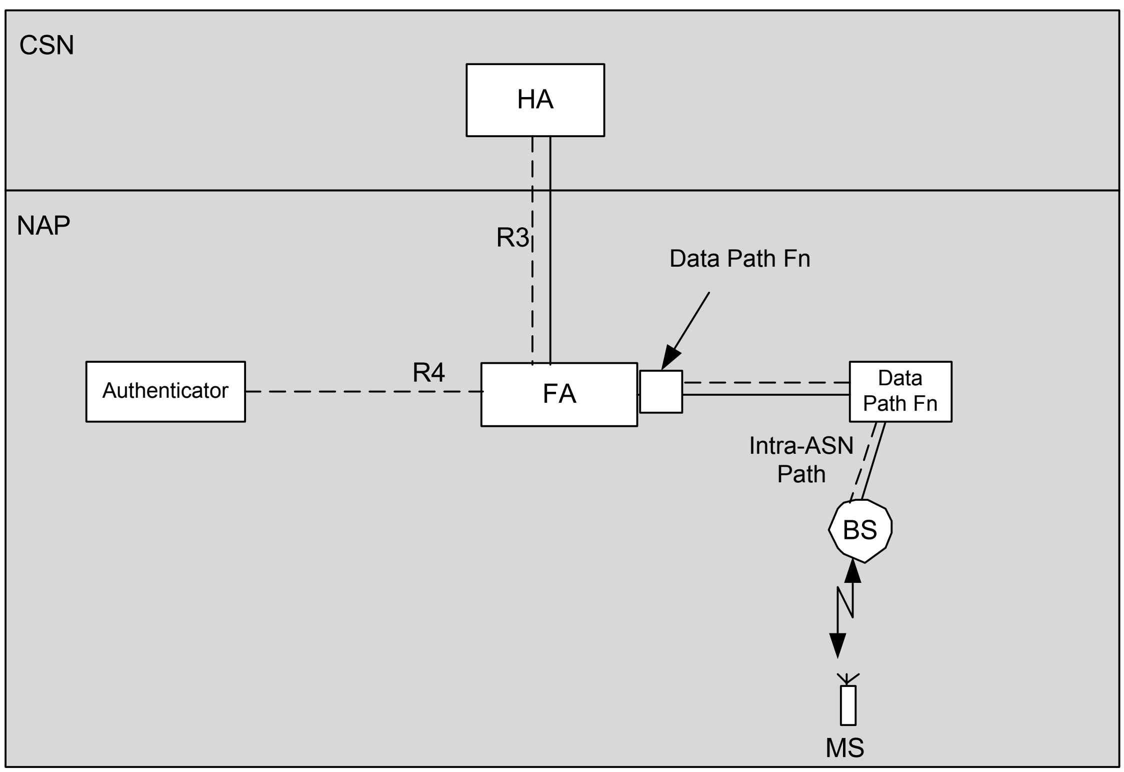


Figure 7-95 - Generic Depiction of Functional Entities Prior to MS Entering Idle Mode

When the MS enters Idle mode a PC entry for the MS is created (instantiated) and the bearer tunnels for data forwarding between Anchor Data Path Function, and BS are removed. If Anchor DPF and FA are collocated, all bearer tunnels between FA and BS are removed. Note that the ability to send R4 and R6 signaling is not impacted by the removal of the bearer tunnels. As idle mode MS moves in the network, the FA itself could be migrated as well but that is left as an implementation option.

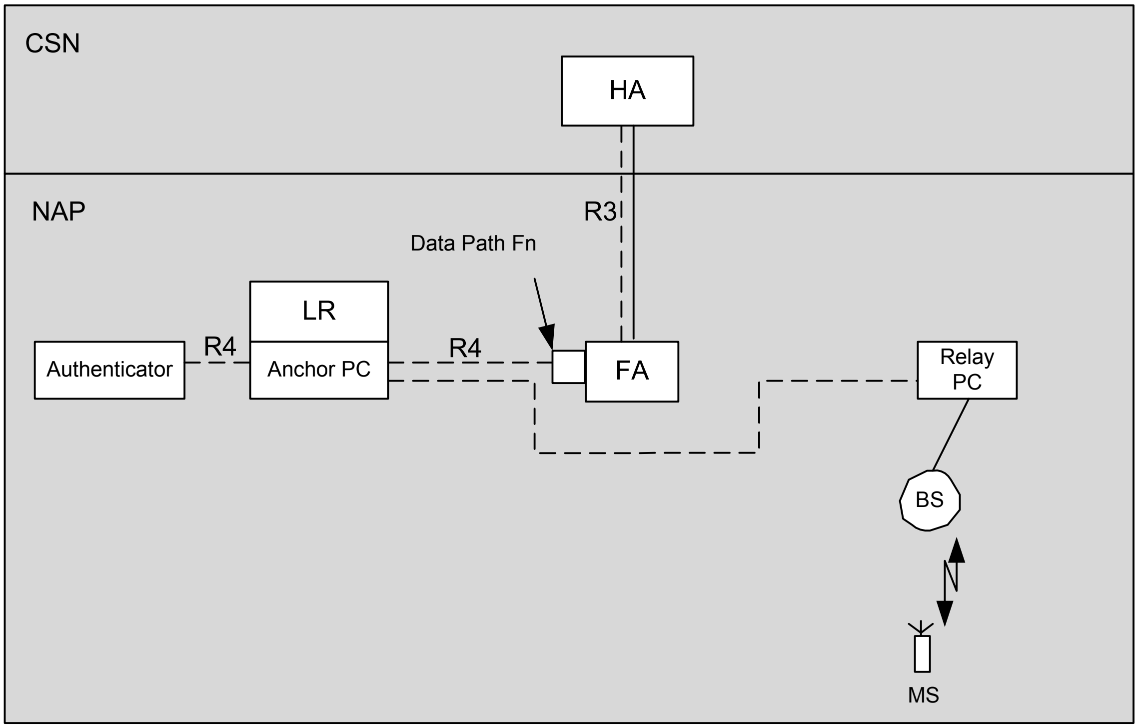


Figure 7-96 - Generic Depiction of Functional Entities after MS Enters Idle Mode

7.10.3.1 Backbone Primitives for Paging and Idle Mode

Paging and Idle Mode Primitives are divided into the following two groups:

(1) Primitives for signaling paging control and location management

(2) Primitives for signaling LR updates

summarizes the backbone primitives, which may be communicated between PA and PC.

Table 7-5 - Primitives for Paging Control and Location Management "for information only, the binding facts are defined in the Stage3 Spec"

Primitives	From → To
Paging_Announce	Anchor PC →Relay PC(s) (in PG) → PAs in PG
Location Update Request	PA → Relay PC(s) → Anchor PC
LU_Rsp	Anchor PC → Relay PC(s) → PA
Delete_MS_Entry_Req	Data Path Fn → PC
LU_Cnf	PA -> Relay PC(s) -> Anchor PC
Initiate_Paging_Req	Data Path Fn → Anchor PC

Primitives	From → To
Initiate_Paging_Rsp	Anchor PC → Data Path Fn
IM_Exit_State_Change_Req	Data Path Fn → Anchor PC
IM_Exit_State_Change_Rsp	Anchor PC → Data Path Fn
IM_Entry_State_Change_Req	Relay PC → Anchor PC
IM_Entry_State_Change_Rsp	Anchor PC → Relay PC
R4 *Delete_MS_Entry_Req*	ADPF→ APC/LR, BS/DPF→DPF/Relay PC, DPF/Relay PC→ APC/LR
R4 Anchor PC Indication	Anchor DPF/FA → Anchor PC / LR
R4 Anchor PC Ack	Anchor PC / LR → Anchor DPF/FA
R4 PC Relocation Indication	Current Anchor PC ASN → Anchor DP / FA ASN
R4 PC Relocation Ack	Anchor DP / FA ASN → Current Anchor PC ASN

The following backbone HO primitives (Table 7-6) can also be utilized in the paging 1 and location management for idle mode MS.

Table 7-6 - Reuse of HO Primitives for Paging Operation

Primitives	From → To
Context_Req	PA → Anchor PC
Context_Rpt	Anchor PC → PA
Path_Reg_Req	BS/DPF → DPF/Relay PC
Path_Reg_Rsp	DPF/Relay PC → BS/DPF
Path_Reg_Ack	BS/DPF → DPF/Relay PC
Path_Dereg_Req	BS → Serving ASN
Path_Dereg_Rsp	Serving ASN → BS

Path_Dereg_Ack	BS → Serving ASN
CMAC Update	Serving ASN → Authenticator
CMAC Update Ack	Authenticator → Serving ASN

7.10.3.2 Procedures for Paging the MS and MS Exiting IDLE mode

Paging_Announce occurs under several scenarios which include:

a) Data arriving for the MS at the Anchor DPF

b) Location update forced by the network for this MS

c) MS re-entry into the network as forced by the network

d) Cancel *Paging_Announce* once the MS has exited IDLE state.

In scenario a), when Data arrives at the anchor DPF (which may be collocated with the FA as in Figure 7-97) for the MS, thus triggering a *Paging_Announce*, the Paging context information (including PGID, Relay PCID, BSID, etc.) would be retrieved from LR associated with Anchor PC for the MS. The anchor PC may issue one or more *Paging_Announce* messages based on whatever knowledge it has of the topology of the paging group for the MS. If the anchor PC has no knowledge of the topology of the PG, it should send the Paging Announce message to an appropriate Relay PC, which can then relay the message to BSs in a Paging Region comprising BSs and zero or more relay PCs. Figure 7-97 illustrates the procedure for MS Paging upon receipt of downlink data for the MS.

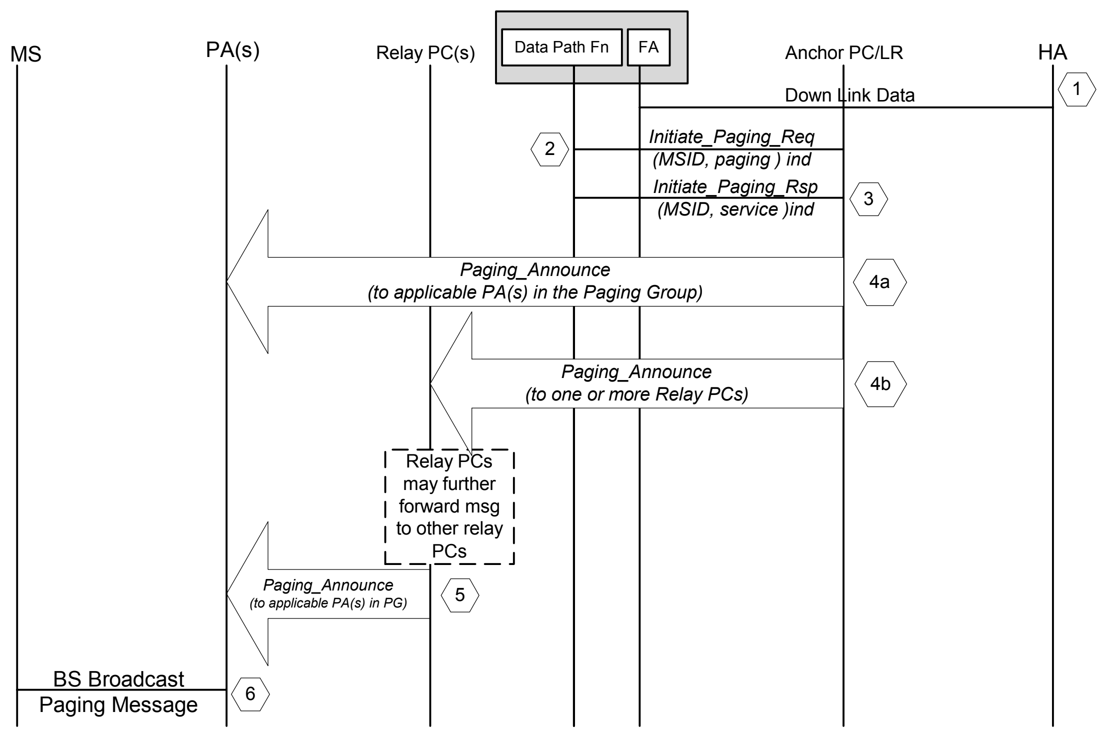


Figure 7-97 - Paging Generated for MS by Incoming Packets for MS in Idle Mode

Paging flow**:**

(1) HA sends downlink data to MS over MIPv4 tunnel to Data Path function associated with FA. In the event that there is no FA (e.g.: MIPv6), the incoming data will be buffered at the anchor DPF (not shown in the figure).

(2) The Anchor Data Path Function recognizes that MS is in Idle mode. Receiving downlink data triggers sending *Initiate_Paging_Req* to Anchor PC to initiate Paging. (anchor Data Path function keeps track of MS's Anchor PC). *Initiate_Paging_Req* contains: MSID, indication that MS is a paging candidate.

(3) Anchor PC sends *Initiate_Paging_Rsp* to Data Path function. This message may be utilized to indicate that the MS is authorized for service. For such a case, *Initiate_Paging_Rsp* contains: MSID, and service authorization indicator.

(4) Anchor PC retrieves the MS paging info (comprising PGID, paging cycle, paging offset, a relay PCID, or a set of BSIDs including last reported one) and constructs *Paging_Announce* message. The Anchor PC may issue one or more *Paging_Announce* messages based on its knowledge of topology of the Paging region. Figure 7-96 depicts two alternative methods (step 4a and 4b, respectively) for generating *Paging_Announce* messages:

a) Anchor PC may be topologically aware of Paging region to be Paged (e.g. PG). For example, it may be aware of BSs in region. In this case, the Anchor PC may issue *Paging_Announce* messages to one or more BSs and/or relay PCs in this region, or,

b) The Anchor PC may be topologically unaware of the Paging region except that it is aware of one or more Relay PCs that can forward the *Paging_Announce* message appropriately to the Paging region. In this case, the Anchor PC may issue *Paging_Announce* message to this relay PC (or relay PCs) that would in turn forward it to the Paging region.

Messages 4a) and 4b) can also be used to cancel *Paging_Announce*. This can happen in the events such as: the MS is successfully paged by one of the BSs or PC wants to stop paging, etc.

Relay PCs receiving Paging Request for the specific PG forward it to the relevant BSs or other relay PCs associated with the PGID received in Paging Request.

BSs send BS Broadcast Paging Message requesting that MS exit Idle mode. If not receiving response from MS, BS has to resend BS_Broadcast_Paging Message as specified in IEEE 802.16e specification.

Other paging scenarios described above would follow steps 4a-6 as in the above figure.

Note: The above flow does not illustrate termination of Paging Broadcast by BS.

The following depicts an example of the message flow for MS exiting IDLE mode procedure:

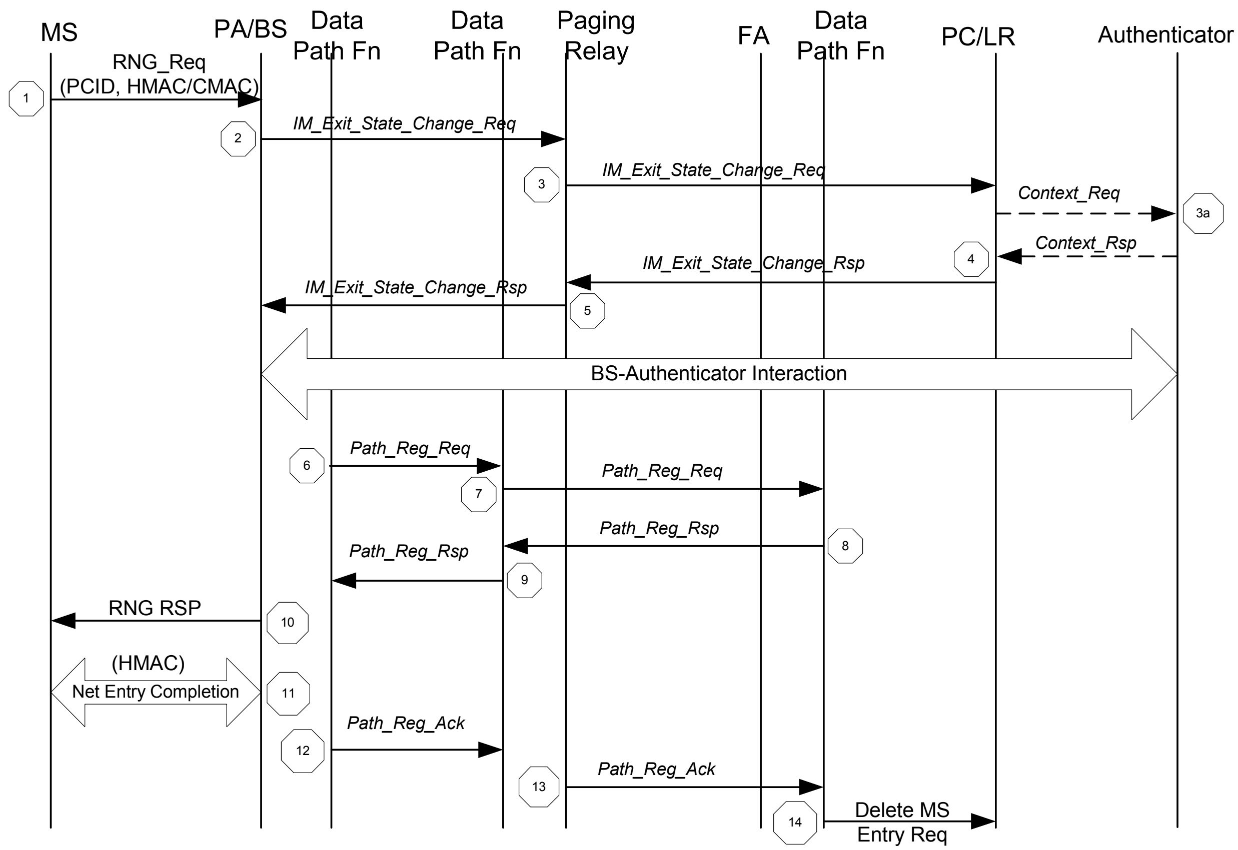


Figure 7-98 - MS Exiting Idle Mode

Flow description:

1) MS initiates exit from IDLE mode procedure (e.g., as a result of Paging) and sends RNG_REQ as described in IEEE 802.16 specification. Ranging Purpose Indication must be set to one (1) and PC ID TLV must be present, thus indicating that the MS intends to Re-Entry from Idle Mode.

2) BS receives RNG_REQ message from MS. Correspondingly, PA sends IM-Exit-State-Change Request to Paging Relay (when PA is not directly connected to Anchor PC, as shown). IM-Exit-State-Change Request contains the following information from the RNG_REQ: MS ID (MAC Address), BSID, PC ID (PCID). If the BS has the Authenticator ID and CMAC/HMAC digest already when the BS receives RNG-REQ message from MS, the BS_Authenticator interaction procedure of verifying RNG-REQ can be started simultaneously.

3) Paging Relay receives *IM_Exit_State_Change_Req* from BS and sends it to Anchor PC. Paging Relay recognizes the PC according to the received PCID field. *IM_Exit_State_Change_Req* contains the following information: MS ID (MAC Address), BSID;

4a) When receiving the *IM_Exit_State_Change_Req*, the Anchor PC/LR proceeds to request the security context from the Anchor Authenticator and receives it in a *Context_Rpt* message. If the PC and Authenticator are co-located this step is not required. It also initiates the cancel Paging Procedure at this point.

4b) Anchor PC receives the *IM_Exit_State_Change_Req*, and sends *IM_Exit_State_Change_Rsp* to the Paging Relay. *IM_Exit_State_Change_Rsp* contains the following information: MSID, ID of Anchor DPF, Authenticator ID, MS Idle Mode Retain Information, (SFIDs, CIDs, QoS context, etc.);

5) Paging Relay forwards the *IM_Exit_State_Change_Rsp* to the BS; The AK is fetched from the appropriate authenticator in order to verify the RNG-REQ.

6) The Data Path function in BS starts data path establishment – it sends *Path_Reg_Req* to the Data Path Function across R6. *Path_Reg_Req* contains the following information: MSID, Data Path Fn Id (e.g., IP Address), Service Flow info (SFIDs, QoS context, etc.) It also initiates the cancel Paging Procedure at this point.

7) The Data Path Function across R4 continues data path establishment to the anchor Data Path function (which could be collocated with FA as shown in the figure) - sends *Path_Reg_Req* to anchor Data Path Function. *Path_Reg_Req* contains the following information: MSID, Service Flow info (SFIDs, QoS context, etc.)

8) The anchor Data Path Function confirms data path establishment - sends Data Path Establishment across R4. *Path_Reg_Rsp* contains: MSID, Service Flow info (SFIDs, Tunnel parameters, QoS context, etc.)

9) The Data Path functions cross R6 confirms data path establishment toward SBS— sends Data Path Establishment Response to the Data Path Function in SBS. *Path_Reg_Rsp* contains: MSID, Service Flow info (SFIDs, QoS context, etc.)

10) BS sends RNG_RSP to the MS formatted according to IEEE 802.16e specification. This RNG_RSP SHOULD deliver information necessary to resume service in accordance with Idle Mode Retain Information.

11) The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification.

12) Upon the MS Network Re-Entry completion the BS sends *Path_Reg_Ack* to the Data Path function across R6 confirming data path establishment completion. *Path_Reg_Ack* message contains: MSID

13) The Data Path function across R4 sends *Path_Reg_Ack* to the anchor Data Path function. *Path_Reg_Ack* contains: MSID.

14) The anchor Data Path function sends a Delete MS entry message to PC/LR in order to delete the idle mode entry associated with the MS in the PC.

7.10.3.3 MS Performing Location Update, Secure Location Update

MS performs Location Update procedure when it meets the LU conditions as specified in IEEE 802.16e specification. The MS shall use one of two processes for Location Update: Secure Location Update or Unsecure Location Update. Un-Secure Location Update process is performed when MS and BS do not share valid security context means that BS is not able to receive a valid AK (e.g., MS crossed Mobility Domain boundaries or PMK expired).

Un-Secure Location Update results in MS network re-entry and re-authentication. It is performed in the same way as a regular MS network entry process.

The Secure Location Update procedure:

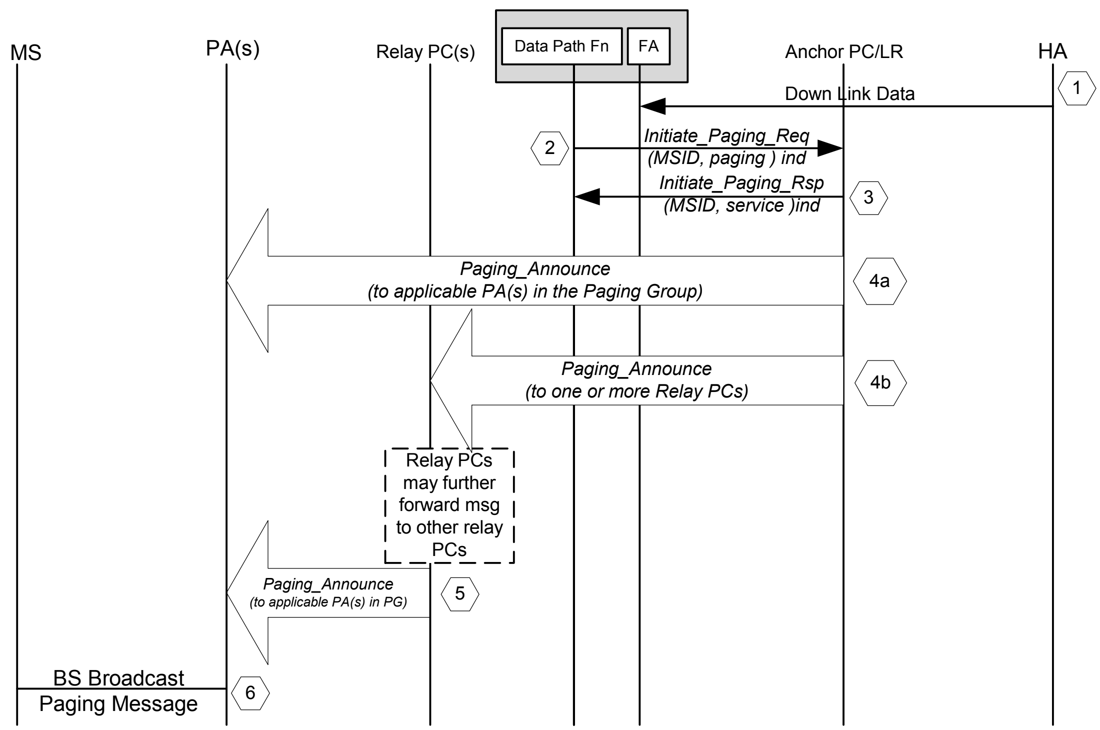


Figure 7-99 - Secure Location Update

1) MS initiates Location Update, or the Location Update is forced by network if the conditions described in IEEE 802.16e specification are met and as a result, the MS sends RNG_REQ. Ranging Purpose Indication must be set as described in IEEE 802.16e specification indicating that the MS intends to update its location. PC ID (which points to PC acting as MS's Anchor PC) must also be present.
2) PA sends *LU_Req* to the Paging Relay (as shown in the figure). It contains information like PCID, BSID.
3) Paging Relay sends *LU_Req* to Anchor PC. It contains: MSID, BSID and recommended paging parameters (PGID, Paging cycle, Paging Offset) etc.
4) When PC/LR receives a *LU_Req* message and the security information is not retained in the LR, it will request the security information from the Authenticator. If the PC and the Authenticator are co-located this step is not required.
5) If the *LU_Req* is accepted by Anchor PC and the Paging operation is still continuing, at this step .Paging_Annouce to 'Stop Page' may also be sent to the Paging groups defined for the MS. Anchor PC either accepts the recommended paging parameters or assigns new PGID and the paging parameters and sends *LU_Rsp* message to Paging relay. *LU_Rsp* includes: MSID, BSID, PGID and paging parameters, Anchor Authenticator ID, PCID etc.
6) Paging Relay forwards *LU_Rsp* to PA.
7) BS (where PA resides) determines whether it has a valid AK for the MSID from the indicated Anchor Authenticator. If it does not, the BS sends *Context_Req* (not shown in the diagram) to the Anchor Authenticator. *Context_Rpt* (not shown) provides the AK sequence number, as well as the AK for the BS-MS secure association (as specified in 7.20.2 "Context Transfer Protocol"
8) BS (where PA resides) uses AK to verify the integrity of the RNG-REQ received from MS. If the MS's RNG_REQ is successfully verified, the BS responds to the MS with RNG_RSP with HMAC/CMAC. If the RNG-REQ could not be verified (such as when the Anchor Authenticator could not provide an AK), the BS begins the "Un-secure Location Update" sequence by initiating re-authentication;;
9) In the case where RNG_REQ was verified, PA sends *LU_Cnf* to Paging Relay (incl. BSID, success indication). It indicates location update from MS has been authenticated and the process is successfully completed.

10) Paging Relay forwards LU_Cnf to Anchor PC. Anchor PC receives LU_Cnf and finally updates MS location in the LR. In the event that the Location Update was triggered by paging the MS, the PC/LR initiates the cancel paging procedure (as described above). It may send the Paging Announce message to stop the paging operation within the paging groups.

11) If PC relocation has occurred during the LU procedure, the PC will send Context Response Ack message with the LU result to the Authenticator.

.

7.10.3.4 Paging Operation and R3 Mobility Management

Migration of foreign agent while the MS is in idle mode (e.g., when idle mode MS moves) shall be considered an implementation option. Such FA migration requires that MS come out of idle mode to complete MIP registration procedure.

The alternative is to not migrate FA while MS remains in idle mode. For such a scenario, the following points are noteworthy:

1) For the registration lifetime for L3 connectivity (e.g., MIP registration lifetime or DHCP lease time), the idle mode MS shall retain its IP address without IP address renegotiation. Registration lifetime will be set to max by the MS when Idle mode is entered.

2) While MS moves across PG boundaries, it performs LU as per procedures above, without resulting in any FA migration. During this time, R3 shall be maintained between Home Agent and the FA. If Anchor DPF and FA are not collocated, the bearer tunnel between the FA and Anchor DPF is also maintained.

3) Upon packet arrival at HA destined for MS, and their delivery over R3 to Data Path function associated with FA, packets shall be buffered in ASN until MS paging procedures are completed.

4) The Anchor PC sends *Paging_Announce* over R4 using either topologically aware or topologically unaware procedures. Paging Relays receiving *Paging_Announce* from PC forward it over R6 interface to all the BSs (or Paging Relay(s)) associated with the PGID in the Paging Request.) via single step or multi-step procedures (see stage 3 [xx] for details).

5) MS performs a full network entry.

6) MS may re-register with its old Home IP address. Tunnel establishment (over R6 and R4) is performed between Data Path functions in SBS, intermediate Data Path Functions, and the Data Path function associated with FA in a way similar to HO process.

7) Packets are transferred from Data Path associated with FA to other Data Path Functions in the path over R4.

8) R3 traffic anchor point (i.e., Data Path function associated with FA) and FA may migrate from the current Anchor point to another Anchor point or may optionally stay as they are.

9) When MS goes out of Idle Mode, the PC/ LR entry corresponding to this MS is deleted.

10) When MS goes into Idle Mode, serving FA could migrate to the same ASN as the anchor authenticator or as the anchor PC. This is left as an implementation option, as Idle but stationary MS will not benefit from such migration.

11) As the MS has no way to determine a-priori whether it shares a valid security context with the BS,, the MS will always include a HMAC/CMAC tuple in the RNG-REQ. The BS and the anchor authenticator will either validate the HMAC/CMAC or reject the *LU_Req*.

7.10.3.5 MS entering IDLE mode

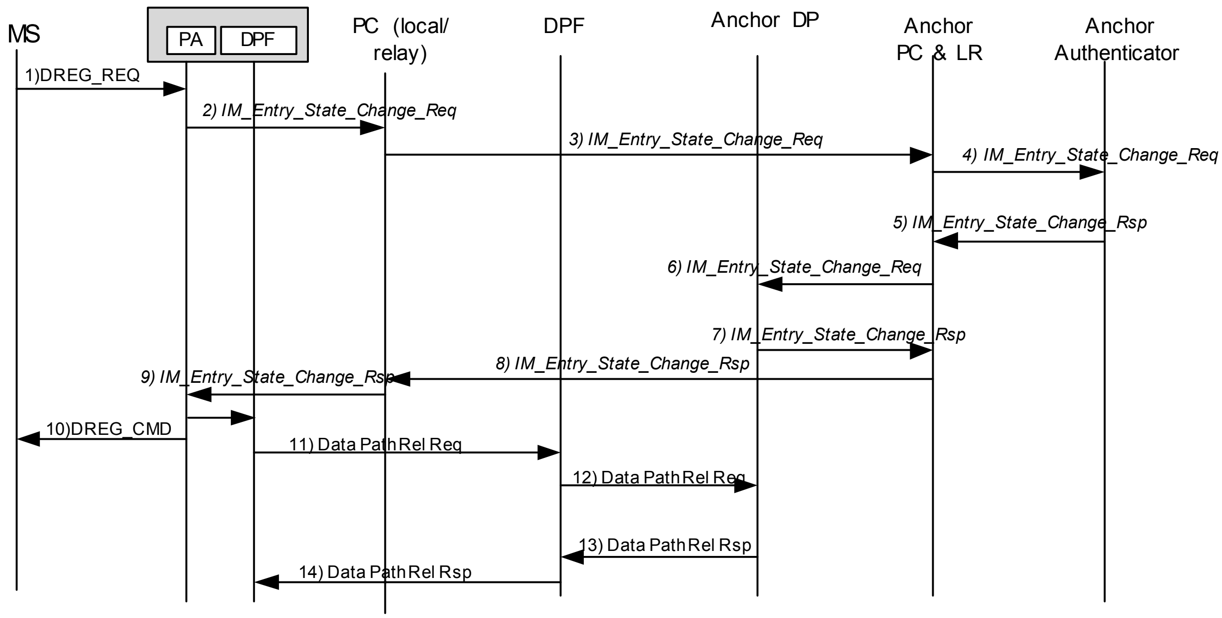


Figure 7-100 - MS Entering Idle Mode

Dashed arrows are internal to network elements and out of scope.

MS enters Idle mode when there is no data to exchange between the MS and the network. MS Idle mode entry could be initiated by either the MS or the BS.

1) If MS decides to initiate entry into Idle Mode, then it sends DREG_REQ formatted as described in IEEE 802.16e. The De-Registration Request Code is set to 0x01 indicating that the MS intends entering Idle Mode.

2) Regardless of who (MS or BS) initiated the entry into idle mode, the PA in the serving BS sends *IM_Entry_State_Change_Req* message to its local Paging Controller (who oversees paging at this base station). The *IM_Entry_State_Change_Req* contains the following information: MSID, BSID, PG_ID, Idle Mode Retain Information, etc

3) Upon receipt of *IM_Entry_State_Change_Req* from the PA, the local PC assigns an Anchor PC for this mobile, and puts this information as a recommendation into the message. The chosen anchor PC could be the local Paging Controller itself or a different PC based on implementation considerations such as network policy, MS profile or Relay PC loading conditions. Further, the local PC sends the *IM_Entry_State_Change_Req* message to the recommended Anchor PC, the *IM_Entry_State_Change_Req* message contains the following information: Recommended PC_ID, PG_ID, Paging_CYCLE, Paging_OFFSET, some MS contexts(including Anchor Authenticator ID, Anchor DPF ID etc.

4～5) The Anchor PC contacts the Anchor Authenticator to verify that the MS is allowed to enter Idle mode, and may transfer some security context to Anchor Authenticator to retain, such as PKM contexts. Anchor Authenticator records the Anchor PC ID into MS context and reply *IM_Entry_State_Change_Rsp* to Anchor PC including Idle mode authorization indication;

6~7) These steps represent the handshake between the Anchor PC and Anchor DPF of the MS entering Idle mode. Anchor PC/LR sends *IM_Entry_State_Change_Req* message to the Anchor DPF/FA to indicate the MS entering Idle Mode. The Anchor DPF updates the information of this MS including the Anchor PC ID of this MS, and then the Anchor DPF responds back with *IM_Entry_State_Change_Rsp* to Anchor PC/LR.

8) If confirmed, Anchor PC either accepts the recommended paging parameters and PGID or newly assigns these parameters and updates Location Register with current information including the DPF ID, and sends *IM_Entry_State_Change_Rsp* back to the Local PC. The *IM_Entry_State_Change_Rsp* contains: MSID, actual paging parameters (selected PGID, Paging CYCLE, Paging OFFSET), PCID (The ID of the GW Acting as

Anchored PC formatted as specified in IEEE 802.16e to be delivered to the MS with DREG_CMD as "PC ID") and IDLE mode authorization indication

9) The Local PC forwards the *IM_Entry_State_Change_Rsp* message to PA;

10) The PA sends DREG_CMD to the MS either in response to its DREG_REQ or as an unsolicited response (BS initiated entry into idle mode), as specified in IEEE 802.16e containing "PC ID" field in the DREG_CMD which points to the assigned Anchor PC for the MS, the assigned Paging CYCLE, and the assigned Paging OFFSET

11～14） After receiving DREG_REQ message from MS and the expiration of the Management Resource Holding Timer, the DPF associated with PA located in BS initiates the related R6, R4 data path release procedure.

Note: The procedure illustrated in Figure 7-100 and described here is the general procedure of accomplishing entry into idle mode. Depending on the implementation and choice of ASN profile, the procedure can be optimized by changing the sequence and flow of messages. The implementation would still be compliant to the specification as long as the messages and functional behaviors are not changed. Implementation details and optimizations are out of Stage 2 document scope, therefore a general case that is profile agnostic is described in this document.

7.11 Data Path

Section 7.7.2.2.2 introduces Type 1 Data Paths for carrying either IP or Ethernet packets between peers within an ASN or between ASNs. User payload packets are transferred over Type 1 Data Paths between ASNs (R4) or between the BS and the ASN-GW of an ASN exposing an interoperable R6 reference point. The functions to set up and manage such data paths are described in Section 7.7.2.2.2.2.

This section provides additional information about the encapsulation of user payload packets within Type 1 Data Paths. Detailed message formats and tag values are given in Stage 3. For routed transport architecture an IP-in-IP type of tunnel protocol has to be applied. GRE is taken as an example in this section to show the required functions of the tunnel protocol.

For transport of user payload packets over R1, the [1] specification amended by [2] supports various types of convergence sub-layers to address different types of service deployment scenarios. Different convergence sub-layers are provided for Ethernet as well as for IP providing particular classification and encapsulation functionalities.

Several different convergence sub-layers can coexist within the same ASN, e.g. IPv4-CS can coexist in the same ASN with IPv4oETH-CS. Handover of MS from an Ethernet based CS to a plain IP based CS within the same ASN or when moving from one ASN to another ASN is not supported.

7.11.1 IP Convergence Sub-layer

The IP convergence sub-layers are defined in [2] in Section 5.2.6. When one of the IP CS is employed, IP datagrams are carried directly in the payload of 802.16 PDUs. Classifiers for IP CS connections can make use of fields in the IP header as well as source and destination port numbers of transport protocol fields. Packet header suppression is an optional method operating with existing convergences sub-layers.

7.11.2 Services Provided over IP Convergence Sub-layer

7.11.2.1 IP Connectivity for a Single Host MS

A single IP address is assigned to the MS deploying separate CIDs for up- and downlink. Multiple CID assignments are possible to provide multiple service flows under the same IP address.

7.11.2.2 IP Connectivity for Multiple Hosts Behind the MS

This service is out of scope for Release 1.0.0

7.11.3 IP Convergence Sub-layer Transport Architecture

Figure 7-101 shows the generic protocol layering for the control plane as well as the data path applying IP-CS on R1, R6 (when exposed), R3 and R5. GRE is provided as example of an IP-in-IP tunnel protocol.

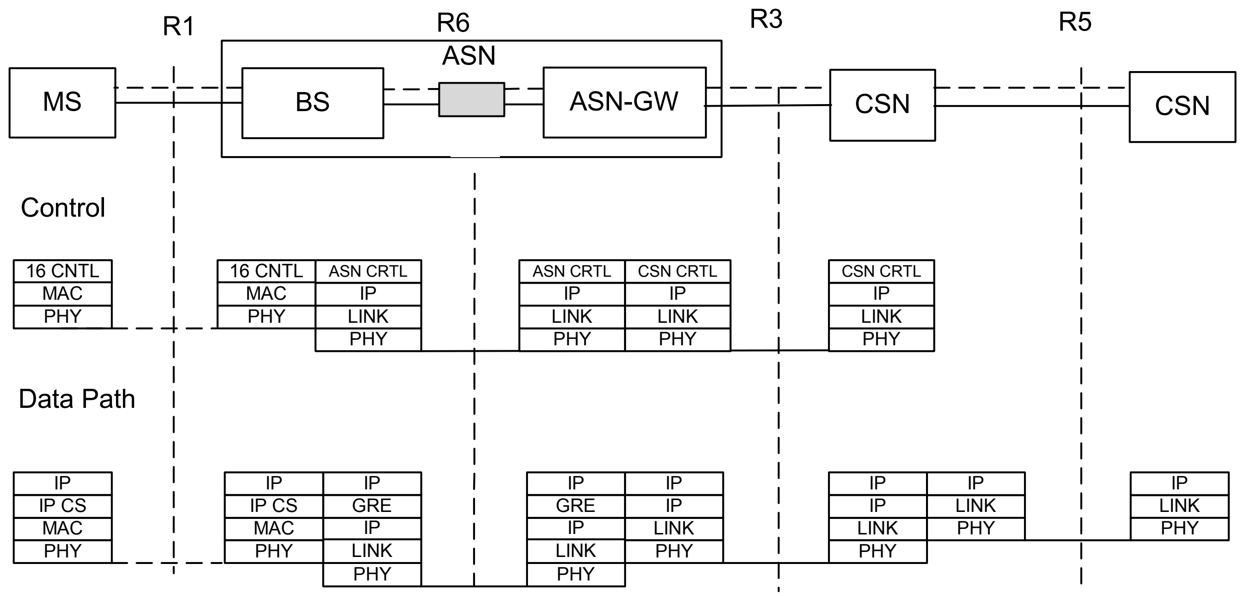


Figure 7-101 - Protocol Layer Architecture for IP-CS

7.11.4 IP Packet Forwarding Over the Air

In case of IP-CS the MS SHALL encapsulate IP datagrams from the IP host layer into 802.16 MAC frames for upstream over the R1 reference point. The BS (on ASN side) SHALL encapsulate IP datagrams received from the ASN-GW IP router via R6 into 802.16-MAC frames for downstream over R1. All IP datagrams are transferred over R1 according to the applied classifier for the particular CID.

7.11.5 Ethernet Convergence Sub-layer

The Ethernet convergence sub-layers are defined in [2] in Section 5.2.4. When one of the Ethernet CS is employed, IEEE802.3 frames carrying the IP datagrams are encapsulated in the payload of 802.16 PDUs. Classifiers for Ethernet CS connections can make use of fields in the 802.3 header as well as higher layer protocol fields (according to the specific Ethernet CS type). Packet header suppression (PHS) is an optional method operating with existing convergences sub-layers. PHS can serve to replace the entire 802.3 header and eventually even higher layer header fields with a one-byte PHS-Index. The BS MAY implement subnet-wide forwarding of subscriber broadcasts so as to complete LAN emulation functionality. This broadcast functionality MAY include filtering, filters MAY be implemented at the MS (using classifiers with the "Drop action" or with a filter above the MAC layer) so as to restrict inappropriate traffic (e.g. Printer announcements) from the uplink; or the BS MAY respond to ARP requests rather than propagating them.

7.11.6 Services Provided Over ETH CS

7.11.6.1 IP Connectivity for a Single Host MS

In this scenario, the MS implements a single "virtual LAN" endpoint that can be attached beneath a standard host IP stack on the client MS. Use of the 802.3/Ethernet CS (with optional PHS) provides various benefits, such as:

- Support for transport of downlink-direction unicast data packets that lack IP addresses (e.g. DHCPOFFER as described in [11]; Mobile IP signaling messages in scenarios described in [43] which carry destination IP address of 0.0.0.0)
- Seamless and reduced-latency support of client-based Mobile IP handovers: after an MS enters a new FA domain, the MAC-address-based classifiers associated with its active connections will still be valid (as they are independent of the care-of address) - so there is no need for the 3-way DSC handshake that is mandated by [1] to modify the classifiers.
- Ability to operate with a private Ipv4 address space (i.e. Even if multiple connectivity providers use the same private IP addresses, packets will be forwarded to the correct MSs).

- Support for multiple access routers and load-balancing: the access router at the headend (which might be located at the end of a L3 tunnel) MAY send ICMP-redirect to instruct the MS to communicate via a different L3 gateway.
- Independence of layer 2 data connectivity from IP endpoint configuration mechanisms: A fully functioning ASN can be deployed using static layer-2 configuration only. The ASN can then work easily with AAA-based IP parameter assignment or stateless autoconfiguration mechanisms (in addition to the more typical DHCP or Mobile IP – and need not know which is in use.
- Facilitation of bridging-based ASN architecture: Use of the 802.3/Ethernet CS enables the BS application to perform transparent bridging or ARP-based bridging (i.e. [6], which ensures all packets traverse the gateway for accounting purposes). A bridging-based ASN enables a simple mechanism for intra-ASN datapath updates via gratuitous broadcasts

7.11.6.2 IP Connectivity for Multiple Hosts Behind a MS

This topic is for further study and deferred beyond Release 1.0.0

7.11.6.3 WiMAX Access to DSL Infrastructure

This is typically a fixed/nomadic usage scenario, in which a user host (typically a PC or network equipment hosting IP based applications) behind the MS has an Ethernet connection to an IEEE 802.16 MS, which provides broadband access from a service provider with a DSL infrastructure. There is an Ethernet connection from the SS to the BS using the Ethernet CS. There is an Ethernet connection over the ASN from the BS to the BRAS (Broadband Remote Access Server). PPPoE is used on top of the mobile WiMAX access network to provide a user connection that is similar to the existing DSL deployment.

7.11.6.4 Ethernet Service to Enterprise Customer Locations

This is typically a fixed/nomadic usage scenario. An enterprise location has a MS with an Ethernet interface that could support one or many user hosts in the local network through a switch. There is an Ethernet connection from the SS to the BS using the Ethernet CS. An Ethernet connection from the ASN to the core network edge point could be provided over IP. The network service to the enterprise customer is an Ethernet service from the core network all the way to the enterprise MS. This could be an extension of a MetroEthernet connection based on IEEE 802.1Q VLANs to manage the service. The MS location could be a branch of a main network that benefits from being connected at the Ethernet layer. If the local network is controlled by the enterprise, the hosts can be assumed to be trusted to use proper QoS signaling such as IEEE 802.1Q VLAN tags or DSCP markings.

7.11.6.5 IEEE802.1Q VLAN Network Service

IEEE802.1Q support can be viewed in the following two ways:

- The VLAN ID and the priority bits are transported across the WiMAX link with no alteration (IEEE802.1Q VLAN transport). This assumes the MS part of the VLAN transport network architecture and the hosts behind the MS are trusted to use the correct VLAN Id and Priority.
- The VLAN ID and the Priority are translated or stacked or inserted/removed when transitioning the WiMAX link (IEEE802.1Q VLAN translation). This allows the network connected to the MS to have its own set of VLAN IDs and Priorities, which can be independent of the VLAN transport network architecture. The translation of these VLAN IDs and priorities will allow the CSN to switch relatives to its provisioned VLAN IDs. This also allows for networks connected to the MS that have no tagging capability to be able to be switch to the customer specific VLAN (in the case of a wholesaler model) in the core network.

IEEE802.1Q VLAN Network Service is deferred into Release 1.0.0.5.

7.11.7 ETH-CS Transport Architecture

Figure 7-102 shows the generic protocol layering for the control plane as well as the data path applying ETH-CS on R1, R6 (when exposed), R3 and R5. GRE is provided as example of an IP-in-IP tunnel protocol.

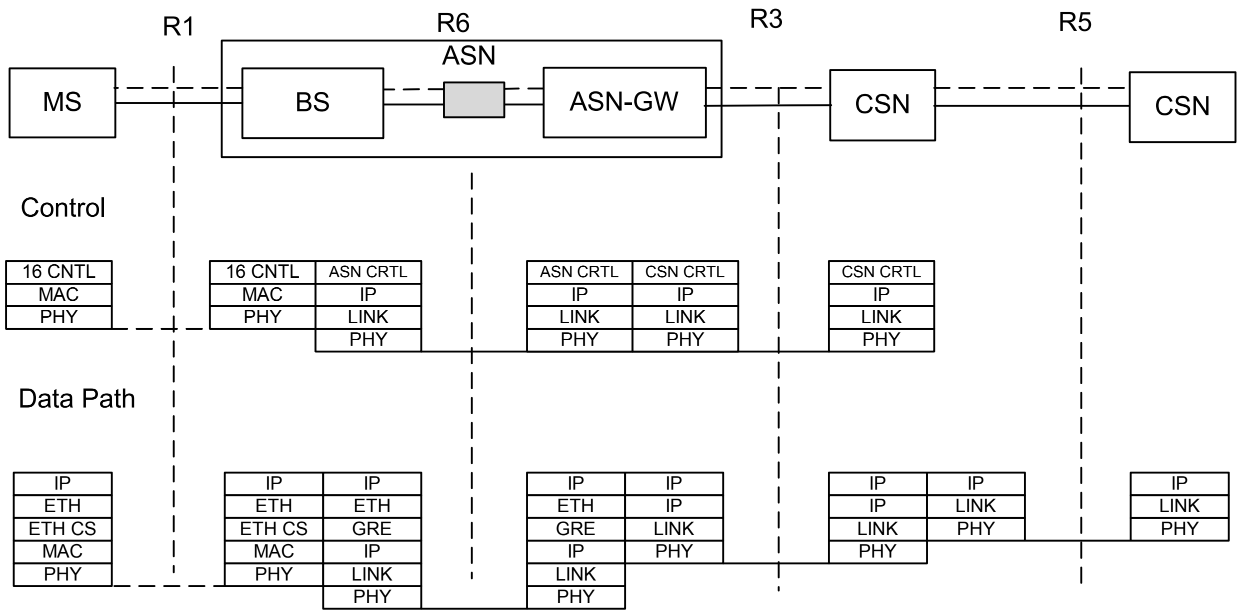


Figure 7-102 - Protocol Layer Architecture for ETH-CS

7.11.8 ETH CS Packet Transmission Format over R1

IEEE802.16 MAC frames are protected by a MAC layer FCS. The FCS trailer of Ethernet packets does not provide a higher level of protection and will be suppressed for the transmission over the air. This reduces the packet overhead by 4 bytes. The Ethernet FCS is re-generated at the receiving side out of the transmitted data and appended to the packet.

Ethernet frame format

DA	SA	Length/Type	Data	FCS

Transmission of Ethernet over R1

DA	SA	Length/Type	Data

IEEE 802.1Q frame format

DA	SA	0x8100	Tag Control Information	Length/Type	Data	FCS

Transmission of IEEE 802.1Q over R1

DA	SA	0x8100	Tag Control Information	Length/Type	Data

Figure 7-103 - FCS Suppression Over R1

7.11.9 Ethernet Packet Filtering Over the Air

To reserve resources over the R1 reference point, Ethernet broadcast packets are filtered. The filter MAY be implemented at the MS (using classifiers with the "Drop action" or with a filter above the MAC layer) so as to restrict inappropriate traffic (e.g. Printer announcements) from the uplink; or the ASN MAY respond to ARP requests rather than propagating them. Both Ingress Broadcast Filtering and Egress Broadcast Filtering SHALL have the ability of being enabled or disabled. A summary of the filter operation is described below. Details of operation are given in Stage 3.

7.11.9.1 Ingress Filter MS

The MS Ingress Filter is responsible for filtering and discarding unwanted packet from going over the air. Filtering can be enforced at the MAC or the IP layer. Packet from a host SHALL be discarded if that packet's source MAC address cannot be found in the current MS authenticated managed MAC list. The authenticated MAC list is composed from the authentication methods defined this document (DHCP Response MAC/IP). In the case of Address Resolution Protocol messages, the MS Ingress Filter SHALL permit all to pass to be solved by the BS. The Ingress Filter SHALL permit all DHCP messages to pass to the BS for further processing. Upon receiving any packet from the MS that is identified as an IP datagram, the Ingress Filter SHALL discard the datagram if the source IP address cannot be found in the current MS Authenticated MAC List.

7.11.9.2 Egress Proxy ARP/Filter

The ASN SHALL have the ability to enable or disable all ARP Ingress Proxy Agent and/or ARP Egress Proxy Agent functionality defined herein. The functionality of these agents is to manage broadcast traffic going over the R1 reference point. ARP Egress Proxy Agent SHALL unicast an ARP Response back to that trusted source on behalf of the MS and unicast the APR request to the MS, provided that the target MAC address matches an entry in the Authenticated MAC List. The ARP Egress Proxy Agent SHALL issue a gratuitous ARP for any new addition to the Authenticated MAC ID.

7.11.10 Tunneling within the ASN

7.11.10.1 IP-in-IP Tunnel Protocol GRE

If GRE is used as the tunneling mechanism between the ASN-GW and the BS (over R6) and between ASN-GW and ASN-GW (over R4), then the Tunneling Info Extension SHOULD be set to GRE. The value for the GRE Key is negotiated between the ASN-GW and the BS or between ASN-GW and ASN-GW. The GRE Payload Protocol Types are assigned according to [3] for IP and Transparent Ethernet Bridging.

The encapsulation format for GRE appears in Figure 7-104.

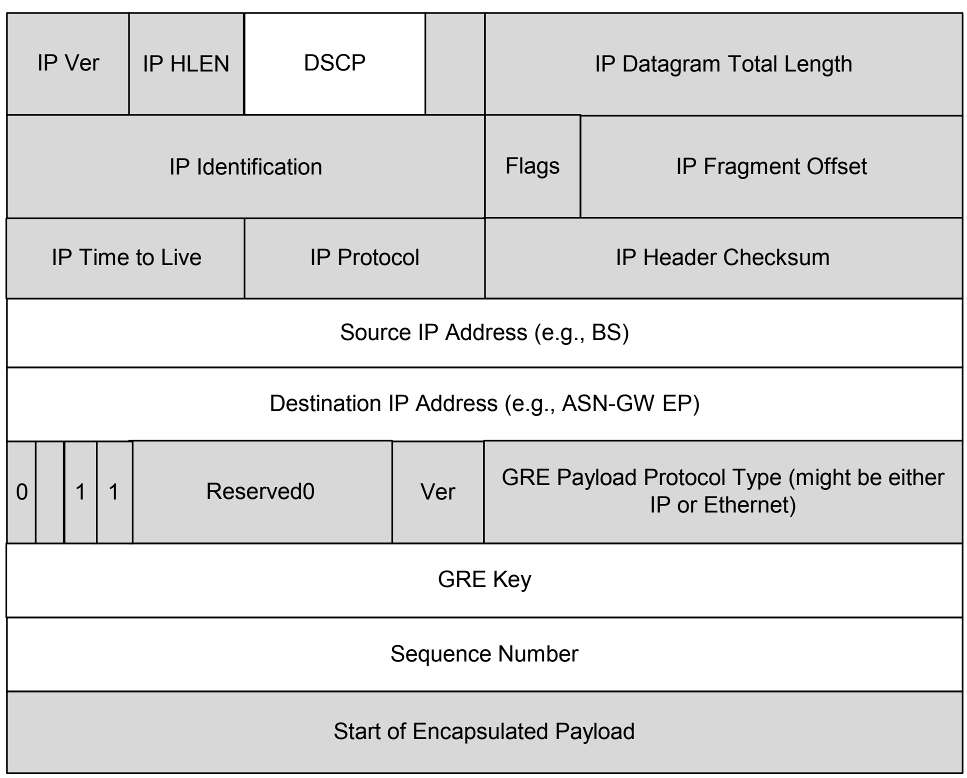


Figure 7-104 - GRE Encapsulation

- DSCP in the Encapsulation IP Header specifies the QoS Class. Note that it MAY differ from the DSCP in the Encapsulated Payload.
- Source and Destination IP Addresses specify the tunnel end points.
- The meaning of the GRE Key value is defined by the node that allocates the Key value.
- The Sequence Number might be used for synchronization of Data Delivery during HO.

Figure 7-105 shows an example of IP Data Path with GRE Encapsulation within the ASN.

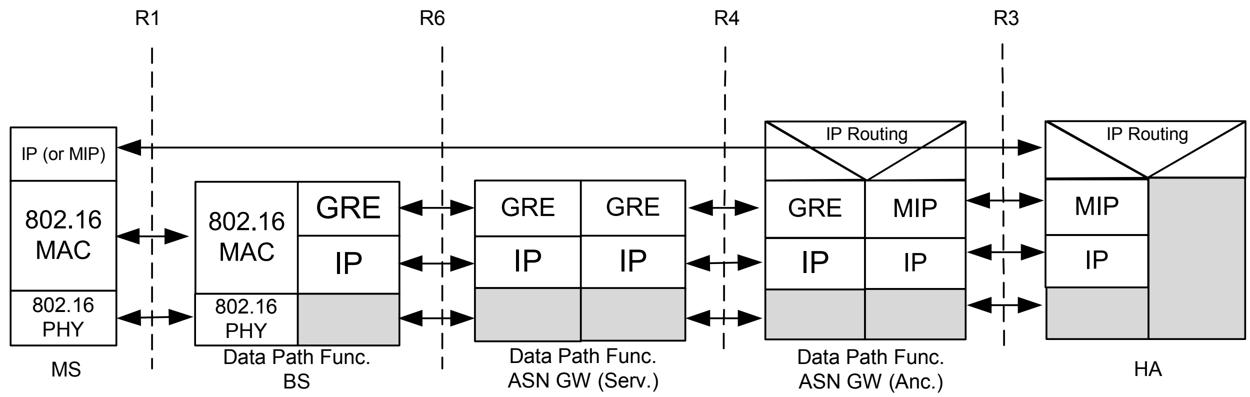


Figure 7-105 - GRE Encapsulation for IP CS

The same IP CS Data Path can be used either for Proxy MIP or for Client MIP.

The BS maps the IEEE 802.16 Connections (CID) on the R6 GRE Tunnels for both downstream and upstream traffic. There is 1 to 1 correspondence between the IEEE 802.16 Connections and the GRE Keys (in case per Service Flow granularity on R6/R4) or 1 to n correspondence (in case per MS granularity on R6/R4). The BS does not need to implement any IP routing functionality. This mechanism is applied either for unicast or for multicast traffic.

The ASN-GW terminates the R6 Tunnels from BS. Various encapsulation techniques (e.g. GRE, MPLS, etc.) might be used for R6 Tunnels and the granularity of the tunnel IDs might also vary (e.g. the Tunnel IDs might be assigned per Connection, per MS, per IP Realm, etc.). The R6 Data Path Function protocol supports encapsulation type and Tunnel ID granularity negotiations.

- In case of “per SF granularity” Anchored ASN-GW (Data Path Function) SHALL classifying the downstream traffic.
- In case of “per MS granularity” BS (Data Path Function) SHALL classifying the downstream traffic.

MS SHALL always classify the upstream traffic.

7.12 VoIP Services

While existing mechanisms specified in the QoS framework and accounting and charging framework could be used by the CSN operator to support VoIP, fulfillment of all quantitative requirements, regulatory requirements and requirements mentioned in Section 7.12 for VoIP are outside the scope of Release 1.0.0.

7.12.1 Emergency Service

Emergency Service is considered as a non-subscription based service, provided by the network operator (NSP) or third party IP service providers (ASP). This service does not require explicit authentication and authorization of the Caller. Decision on the access authentication for using emergency service and analysis of the security threats are FFS.

Figure 7-106 depicts the high-level view of the emergency service architecture.

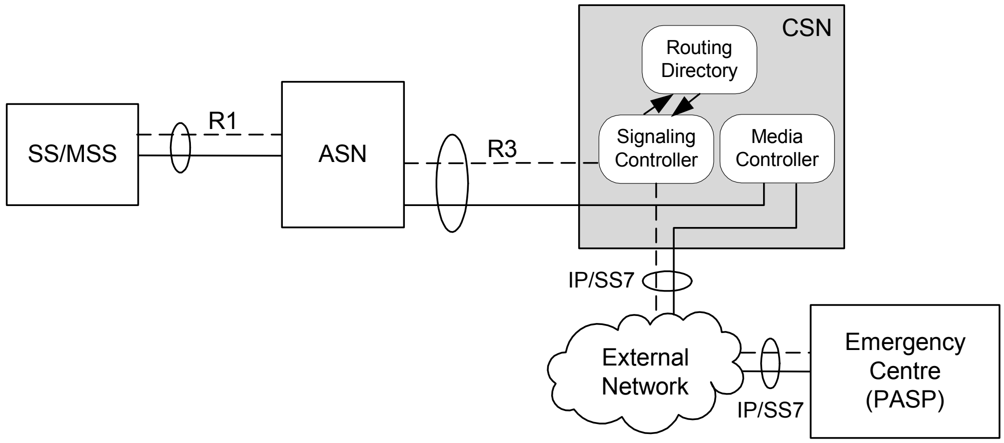


Figure 7-106 - High-Level View of Emergency Service Architecture

There are four basic steps involved for supporting emergency service. They are as follows:

a) *Detection of emergency request:* Detection of the emergency request MAY be done by the MS or by the network entities within CSN based on certain criteria outside the scope of Release 1.0.0.

b) *Location information:* Caller location plays a central role in routing emergency calls. The location information MAY be communicated from MS, BS, ASN entities, or by some other means. The exact procedure on communicating location information as required by emergency services regulatory requirements is outside of the scope of Release 1.0.0.

c) *Finding the location of nearest PSAP (Public Safety Answering Point):* For practical reasons, each PSAP generally handles only calls for certain geographic area. Also, for time sensitive request like emergency service, it is better to handle request locally. Upon contacting PSAP, it forwards emergency calls to the emergency control center for the purpose of dispatching police, fire and rescue services. The address of the PSAP is based on the Caller's location information. The support is provided by the CSN through a functional entity labelled as "Routing Directory." This step is assumed to be supported by CSN in Release 1.0.0.

d) *Routing call to PSAP:* Once the location of the Caller and the address of PSAP are identified, the request is routed to the PSAP. This step is also assumed to be supported by CSN in Release 1.0.0.

Prioritization of the access and network resources is typically required in order to support emergency service in a reliable manner. The selection of an appropriate QoS for prioritization required by emergency service is based on the QoS framework discussed in this document. While the CSN operator could use an existing QoS signaling method specified in the framework, explicit prioritization support for emergency service support is outside the scope of Release 1.0.0.

8. ASN Profile Introduction

A profile maps ASN functions into BS and ASN-GW so that protocols and messages over the exposed reference point are identified. The following text describes the three profiles of an ASN based on the current Stage 2 specifications. These three profiles show three possible implementations of the ASN and do not necessarily mandate a vendor to support all three. If a vendor chooses to implement any given profile, then that vendor's implementation SHALL conform to the chosen profile as specified in this text. The depiction of a function on either the ASN GW or the BS in the figures below does not imply that the function exists in all manifestations of this profile. Instead, it indicates that if the function existed in a manifestation it would reside on the entity shown. For example, PMIP Client MAY not always be present in all manifestations of Profile A. However, if it is used, it SHALL reside on the ASN GW. Note that the intent of an ASN profile is to describe intra-ASN reference points for intra-ASN interoperability within the context of that profile. An ASN of any profile SHALL be interoperable with an ASN of any other profile through the inter-ASN reference points R4. Thus, the inter-ASN interoperability through reference points R4 is independent of any particular ASN profile.

Identification of the ASN profiles was done for the specific goal of providing a bound framework for interoperability among entities inside an ASN. Specifically, interoperability in relation to the protocols, primitives and messages associated with the reference points R6 and R4 is addressed. In this section, R6 is normative only for the profiles where it is exposed.

8.1 Profile A

ASN functions are mapped into ASN-GW and BS as shown in Figure 8-1. Some of the key attributes of Profile A are:

- HO Control is in the ASN GW
- RRC is in ASN GW that allows RRM among multiple BSs
- ASN Anchored mobility among BSs SHALL be achieved by utilizing R6 and R4 physical connections.

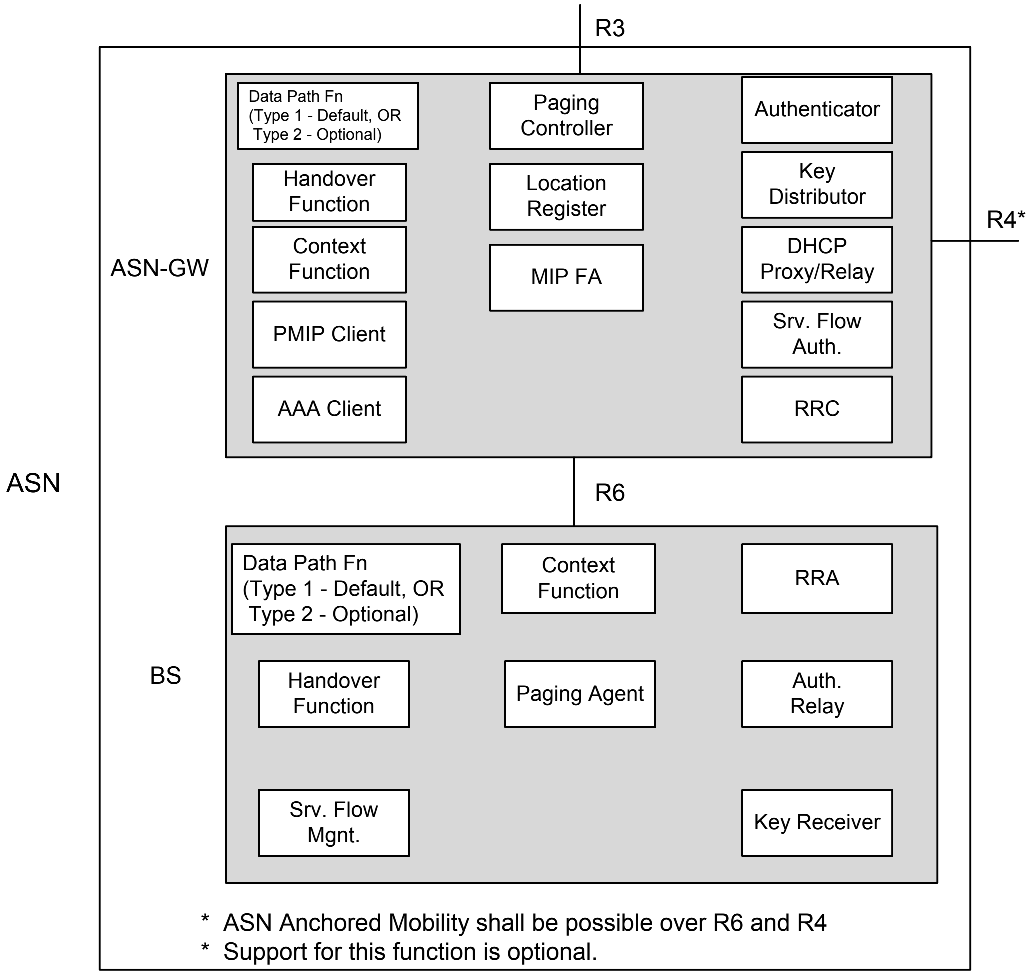


Figure 8-1 - Functional View of ASN Profile A

Table 8-1 illustrates the reference points over which intra-profile intra-ASN interoperability is achieved in accordance with Profile A.

Table 8-1 - Profile A Interoperability Reference Points

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
Security	Authenticator	ASN GW	Auth Relay Primitives	R6
	Auth Relay	BS	Auth Relay Primitives	R6
	Key Distributor	ASN GW	AK Transfer Primitives	R6
	Key Receiver	BS	AK Transfer Primitives	R6

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
IntraASN Mobility	Data Path Fn (Type 1 or 2)	ASN GW & BS	Data Path Control Primitives	R6
	Handover Fn	ASN GW & BS	HO Control Primitives	R6
	Context Server & Client	ASN GW & BS		R6
L3 Mobility	MIP FA	ASN GW	Client MIP	R6
	MIP AR	ASN-GW	Client MIP	R6
Radio Resource Management	RRC	ASN GW	RRM Primitives	R6
	RRA	BS	RRM Primitives	R6
Paging	Paging Agent	BS	Paging & Idle Mode Primitives	R6
	Paging Controller	ASN GW	Paging & Idle Mode Primitives	R6
QoS	SFA	ASN GW	BS	R6
	SFM	BS		

8.2 Profile B

Profile B ASNs are characterized by unexposed intra-ASN interfaces and hence intra-ASN interoperability is not specified. However, Profile B ASNs shall be capable of interoperating with other ASNs of any profile type via R3 and R4 reference points. Inter-ASN anchored mobility SHALL be possible via R4.

Mapping of ASN functions is not specified for Profile B ASNs and as such there can be several different realizations of a Profile B implementation. These include, for example, implementations where all the ASN functions are located within a single physical device such as an Integrated BS network entity (IBS), and ones where ASN functionality is distributed over multiple network nodes. Specification of entities, interfaces, and protocols within a Profile B ASN are vendor specific implementation and outside the scope of this document.

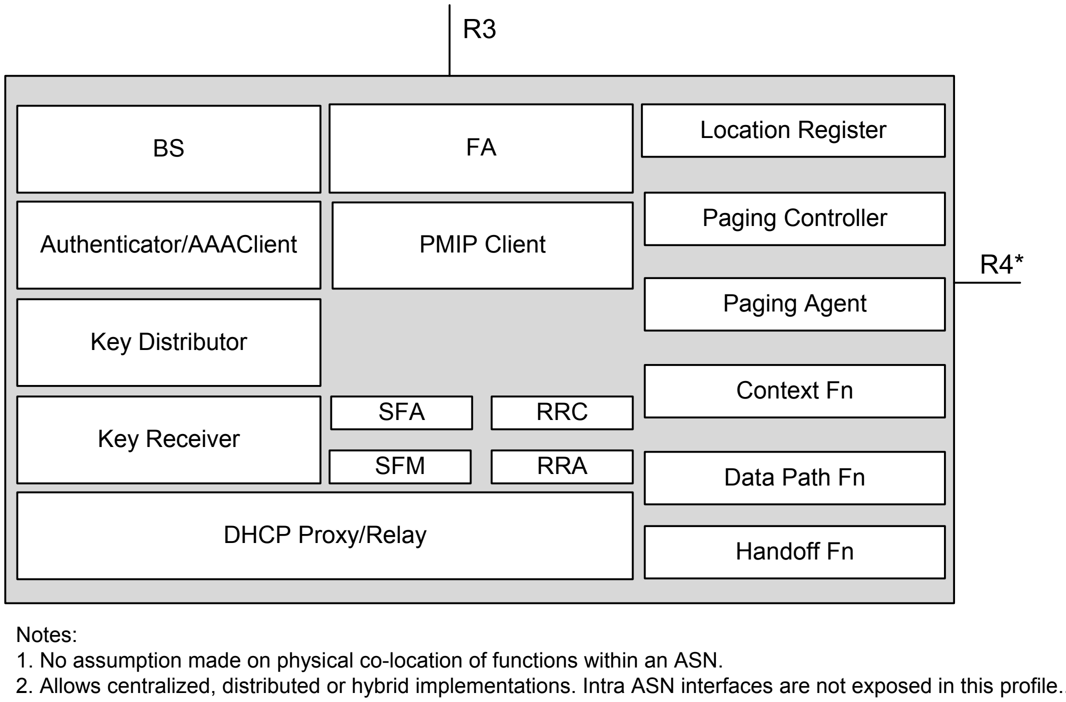


Figure 8-2 - Functional View of Profile B

8.3 Profile C

According to Profile C, ASN functions are mapped into ASN-GW and BS as shown in Figure 8-3. Key attributes of Profile C are:

- HO Control is in the Base Station.
- RRC is in the BS that would allow RRM within the BS. An "RRC Relay" is in the ASN GW, to relay the RRM messages sent from BS to BS via R6.
- As in Profile A, ASN Anchored mobility among BSs SHALL be achieved by utilizing R6 and R4 physical connections.

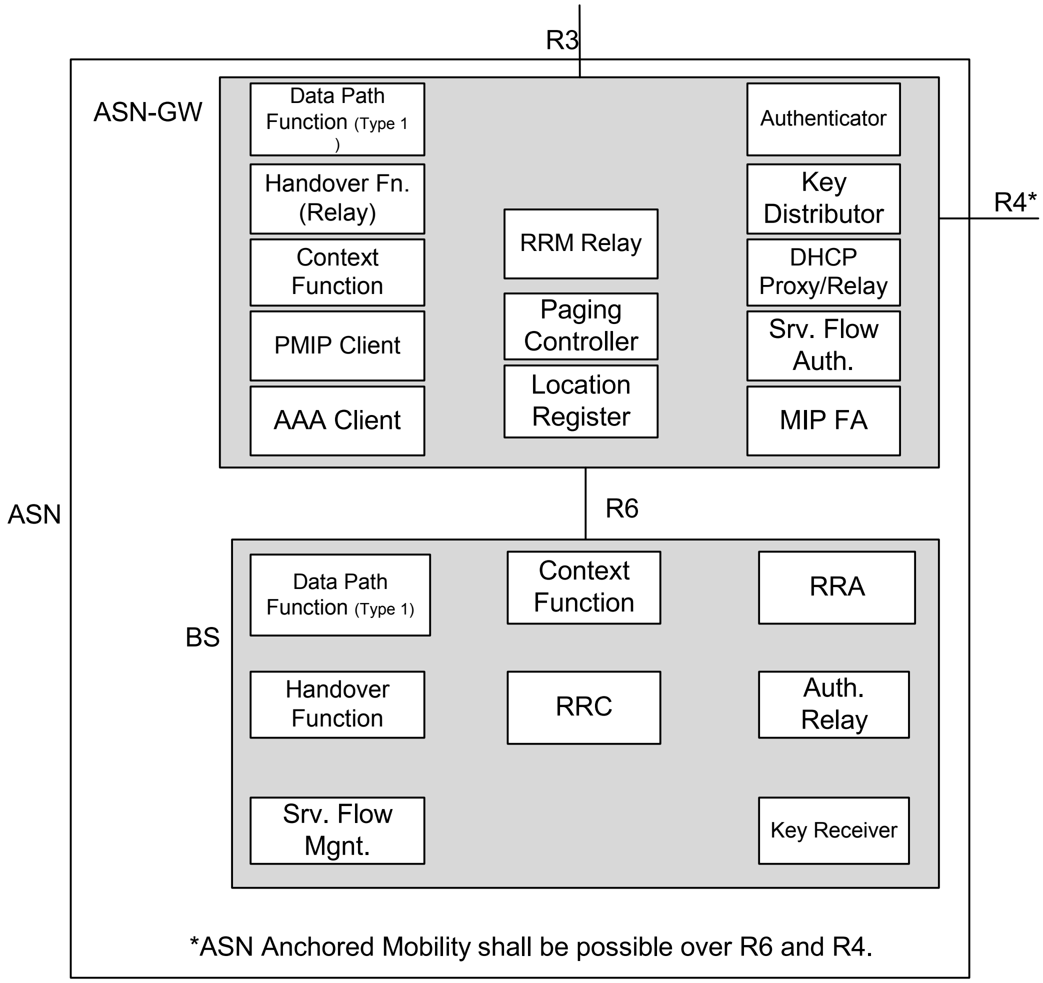


Figure 8-3 - Functional View of ASN Profile C

Table 8-2 illustrates the reference points over which intra-profile intra-ASN interoperability is achieved in accordance with Profile C.

Table 8-2 - Profile C Interoperability Reference Points

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
Security	Authenticator	ASN GW	Auth Relay Primitives	R6
	Auth Relay	BS	Auth Relay Primitives	R6
	Key Distributor	ASN GW	AK Transfer Primitives	R6
	Key Receiver	BS	AK Transfer Primitives	R6

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
IntraASN Mobility	Data Path Function (Type 1)	ASN GW & BS	Data Path Control Primitives	R6
	Handover Fn	ASN GW & BS	HO Control Primitives	R6
	Context Server & Client	ASN GW & BS		R6
L3 Mobility	MIP FA	ASN GW	Client MIP	R6
	MIP AR	ASN-GW	Client MIP	R6
Radio Resource Management	RRC	BS	RRM Primitives	R6
	RRA	BS	None (BS internal)	-
	RRC Relay	ASN GW	RRM Primitives	R6
Paging	Paging Agent	BS	Paging & Idle Mode Primitives	R6
	Paging Controller	ASN GW	Paging & Idle Mode Primitives	R6
QoS	SFA	ASN GW	QoS Primitives	R6
	SFM	BS		

Attachment 4-5

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[Part 3 – Informative Annex]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 3 – Informative Annex]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

A. WiMAX NWG Reference Architecture Deployment Scenarios

Note: See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

This annex illustrates the motivations behind functional partitioning in WiMAX NWG reference architecture by depicting.

- Business relationships between WiMAX subscriber, NAP and NSPs
- Decomposition of NAP into physical elements and sharing of NAP by multiple NSPs
- A few end-to-end WiMAX deployment scenarios by NAPs and NSPs.

A.1 Business Relationships Between WiMAX Subscriber, NAP, and NSPs

Figure A-1 illustrates the contractual interrelationships between WiMAX subscriber, NAP, and NSPs.

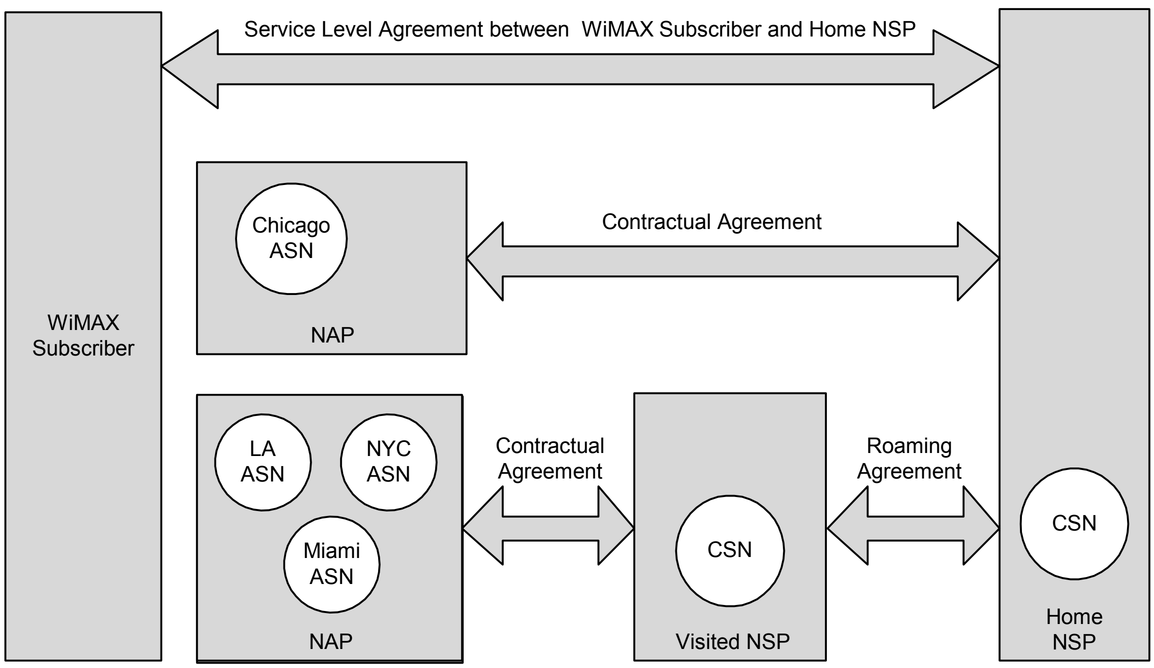


Figure A-1 - Business Relationship Between WiMAX Subscriber, NAP, and NSPs

As Figure A-1 illustrates, there are three basic types of business agreements between various business entities in WiMAX network:

a. **Service Level Agreement between WiMAX Subscriber and Home NSP.** This agreement allows the WiMAX subscriber to have access to a suite of WiMAX services and enable accurately billing for these services by the Home NSP.

b. **Contractual Agreement between NSP and NAP.** This agreement authorizes an NSP to use a given NAP's coverage area (or a part of it).

c. **Roaming Agreement between NSPs.** This agreement establishes roaming agreements between NSPs.

A.2 NAP Decomposition and NAP Sharing

Figure A-2 illustrates how a NAP may be decomposed in a given deployment.

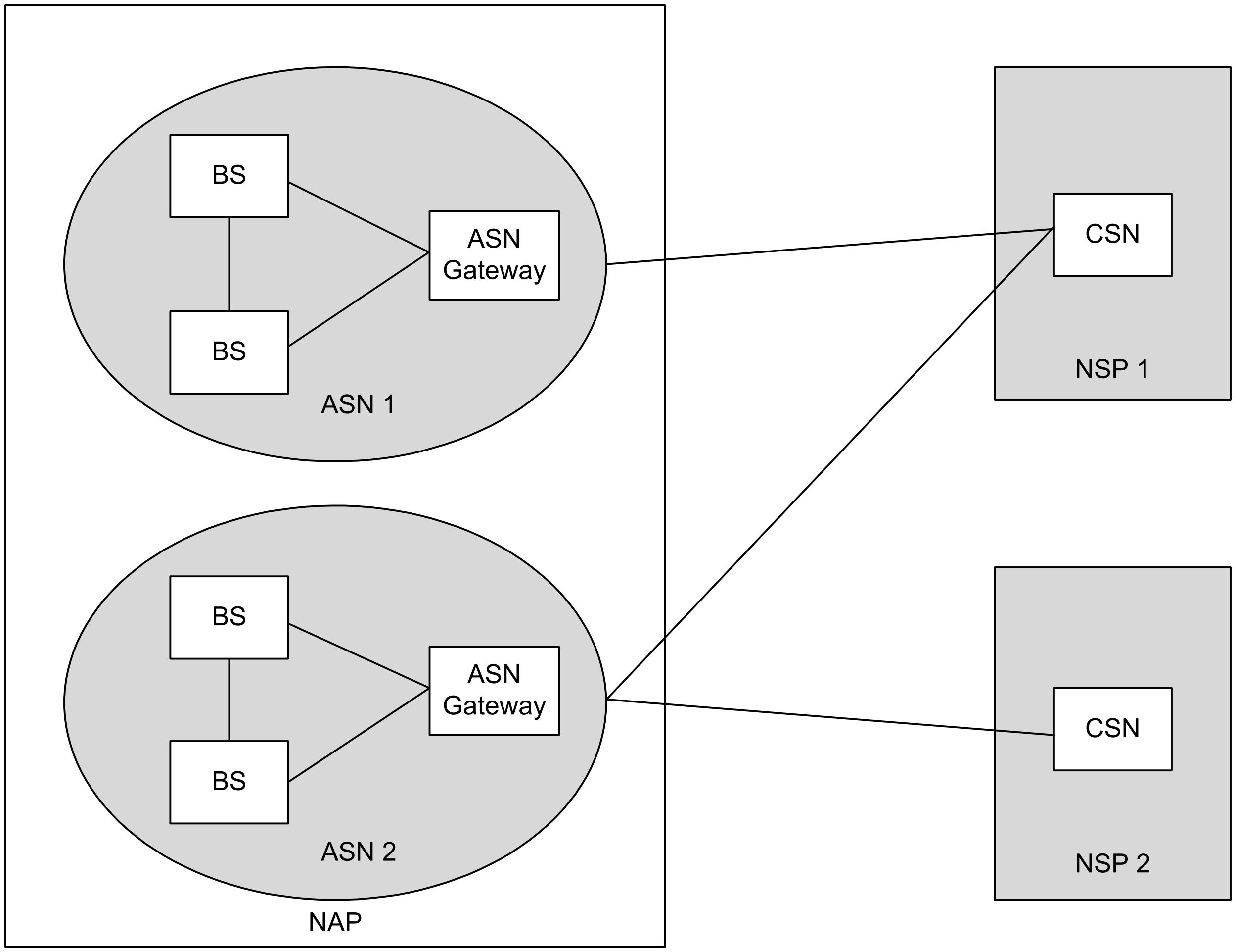


Figure A-2 - Decomposition and NAP Sharing by Multiple NSPs

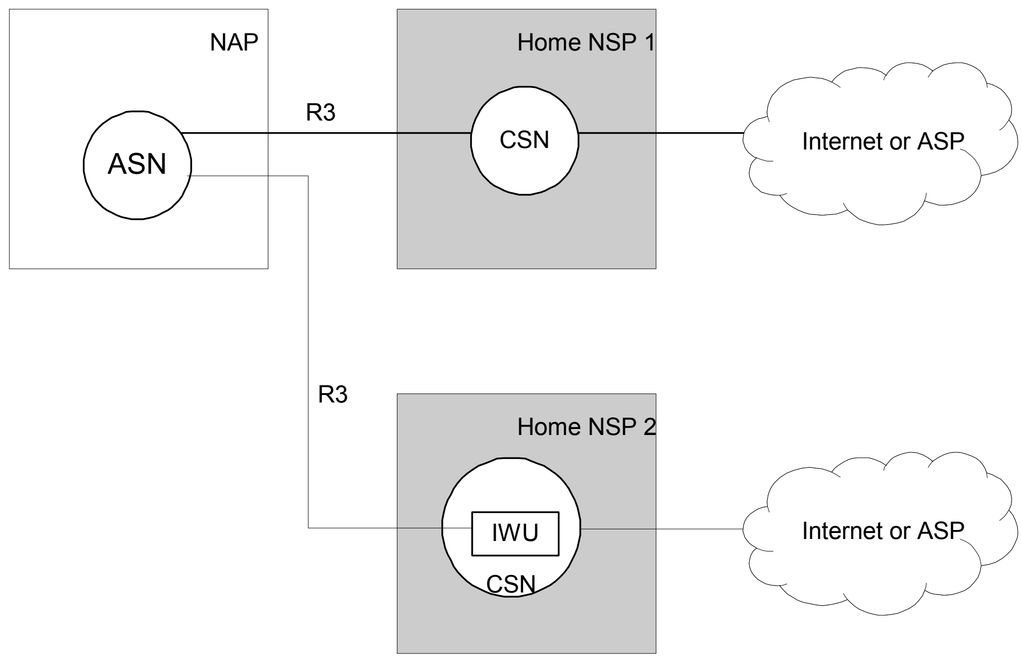
Following salient features of NAP decomposition and NAP sharing are worth noting:

- A NAP may deploy one or more ASNs in a single or diverse geographic area. (NOTE— An NSP may use multiple NAPs).
- An ASN in profiles A& C comprises Base Stations (BS) (or BS clusters) and ASN Gateway(s). In profile B, ASN-GW may not be included.
- An ASN Gateway provides connectivity to one or more CSNs over a WiMAX NWG defined interface. Such CSNs may belong to same or different types of NSPs. For example, , NSP1 may be a WiMAX Greenfield NSP whereas NSP 2 may be an incumbent 3G operator (e.g., CDMA operator) that is also an NSP (i.e., providing WiMAX services).

A.3 Deployment Scenarios

This section depicts seven deployment scenarios that illustrate interrelationships between NAP, NSP, ASN, and CSN. Following deployment scenarios are depicted in following subsection:

A.3.1 NAP Sharing by Multiple NSPs



H-NSP1 and HNSP2 may be different types of NSPs. For example, in the above figure, H-NSP1 may be a Greenfield WiMAX operator whereas H-NSP2 may be an incumbent 3GPP2 operator.

Figure A-3 - NAP Sharing by Multiple NSPs

A.3.2 Single NSP Providing Access Through Multiple NAPs

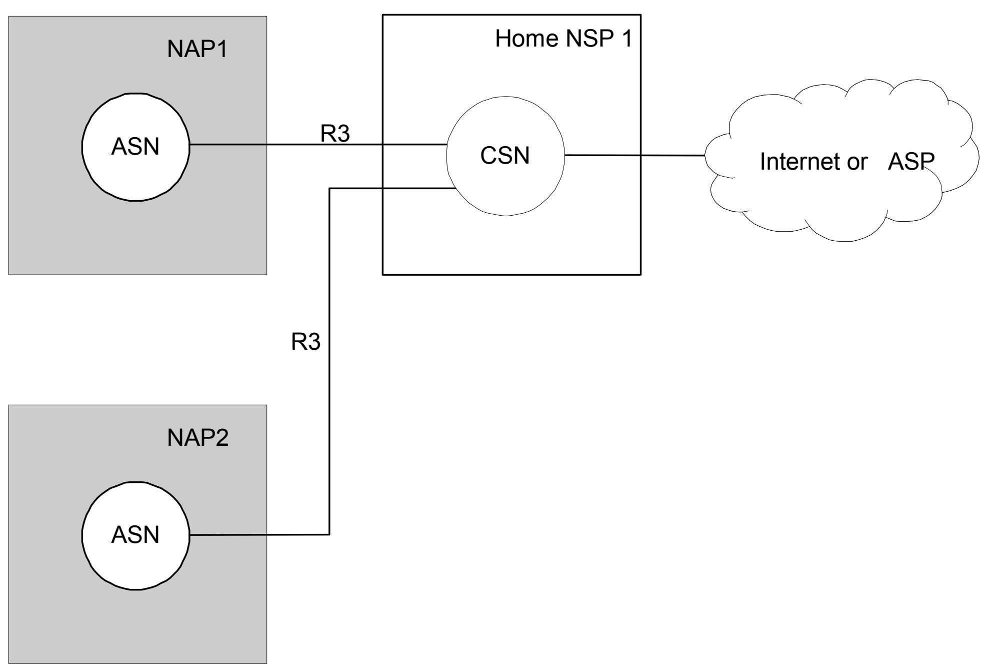


Figure A-4 - Single NSP Providing Access Through Multiple NAPs

A.3.3 Greenfield WiMAX NAP+NSP

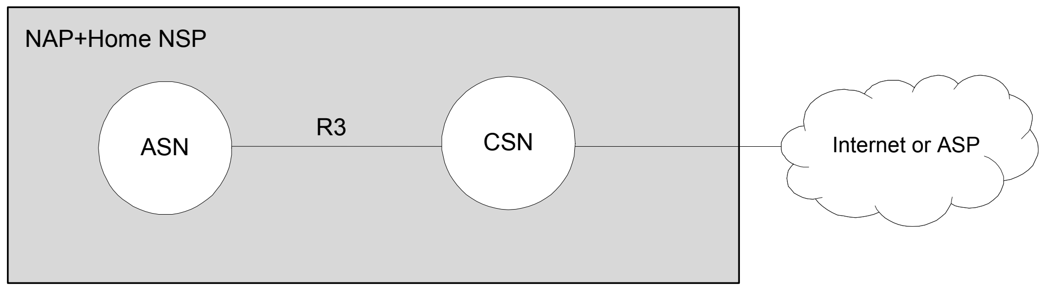


Figure A-5 - Greenfield WiMAX NAP + NSP

A.3.4 Greenfield WiMAX NAP+NSP with NAP Sharing

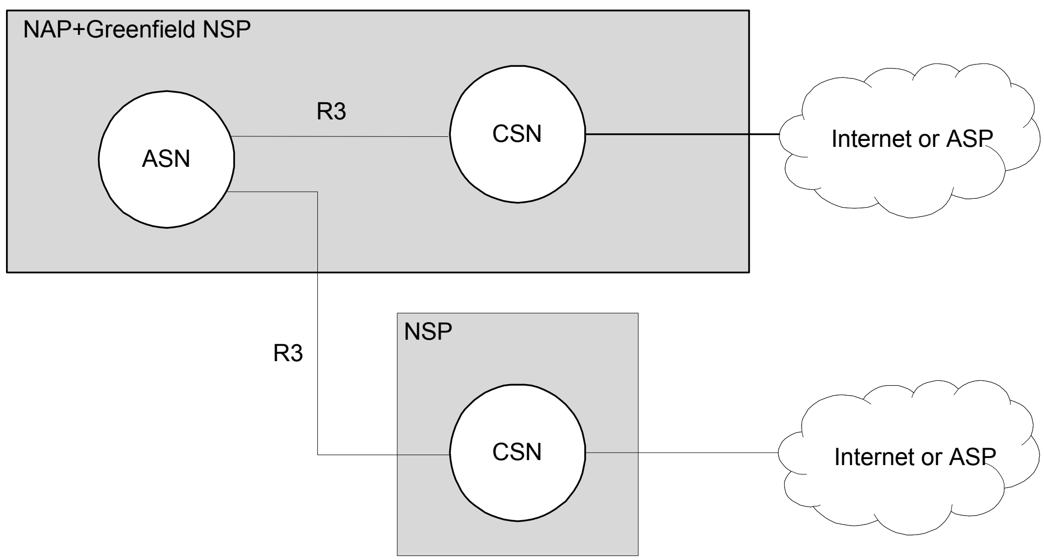


Figure A-6 - Greenfield WiMAX NAP+NSP with NAP Sharing

A.3.5 Greenfield WiMAX NAP+NSP Providing Roaming

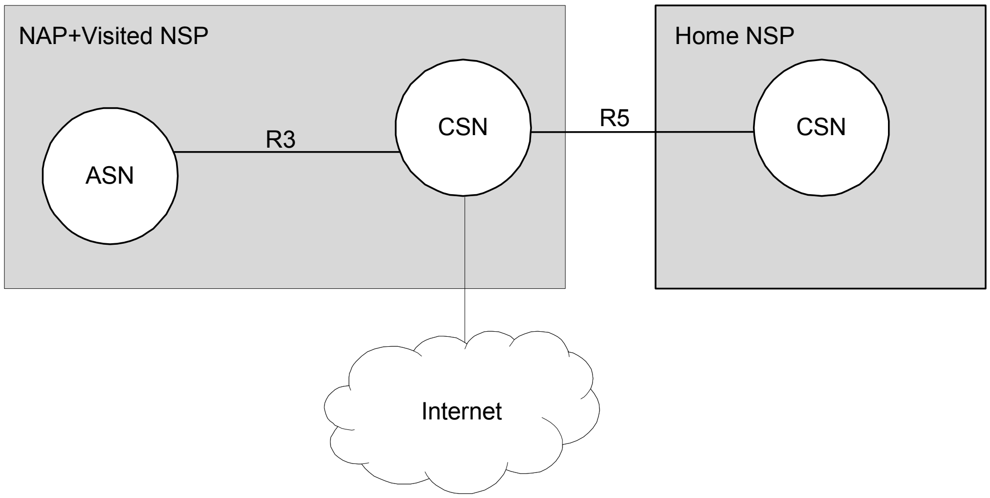


Figure A-7 - Greenfield WiMAX NAP+NSP Providing Roaming

A.3.6 Visited NSP Providing WiMAX Services

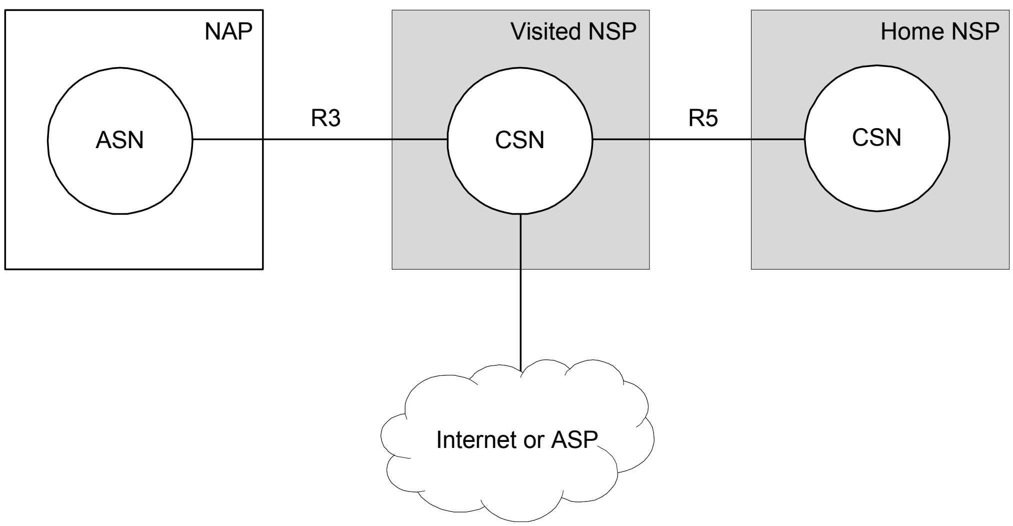


Figure A-8 - Visited NSP Providing WiMAX Services

A.3.7 Home NSP Providing WiMAX Services

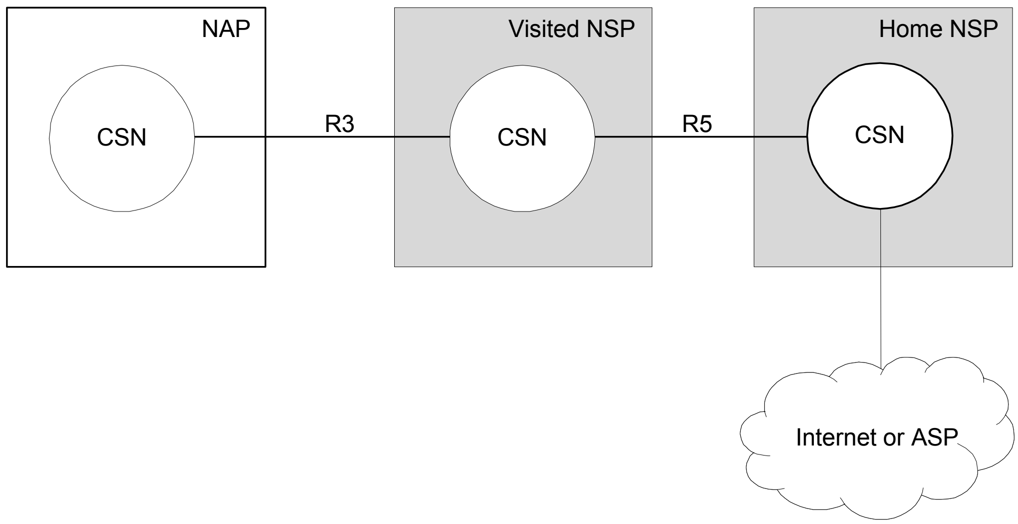


Figure A-9 - Home NSP Providing WiMAX Services

B. MS Movement with FA change, no PC change

If PMIP is used for a given mobile, when the mobile performs a location update procedure, the foreign agent that receives data for the mobile may be migrated using PMIP without having the mobile itself send any MIP registration request. Note that migration of the FA is optional. When the foreign agent is migrated to a new FA, it may be necessary to notify a Data Path Function associated with the new FA to monitor for data arriving for the mobile in idle mode. The Data Path Function can be provided with the identity of the Anchor PC, so that when data arrives for the mobile in idle mode, the Data Path function can trigger the Anchor PC to initiate paging for the mobile in the appropriate paging group.

The following figure illustrates the case of migration of the FA by triggering PMIP procedures when the Anchor PC remains the same (i.e. the mobile's context information is not relocated to a new PC but remains at the same Anchor PC where it was prior to the location update). The following steps describe the steps shown in the illustration.

a. Mobile sends a RNG_REQ to a serving base station to perform location update.

b. The serving BS sends a LU Req to its Relaying PC, which contacts the Anchor PC based on the PC_ID provided by the mobile. (Note that in some cases the Anchor PC may be the same as the Relaying PC associated with the Serving BS). It also asks for the mobile's context information, so as to determine the identity of the KDF/Authenticator from where the AK for the mobile can be obtained.

c. The Anchor PC acknowledges the location update using LU_Rsp and provides the mobile's context information to the Relaying PC, which provides it to the BS. However, in this case the Anchor PC retains the mobile's context (i.e. remains the anchor PC), and the mobile will be provided with the PC_ID of the same Anchor PC while confirming the location update.

d. In order to verify the HMAC/CMAC-tuple on the RNG_REQ, the S-BS' associated Key Receiver fetches the AK from the KDF associated with the authenticator where the mobile had last authenticated, using the KDF/Authenticator ID provided in the mobile context information.

e. LU_Confirm is sent from the S-BS (through the Relaying PC) to the Anchor PC to confirm the validation of the RNG_REQ.

f. The appropriate functional entity determines that the Data Path Function associated with the mobile's new location (shown as "Data Path Fn-New") is different from the mobile's previous Data Path Function. The logic for making this determination is unspecified and may be dependent on the physical configuration.

g. The appropriate functional entity (e.g. Anchor PC) sends a message called "Data Path Monitor Notification" to the Data Path Fn-New indicating that if new data arrives for this mobile in idle mode, the Data Path Function should contact the Anchor PC to initiate paging for the mobile.

h. The appropriate functional entity determines that the FA associated with the mobile's new location (shown as "FA-new") should be different from the mobile's previous anchor FA. The logic for making this determination is unspecified and may be dependent on the physical configuration. The PMIP client entity is triggered to initiate a Proxy MIP registration request.

i. The Proxy MIP registration procedure is executed to switch the R3 tunnel from the HA to point to the new FA.

j. An RNG_RSP message is sent to the mobile confirming the location update and providing the PC_ID of the Anchor-PC. Note that this step may occur any time after the RNG_REQ is validated by the SBS.

Note that in the above, the exact timing of steps f through g, and h through I, may be interchanged depending on physical configuration.

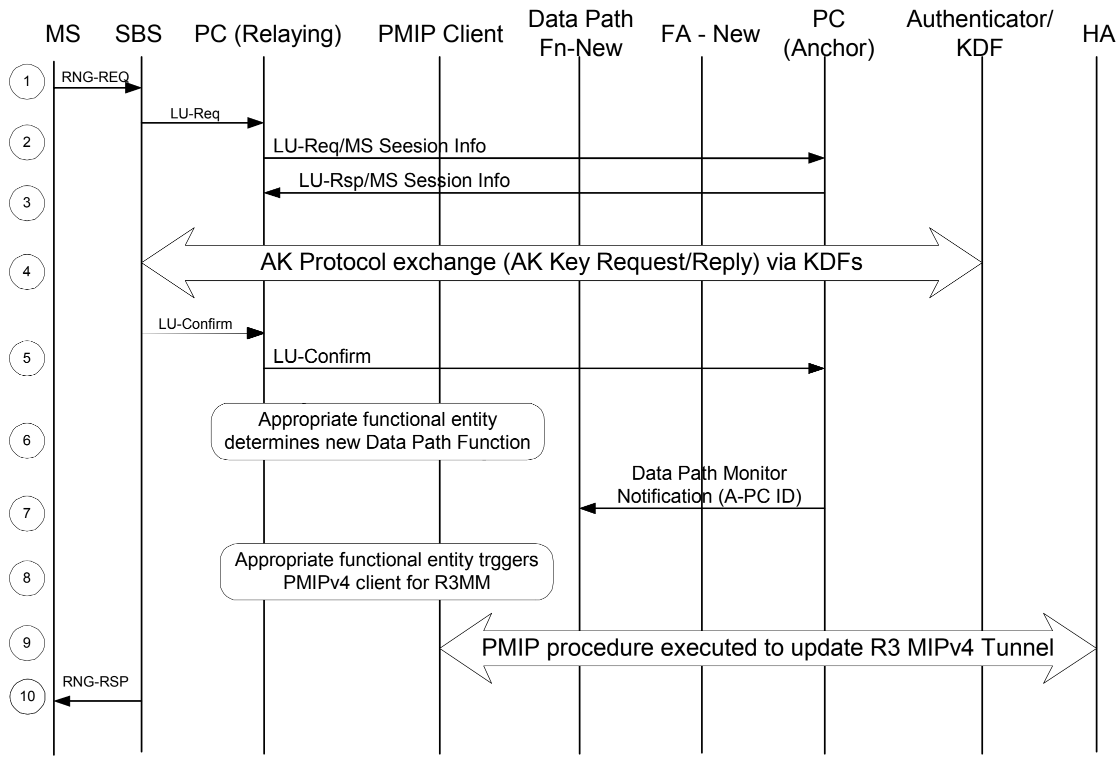


Figure B-1

The following figure illustrates the case of migration of the FA by triggering PMIP when the mobile context is relocated to a new PC from the Anchor PC prior to the location update. Note that relocation of the mobile context to a new PC is optional. If this option is exercised, it results in the new PC taking on the role of the Anchor PC for that mobile. In the following illustration, this occurs along with an FA migration using PMIP.

a. Mobile sends a RNG_REQ to a serving base station to perform location update.

b. The serving BS sends a LU Req to its Relaying PC, which contacts the (old) Anchor PC based on the PC_ID provided by the mobile (assuming here that the Relaying PC is different from the (old) Anchor PC). It also asks for the mobile's context information, so as to determine the identity of the KDF/Authenticator from where the AK for the mobile can be obtained.

c. The (old) Anchor PC acknowledges the location update using LU_Rsp and provides the mobile's context information to the Relaying PC, which provides it to the BS. In this case, the Relaying PC will become the new Anchor PC for this mobile, and the mobile will be given a PC_ID corresponding to the new Anchor PC when confirming the location update.

d. In order to verify the HMAC/CMAC-tuple on the RNG_REQ, the S-BS' associated Key Receiver fetches the AK from the KDF associated with the authenticator where the mobile had last authenticated, using the KDF/Authenticator ID provided in the mobile context information.LU_

e. Confirm is sent from the Relaying PC (which is now the new Anchor PC for that mobile) to the (old) Anchor PC. This confirms the validation of the RNG_REQ and the relocation of the Anchor PC, and the old Anchor PC can now delete the mobile's information from its LR.

f. The appropriate functional entity determines that the Data Path Function associated with the mobile's new location (shown as "Data Path Fn-New") is different from the mobile's previous Data Path Function. The logic for making this determination is unspecified and may be dependent on the physical configuration.

g. The appropriate functional entity (e.g. new Anchor PC) sends a message called "Data Path Monitor Notification" to the Data Path Fn-New indicating that if new data arrives for this mobile in idle mode, the Data Path Function should contact the new Anchor PC to initiate paging for the mobile.

h. The appropriate functional entity determines that the FA associated with the mobile's new location (shown as "FA-new") should be different from the mobile's previous anchor FA. The logic for making this determination is unspecified and may be dependent on the physical configuration. The PMIP client entity is triggered to initiate a Proxy MIP registration request.

i. The Proxy MIP registration procedure is executed to switch the R3 tunnel from the HA to point to the new FA.

j. An RNG_RSP message is sent to the mobile confirming the location update and providing the PC_ID of the new Anchor-PC. Note that this message may be sent any time after the RNG_REQ has been validated.

Note that in the above, the exact timing of steps f through g, and h through I, may be interchanged depending on physical configuration.

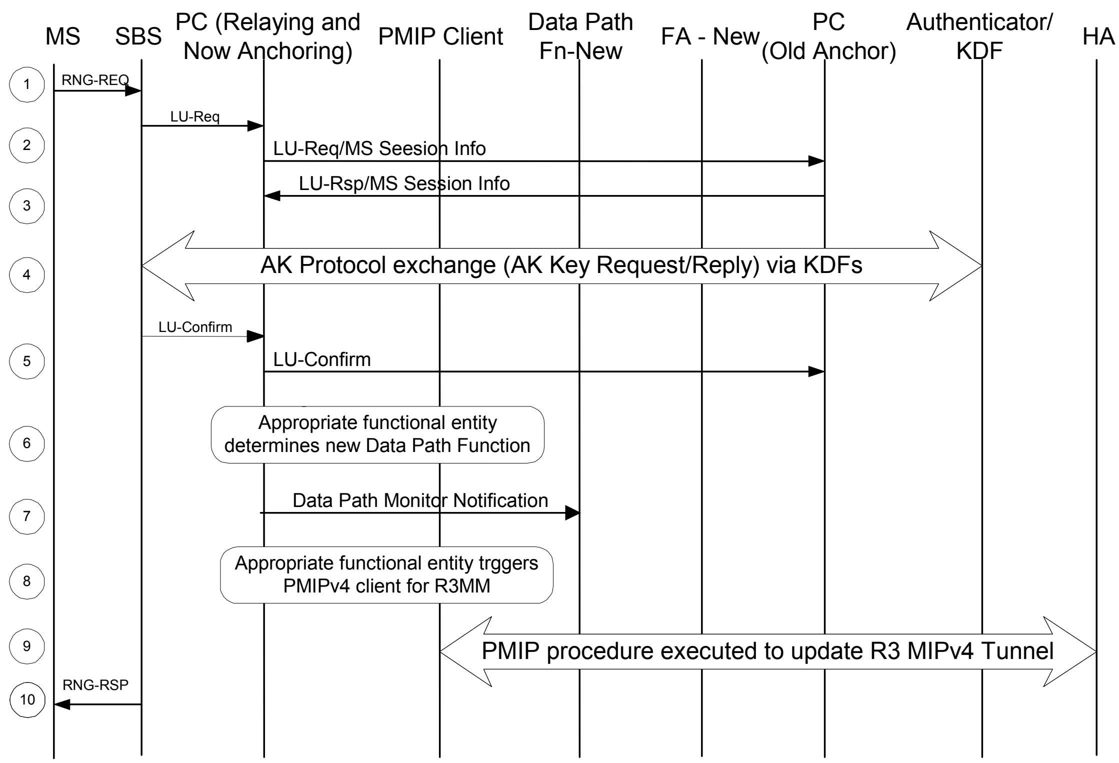


Figure B-2

C. ASN-GW Selection Protocol

This document covers two cases:

- Initial ASN-GW selection for Base Station and ASN-GW communications
- Per Session ASN-GW selection

C.1 Initial ASN-GW Selection by Base Station

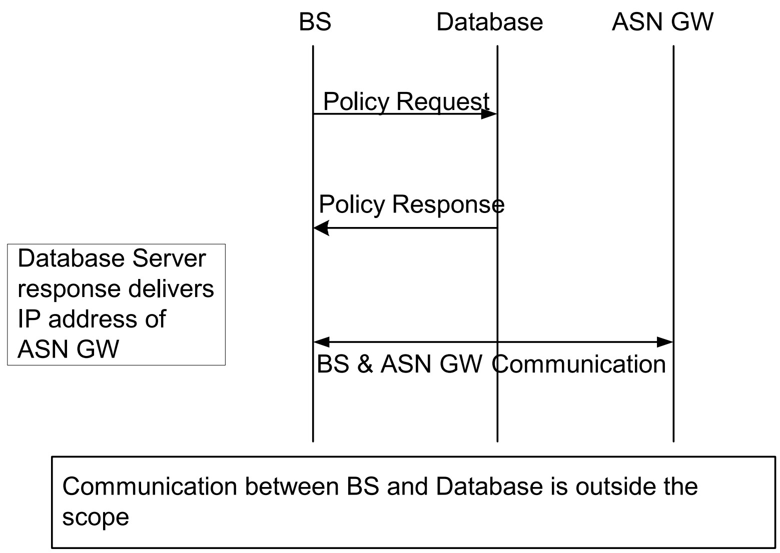


Figure C-1 - Initial ASN-GW Selection by Base Station

On Base Station startup or initial configuration Base Station contacts DB to get information about serving ASN-GW. The response includes the ASN-GW IP address.

The triggers for sending the Policy Request may include but are not restricted to the following:

- Initial Base Station startup
- Base Station reload

C.2 Per Session Selection of Physical Entities of Logical ASN-GW

It may not be scalable to contact policy server/database for each and every session. Base station always contacts known ASN-GW which may be determined by the previous procedure. Once the data path registration request is received by ASNGW1, it may forward to ASN-GW2. The data path registration response is returned by ASN-GW1 (or ASN-GW2) and will include the ASN-GW IP address for the specific session. It may also return IP addresses of different physical entities of the logical ASN-GW if they exists. The ASN-GW IP address may be the same as the initial ASN-GW address or different one. The actual algorithm of determining the specific ASN-GW address returned in the response is out of scope of this document.

Multiple IP addresses of different functional entities of an ASN-GW can also be delivered to the Base Station.

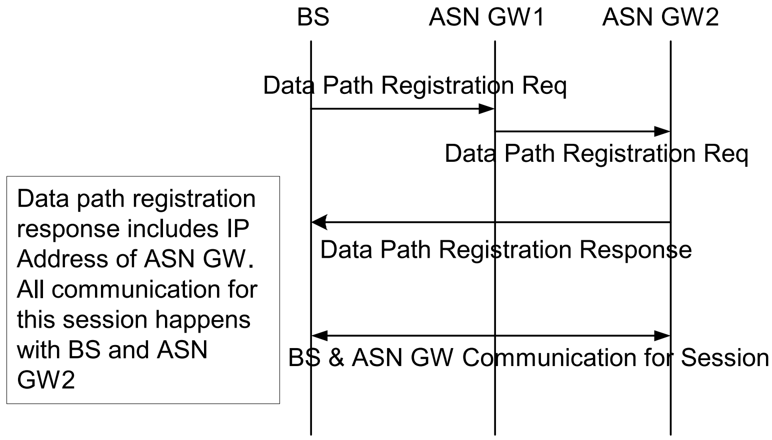


Figure C-2 - Per Session ASN-GW Selection

One example of the selection procedure is shown above. The Data Path Registration Request is sent to the initial ASN-GW, ASN-GW1 that the BS has initial communication with. This request may be forwarded to another ASN-GW2. ASN-GW2 will reply back with Data Path registration response and all communication for the session after this point will happen between BS and ASN-GW2.

C.2.1 Security Considerations

It is assumed that the Security Association between the Base Stations and ASN Gateways are pre-provisioned (e.g., there could be pre-established IPsec tunnels between each BS and ASN-GW). Thus the security context is not part of the ASN-GW Selection.

D. 'RRM': Spare Capacity Report per QoS Profiles

D.1 Introduction to Type 1 and Type 2 Spare Capacity Report

This annex describes Spare Capacity report per-BS, per QoS Profile and per Physical Service Level (PSL), Type 1 and Type 2.

Spare capacity report Type 1 and 2 are indexed by QoS profile ID and PHY service level, see details below. This type of Spare capacity report contains "Spare Capacity Indicator" (SCI) values, indicating the number of MS of the given type that may be added to the BS without degradation. It is calculated by the BS itself, using vendor proprietary algorithm, on the base of detailed knowledge of scheduling algorithm and real time load situation.

- Type 1 is the report for several combinations of DL and UL PSL values within a predefined two-dimensional range
- Type 2 is for exactly one pair of DL and UL PSL values.

The reporting format for spare capacity reports of **Type 1** and **Type 2** is specified in Section 9.10.2.

Type 1 shall not be supported in Release-1 and is for further releases.

Type 2 shall be used in a modified form as part of the Handover Preparation phase, as decided in the "Motion on RRM": "Type-2 (Spare Capacity report for a single QoS Profile and a single PHY service level PSL) for a specific MS during **HO Pre-Notification response**, and QoS Profile and PSL should be in the HO Pre-Notification request". The required modification is:

- It shall be embedded in the HO Pre-Notification request and response messages, i.e. these are no longer RRM primitives; and
- The MS Identity must be added: The report is no longer for an anonymous, potential MS but for a specific MS with already known QoS Profile and PSL value.

Since this Type 2 report will be part of a HO Primitives, rather than RRM primitive, it does not belong to section 7.10 (RRM) but should be considered for section 7.x "Intra-ASN Mobility".

D.1.1 Format of Spare Capacity Records, Type 1 and 2

A spare capacity record is used to carry information on many potential options of BS-MS communication rates. It may be exchanged in one of two formats – Type 1 and Type 2 - as specified in Tables below.

Table D-1 describes aggregate spare capacity report from RRA to RRC:

Table D-1 - Spare Capacity Report, Type 1

QoS profile descriptor	SCI = Spare capacity indicator for DL PSL = 1 UL PSL = 1	SCI = Spare capacity indicator for DL PSL = 1 UL PSL = 2	…	SCI = Spare capacity indicator for DL PSL = N UL PSL = N
4 bytes	2 bytes	2 bytes	…	2 bytes

Value SCI = 0 means "no information available".

Value SCI > 0 means that the BS is able to accommodate (SCI – 32) MS with QoS requirements specified by QoS profile descriptor and specific DL/UL PSL.

The result belongs to the range [-31 .., 65504]. Value SCI < 32 means that the BS suffers from degradation, which will be relaxed if (32 – SCI) MS with corresponding PSL values leave the BS.

Table D-2 describes an optional alternative format of spare capacity report from BS. This format shall be used when RRC queries a specific BS on its ability to accommodate a new service flow characterized by a QoS profile descriptor. For such cases, the BS may decide report the spare capacity for that QoS profile, for a specific set of DL PSL and UL PSL values. Alternatively, the BS may report the spare capacity for all sets of DL PSL and UL PSL values using Type 1 report format.

Table D-2 - Spare Capacity Report, Type 2

QoS profile descriptor	DL PSL	UL PSL	SCI = Spare Capacity Indicator
4 bytes	1 byte	1 byte	2 bytes

Value SCI = 0 means “no information available”.

Value SCI > 0 means that the BS is able to accommodate (SCI – 32) MS with QoS requirements specified by QoS profile descriptor.

The result belongs to the range [-31 to 65504]. Value SCI < 32 means that the BS suffers from degradation, which will be relaxed if (32 – SCI) MS with corresponding PSL values leave the BS.

D.1.2 Format of QoS Profile Descriptor

The QoS profile descriptor contains information on service flows authorized for MS. The descriptor has the following format: {**DescrType, NRTSInd, RTSInd1, RTSInd2**} where **DescrType** identifies the format of descriptor. This field is a function of the number of different services assigned to MS.

Value **DescrType = 0** corresponds to the case when there are **at most *three* services** per mobile terminal including at most two real time (RT) services. Each **RT service** is carried by MAC connection (or **pair of connections, for DL and UL**). All **non-real time services** are carried by a single pair of **DL and UL MAC connection** with certain QoS properties.

Other DescrType values are reserved for future extensions

NRTSInd is an index associated with certain set of parameters for non-real time service (see examples in Table D-3).

Table D-3 - NRT Services Encoding (example)

NRTSInd	Direction	QoS Parameters
…	…	…
18	DL	NRT-VR Max rate =512, reserved rate = 128
	UL	NRT-VR Max rate =128, reserved rate = 64
19	DL	NRT-VR Max rate =1024, reserved rate = 256
	UL	NRT-VR Max rate =128, reserved rate = 64

RTSInd1/2 are indexes associated with certain set of parameters for two real-time services (see examples in Table D-4).

Table D-4 - RT Services Encoding (example)

RTSInd	Activity	Direction	QoS Parameters	Notes
…	…	…	…	
120	Non-active	DL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	Video conferencing
		UL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	
121	Active	DL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	Video conferencing
		UL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	
122	Non-active	DL+UL	UGS packet length = 120, period = 60ms	VoIP call
		DL+UL	UGS packet length = 120, period = 60ms	
123	Active	DL+UL	UGS packet length = 120, period = 60ms	VoIP call
		DL+UL	UGS packet length = 120, period = 60ms	
…	…	…	…	

All indexes are one byte length. Index 0 means no service specified.

Meaning of indexes and their correspondence to QoS parameters is configured, per ASN or NAP. This encoding may differentiate between active and non-active RT services. For example, RT services LSB may be allocated for activity flag. So if the service is for VoIP, LSB will be set for calls, which are currently active (and therefore need an immediate capacity allocation after HO).

Note: The need for the “Activity” indicator in the Spare Capacity indicator for RT Services should be reviewed. – The report might be restricted to active services only. This is FFS.

D.1.3 Dynamic Configuration of Supported Service Types between RRM Entities (BS and RRC)

In order to provide scalability of new service deployments (i.e., new QoS profiles) without impacting changes in RRM procedures across several operators offering services, the supported Service Types to be used in RRM Spare Capacity reports whenever these are indexed by QoS Profiles are learnt dynamically between BS and RRC. Following considerations apply for dynamic learning of supported QoS profiles:

BSs may dynamically learn supported profiles from RRC.

Learning of the profiles may be done via the R6 protocol during initialization.

Each profile is identified for a unique profile ID, which could be used to index further RRM measurements.

A primitive to retrieve profiles on R6 is sent from the BS to RRC, and as a response, the BS receives all the profiles to be used.

A Service is defined as a pair of DL and UL QoS description and is formatted as (Service Indicator ServInd, Type of Service, and parameters associated with profile)

Example of a **Non Real time Service** is as follows:

Table D-5

ServInd	Type	DL Max Rate	DL Reserved Rate	UL Max Rate	UL Reserved Rate
1	NRT	1024	512	512	256

Example of a **Real-Time Service** is as follows:

Table D-6

ServInd	Type	DL Nominal rate	DL Reserved Rate	DL Max Latency	UL Nominal rate	UL Reserved Rate	UL Max Latency
2	RT	384	256	100	384	256	100

Forwarding of Ethernet encapsulated IP frames (ETH-CS w/ IP)

D.2 Alternative RRM reference model

Generic Reference Model #2b is characterized by:

- RRA and RRC collocated in the BSs;
- R8 is used for RRC to RRC communication.

This is shown in Figure D-1.

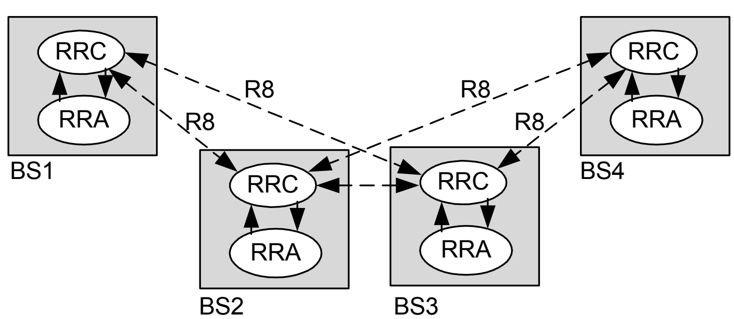


Figure D-1 - RRA and RRC Collocated in BS

The above reference model is based on collocated RRA and RRC in each BS. The interface between RRA and RRC is outside the scope of this specification. It MAY be noted that in this reference model, only the information reporting procedures (dashed lines) are standardized at the NWG-specified R8 reference point, while the decision support procedures (bold lines) between RRA and RRC in each BS are proprietary and not standardized. The R6 reference point is not shown because R6 primitives are not used to exchange RRM information in this reference model.

E. Ethernet Operational Behavior

The sections below cover operational behavior of Ethernet

E.1 Packet Forwarding

The System shall classify any and all hosts connected to a MS as an un-trusted source connected to an un-trusted port.

The System shall classify any and all hosts connected to the BS via its Ethernet interface as trusted sources connected to trusted ports.

The System shall support basic packet forwarding.

The System shall support an Authenticated ID List.

When receiving a packet from an un-trusted port that is not singled out by requirements stated herein, the System shall forward that packet to a trusted port provided the source MAC address is found in the Authenticated ID List.

When receiving a packet from a trusted port that is not singled out by requirements stated herein, the System shall forward that packet to a specific un-trusted ports identified by the destination MAC address provided that this destination MAC address is found in the Authenticated ID List.

E.2 Authenticated ID List

The System shall provide a persistent data storage for the current *MS Authenticated ID List* that is stored in each specific MS.

The System shall synchronize the *BS Authenticated ID List* with the *MS Authenticated List* any time the MS registers with the BS.

The System shall synchronize the *BS Authenticated ID List* for the current BS of a MS when the *system provisioning element Authenticated ID List* is updated for that MS. The Authenticated ID list may be provisioned via PKMv2 EAP authentication, in which case the mechanism for synchronization is described below:

In particular in the case of ETH CS with IP:

The System shall support dynamic additions/deletions to/from the *BS Authenticated ID List* from the *DHCP Authenticating Agent* that is performing *DHCP ACK Snooping.*

The System shall synchronize the *MS Authenticated ID List* as a subset from the *BS Authenticated ID List* any time an entry is added to or removed from the *BS Authenticated ID List* as a result of either the *Authenticating DHCP Agent* or the system provisioning element *Authenticated ID List* synchronization.

In the case where the Authenticated ID list is provisioned via PKMv2 EAP authentication:

When the MS successfully authenticates to the network (using whatever identities and credentials are required by the operator), the AAA server sends to the BS (via the AAA protocol) indication of authentication success as well as the provisioned classifier and service flow parameters.

The prioritized classifier list shall specify classifiers and associated service flow information for the packets originating at MAC address or addresses that are permitted origin addresses for this authenticated user.

The prioritized classifier list shall specify “drop” for non-authentication packets originating at any other MAC address.

If dynamic authentication is supported for additional MS devices (e.g. via 802.1x), then upon successful MS authentication a management element at the provider shall dynamically provision appropriate classifier and service flow parameters for frames bearing the source MAC address of the newly authenticated MS.

In particular, in the case of ETH CS with VLAN Tags..

VLAN tag associations shall be provisioned per MS.

Host generated VLAN tags shall be authenticated using the MS provisioned tag and VLAN feature.

VLAN Ethernet frames as well as plain Ethernet frames shall be forwarded as defined herein to the trusted network after authentication; otherwise the VLAN tagged frames shall be silently ignored.

E.3 Packet Filtering

The System shall support *Broadcast Filtering*.

The System shall have the ability to enable or disable all *Ingress Broadcast Filter* and *Egress Broadcast Filter* functionality defined herein.

If disabled, the *Ingress Broadcast Filter* and *Egress Broadcast Filter* shall pass all packets destined for the MAC broadcast or any MAC multicast address.

Upon receiving any packet destined for the MAC broadcast or any MAC multicast address, the *Broadcast Ingress Filter* shall silently discard the packet.

Upon receiving any packet destined for the MAC broadcast or any MAC multicast address, the *Broadcast Egress Filter* shall silently discard the packet.

The System shall support *Basic Ingress Filtering*.

The System shall have the ability to enable or disable all *Ingress Filter* functionality defined herein.

If disabled, the *Ingress Filter* shall pass all packets.

The *Ingress Filter* shall silently discard any packet received for which the packet's destination MAC address can be found in the *MS Authenticated ID List*.

Upon receiving any packet from the MS, the *Ingress Filter* shall discard the packet if the source MAC address cannot be found in the current *MS Authenticated ID List*.

In particular in the case of ETH CS w/ IP:

The *Ingress Filter* shall permit all Address Resolution Protocol messages to pass to the *ARP Ingress Proxy Agent*.

The Ingress Filter shall permit all DHCP messages to pass to the Authenticating and Tagging DHCP Agents.

Upon receiving any packet from the MS that can be identified as an IP datagram, the *Ingress Filter* shall discard the datagram if the source IP address cannot be found in the current *MS Authenticated ID List*.

E.4 Forwarding of Plain Ethernet Frames (ETH-CS)

The MS may support *Standard Learned Bridging* between its airlink and any physical or logical MS side interfaces

The BS shall support *Standard Learned Bridging* between its airlink and its backhaul links

When performing *Standard Learned Bridging*, the BS or MS shall learn all source MAC addresses originating from a given un-trusted MS port up to MAXMSIP individual learned addresses. Subsequently, any packets destined for one of those learned address should be forwarded directly to that un-trusted port. The accumulation of all learned MAC to port associations constitutes the *MS Learned Bridge Table* as managed by the MS. The accumulation of all learned MAC to port associations constitutes the *BS Learned Bridge Table* as managed by the BS.

When performing *Standard Learned Bridging*, the BS or MS shall silently discard all packets received from an un-trusted port, e.g. MS, for which the packet's destination MAC address is also an entry for that port in the *MS Learned Bridge Table*.

When performing *Standard Learned Bridging*, the BS or MS shall automatically unlearn a MAC to un-trusted port relationship after BRIDGETIMEOUT seconds have expired without any traffic from that MAC address.

When performing *Standard Learned Bridging*, the BS or MS shall forward all packets received from any un-trusted port to a trusted port provided the destination MAC address does not match a currently learned relationship to an un-trusted port. This implies that peer-to-peer communication is not available when performing *Standard Learned Bridging*.

When performing *Standard Learned Bridging*, the BS or MS shall flood any packet received from a trusted port destined for a MAC broadcast or multicast address to all un-trusted ports.

When performing *Standard Learned Bridging*, the BS or MS shall forward all packets received from a trusted port to an un-trusted port that is identified by the destination MAC address. If a learned port corresponding to the destination MAC address does not exist, the packet must be silently discarded. The IP TOS field shall be inspected and may be used as an authenticated QoS trigger.

E.5 Forwarding of Ethernet-encapsulated IP Frames (ETH-CS w/ IP)

The System shall support port and host classification.

E.6 Proxy Address Resolution Protocol (Proxy-ARP)

The System shall support Proxy-ARP.

The System shall have the ability to enable or disable all *ARP Ingress Proxy Agent* and/or *ARP Egress Proxy Agent* functionality defined herein.

If disabled, the *ARP Ingress Proxy Agent* or *ARP Egress Proxy Agent* shall pass all ARP packets without discrimination or modification using *Standard Learned Bridging*.

Upon receiving an ARP Request from a trusted source, the *ARP Egress Proxy Agent* shall unicast an ARP Response back to that trusted source, provided that the target address matches an entry in the *Authenticated ID List*. If the match is found, the *ARP Egress Proxy Agent* shall also forward the original ARP Request to the specific MS identified by the match. Otherwise, the *ARP Egress Proxy Agent* shall silently discard the Request.

Upon receiving an ARP Response message from a trusted source, the *ARP Egress Proxy Agent* shall forward the response to the MS specifically addressed by the destination MAC address, provided that this address can be found in the *Authenticated ID List*. Otherwise, the *ARP Egress Proxy Agent* shall silently discard the Response.

Upon receiving an ARP Request from an un-trusted source, the *ARP Ingress Proxy Agent* shall unicast an ARP Response back to that trusted source provided that the target address matches an entry in the *Authenticated ID List*. If the match is found, the *ARP Ingress Proxy Agent* shall also forward the original ARP Request to the specific MS identified by the match. Otherwise, the *ARP Ingress Proxy Agent* shall flood the Request to all trusted ports.

Upon receiving an ARP Response message from an un-trusted source, the *ARP Ingress Proxy Agent* shall silently discard the Response.

The *ARP Ingress Proxy Agent* shall silently discard any received self-ARP Requests. Those are requests for a target IP address, that when queried in the *Authenticated ID List* results in a response MAC equal to the Request's source MAC address.

The ARP Egress Proxy Agent shall issue a gratuitous ARP for any new addition to the Authenticated ID List resulting from DHCP ACK Snooping, MS Authenticated ID List merging, or provisioning system Authenticated ID List synchronization. An unsolicited broadcast ARP Response constitutes a gratuitous ARP.

E.7 Forwarding of VLAN-tagged Ethernet Frames (VLAN ETH-CS)

Filtering and forwarding of plain Ethernet shall apply to IEEE 802.1pq VLAN tagged frames.

E.7.1 IEEE 802.1Q VLAN Transport

Filtering and forwarding of plain Ethernet shall apply to VLAN tagged frames.

Authenticated host generated VLAN Ethernet frames as well as plain Ethernet frames shall be forwarded to the trusted network.

Unauthenticated VLAN Ethernet frames shall be discarded.

E.7.2 BS VLAN Proxy

The BS shall act as a VLAN proxy and add VLAN tags to ingress traffic and remove egress traffic.

The BS shall transmit only the untagged Ethernet frames over the air.

The BS shall make VLAN tag associations based on BS provisioned policies.

E.7.3 BS VLAN Translation and Stacking

VLAN IDsVLAN IDsVLAN IDsThe BS shall make VLAN tag translation or stacking associations based on BS provisioned policies. The BS shall translate MS private VLAN IDs and Priorities to the CSN core VLAN IDs and priorities, or the BS shall stack MS private VLAN IDs and Priorities inside the CSN core VLAN IDs and priorities.

E.7.4 BS VLAN Classification

The VLAN priority tag IEEE 802.1p shall be inspected and may be used as an authenticated QoS trigger.

E.8 Dynamic Host Configuration Protocol Agent— Address Authentication

The System shall support DHCP Agent Address Snooping.

The System shall have the ability to enable or disable all *Authenticating DHCP Agent* functionality defined herein.

If disabled, the *Authenticating DHCP Agent* shall forward all DHCP messages without discrimination or modification using *Standard Learned Bridge Forwarding*.

The *Authenticating DHCP Agent* shall add an entry in the *Authenticated ID List* upon detection of a DHCP ACK from the server on a trusted port. This is called *DHCP ACK Snooping.* The duration of the lease, LEASE, the moment of lease, LEASEMOMENT, and the corresponding MS shall also be recorded in the *Authenticated ID List*.

The *Authenticating DHCP Agent* shall silently discard all DHCP DISCOVERY, INFORM, REQUEST, and DECLINE messages received on a trusted port.

The *Authenticating DHCP Agent* shall silently discard all DHCP OFFER, ACK, NACK, and FORCERENEW messages received on an untrusted port.

When forwarding DHCP OFFER, ACK, NACK, FORCERENEW to untrusted MS ports, the Authenticating *DHCP Agent* shall correlate the target hardware address (not destination MAC), transaction identifier, and agent remote identifier (if present) with a previously DHCP DISCOVERY, INFORM, REQUEST, or DECLINE. If a correlation is made, only the MS identified from the first message shall be used to forward the subject message, even if destined for a broadcast MAC. Otherwise, the message shall be silently discarded.

When maintaining state for target hardware address, transaction identifier, and agent remote identifier received from a DHCP DISCOVERY, INFORM, REQUEST, or DECLINE that is meant to correlate with a returning DHCP OFFER, ACK, NACK, or FORCERENEW, the *Authenticating DHCP Agent* shall expire the state and reclaim resources if the response is not received within T4 seconds.

When adding an entry to the *Authenticated ID List*, the *Authenticating DHCP Agent* shall start a timer for that entry which is set to expire at a point not to exceed the original lease duration (LEASE) from the original lease moment (LEASEMOMENT). This includes List augmentation from *DHCP ACK Snooping*, *MS Authenticated ID List* merging, and *provisioning system Authenticated ID List* synchronization.

The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* when forwarding a DHCP NACK to an untrusted port.

The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* when forwarding a DHCP DECLINE message issued from an untrusted port.

NOTE—The resulting DHCP ACK must still be forwarded even after the entry is removed from the List.

The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* upon detection of a timer expiration.

The *Authenticating DHCP Agent* shall remove all entries from the *Authenticated ID List* corresponding to a particular MS when a Registration Cancellation is received.

The *Authenticating DHCP Agent* shall remove an old entry from the *Authenticated ID List* upon detection of an existing IP address in the List before adding a new entry. The old entry is only discarded if it has a finite LEASE period. Otherwise, the new entry is discarded.

The *Authenticating DHCP Agent* shall discard the least-recently-leased entry, e.g., the one with the oldest LEASEMOMENT, in the *Authenticated ID List* that uses the same MS if an attempt to added a new entry to the List is made which results in more than MAXMSIP entries for that MS.

E.8.1 Dynamic Host Configuration Protocol Optional Information Tagging

The System shall support DHCP Information Option Tagging.

The System shall have the ability to enable or disable all *Tagging DHCP Agent* functionality defined herein.

If disabled, the *Tagging DHCP Agent* shall forward all DHCP messages without discrimination or modification using *Standard Learned Bridge Forwarding*.

The *Tagging DHCP Agent* shall append (or tag) an Information Option to all DHCP DISCOVERY, INFORM, REQUEST, and DECLINE messages received from an untrusted port. The modified message must be then forwarded/flooded to all trusted ports.

Any DHCP DISCOVERY, INFORM, REQUEST, or DECLINE message received by the *Tagging DHCP Agent* that already contains an Information Option shall be silently discarded.

The *Tagging DHCP Agent* shall remove (or detag) any Information Options from all DHCP OFFER, ACK, NACK, and FORCERENEW messages received from a trusted port. The modified message must be then forwarded to the untrusted MS port.

NOTE—The subject message is not required to have the Information Option.

When tagging a DHCP message, the *Tagging DHCP Agent* shall add the Agent Circuit ID sub-option (1), specifying the BS ID as the circuit ID.

When tagging a DHCP message, the *Tagging DHCP Agent* shall add the Agent Remote ID sub-option (2), specifying the MS ID as the circuit ID.

F. Technical Annex: Support of real time services

As Release 1.0.0 provides only pre-provisioned QoS-Service Flows, Service Flows for real time service could not be activated dynamically. This limitation requires specific arrangements to support real time services also in Release 1.0.0.

As QoS resources are reserved for the whole duration while a subscriber is attached to the network, it is recommended to only activate QoS-services which allow sharing of radio resources dependent on the current traffic. The use of UGS (Unsolicited Grant Service) is not recommended because it will lock radio resources also in case if there is no traffic.

To provide 100% service guarantee it is recommended that the amount of bandwidth of real time services for the maximum of attached users per BS do not exceed the maximum bandwidth provided by the BS.

$$BW_{RT} * Subs_{Max} < BW_{Max}$$

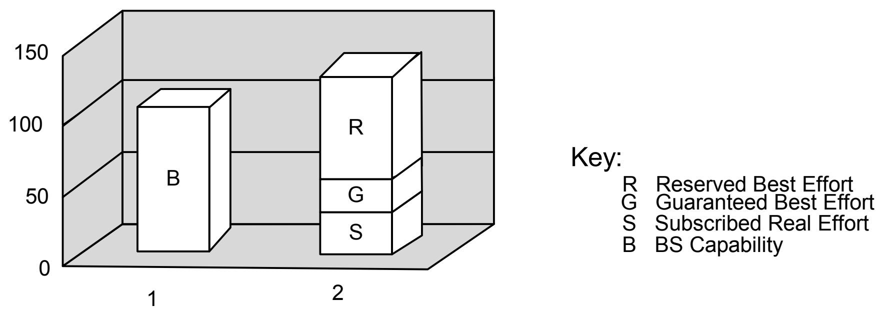
BW_{RT} ...Bandwidth of real time service

$Subs_{Max}$ ... Maximum number of subscribers attached to a BS

BW_{Max} ... Maximum bandwidth provided by the BS

An illustrative example:

A guaranteed best effort together with the amount of active real time services should not exceed the BS capabilities. The unassured bandwidth of best effort traffic could exceed the capability of a BS.



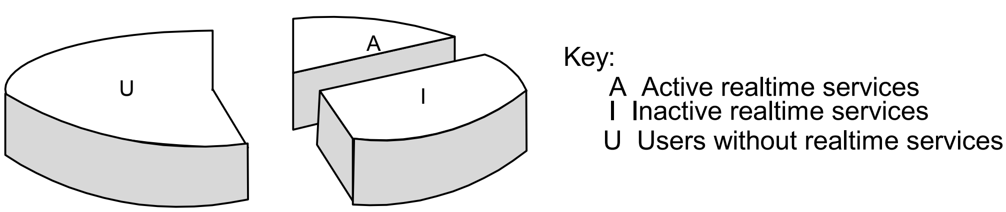
The number of maximum subscribers with real time service could be increased dependent on the distribution of active and inactive subscribers attached to a network and the usage of the real time service. E.g. a usage frequency of 50% for a service (which means, that an attached subscriber uses the service actively 50% of the time) will double the number of subscribers possible to be attached to a BS.

$$Subs_{Max} < BW_{Max}$$

Such extension of supported users may reduce the service guarantee.

An illustrative example:

All the registered subscribers are composed by users with and without a subscription for real time services. Furthermore, subscribers with a subscription can be reduced by them which haven't them activated.



This will reduce the BS capability to guaranteed bandwidth and the traffic expected by subscribers with activated real time traffic.

Attachment 4-6

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[WiMAX Interworking with DSL]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[WiMAX Interworking with DSL]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

1. Internetworking with DSL

Note: See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

1.1 DSL Reference Architecture

A simplified DSL reference model for the most common scenarios according to [62], [63], [64] and [75] of the DSL Forum is depicted in Figure 1. At the bottom of the picture the protocol layering is shown for the PPP over Ethernet as well as for the IP over Ethernet case.

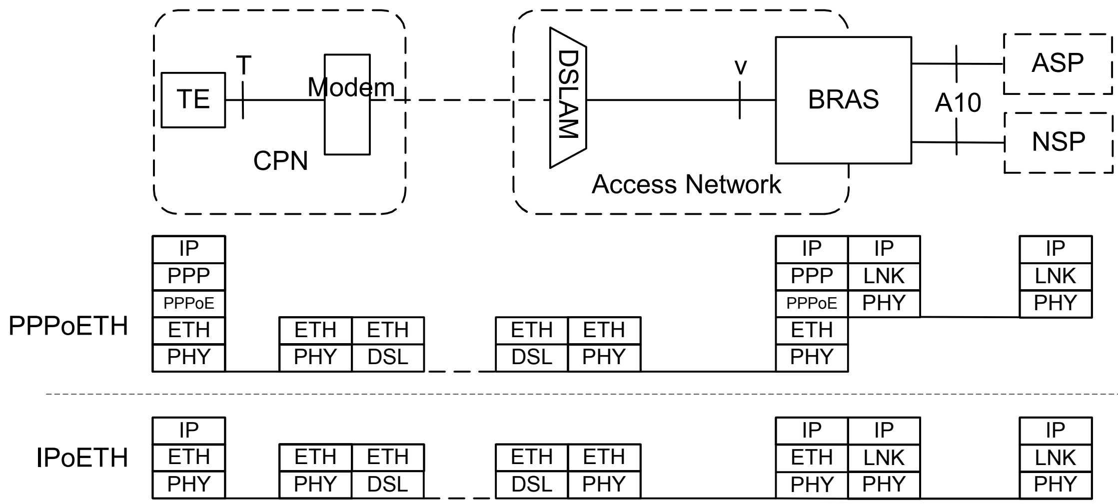


Figure 1 - DSL Reference Architecture

Figure 1 denotes the following reference points:

T: Interface between terminal equipment and DSL modem in the customer premises network (CPN)

V: Ethernet aggregation in the access network

A10: Interface between the access network and service providers. This interface connects either an Application Service Provider (ASP) to the Network Service Provider (NSP) owning the access network or in sharing scenarios the NSP with the access network.

Current DSL deployments for pure data services are mostly based on PPP over Ethernet as link protocol between BRAS and TE for the IP configuration of the terminal and the control and management of the IP link to the terminal. Regarding DSL deployments allowing QoS provisioning (typically used for delivering Data + voice + video service), they are mostly based on IP over Ethernet model.

1.1.1 DSL Service Based on PPPoETH

Widely used as protocol for commercial dial-up access to the Internet, PPP provides all the control functions operators require also for providing broadband access. With the evolution from ATM towards Ethernet as universal link layer protocol, PPP has to be encapsulated into PPPoE frames to emulate on top of Ethernet the point-to-point connectivity, for which PPP is designed for. With the application of PPPoE, just a plain Ethernet network is required between BRAS and TE.

1.1.2 DSL Service based on IPoETH

IP over Ethernet fully relies on DHCP for identification and for the configuration of the customer premises equipment. Additionally, IEEE 802.1x security framework may be used if deemed necessary by the DSL operator.

1.1.3 DSL Internetworking Scenarios

According to the DSL reference architecture the end-to-end DSL network consists of several providers. The role of the Application Service Provider, the Network Service Provider and the Access Service Provider in the DSL reference architecture is similar to the role of the ASP, NSP and NAP in the WiMAX reference architecture.

Aligned to the provider structure of the DSL reference architecture, internetworking between a mobile WiMAX network and a DSL network can be established at different stages of the end-to-end DSL network.

Internetworking Between a Mobile WiMAX Network and a DSL Access Network

Internetworking Between a Mobile WiMAX Network and a DSL NSP Network

The migration of DSL access networks towards Ethernet based aggregation introduces a V reference point in the architecture which allows the combination of a mobile WiMAX network with a DSL access network based on Ethernet bridging. The details of this reference point are defined in WT-101 of the DSL Forum.

A WiMAX network providing plain Ethernet bridging capabilities can be used to extend the reach of a DSL access network over wireless links.

Details of this kind of internetworking are described in Section 1.2 for WiMAX systems based on IEEE802.16-2004 and in Section 1.4 for the mobile WiMAX network.

This internetworking scenario usually requires support of the Ethernet CS in the base station. Under special conditions (only IPoETH DSL service, only single host CPE) also the use of the IP CS is possible.

Internetworking Between a Mobile WiMAX Network and a DSL NSP Network

TR-059 defines the interface between the DSL access network and the DSL NSP network. This interface is denoted A10-NSP and exists in two different flavors. One version is based on forwarding of layer 2 PPP connections over L2TP; the other version describes a layer 3 IP routed interface similar to the R5 interface in the WiMAX architecture used for the roaming case. By use of an appropriate interworking unit it is feasible to convert WiMAX R5 to the IP routed version of the A10-NSP. This kind of internetworking is further detailed in Section 1.3.

It is not possible to provide internetworking between mobile WiMAX and a DSL NSP based on the L2TP version of A10-NSP because the mobile WiMAX network does not handle PPP connections.

Internetworking Between a Mobile WiMAX Network and a DSL ASP Network

[64] also defines the interface A10-ASP between the DSL access network and the DSL ASP network. Internetworking between a mobile WiMAX network, which includes mobile WiMAX Terminals and a DSL ASP network can be achieved by the use of an interworking unit between WiMAX R5 (non-roaming case) and the A10-ASP.. Further details about this kind of internetworking are also provided in Section 1.3.

1.2 Integration of IEEE Std 802.16

Requiring only plain Ethernet bridging behavior between BRAS and TE for both cases, the PPPoETH as well as the IPoETH, allows the replacement of the DSL link by another transmission technology without any impact in the higher layer network architecture. As shown in Figure 2 the first generation WiMAX technology according to [1] is easily deployable in a DSL network by just replacing the DSL link by a wireless WiMAX link providing Ethernet bridging behavior.

At the bottom of the Figure 2 the protocol layering is drawn for both cases, the PPP over Ethernet as well as IP over Ethernet, and highlights the replacement of just the DSL link by a wireless link according to [1].

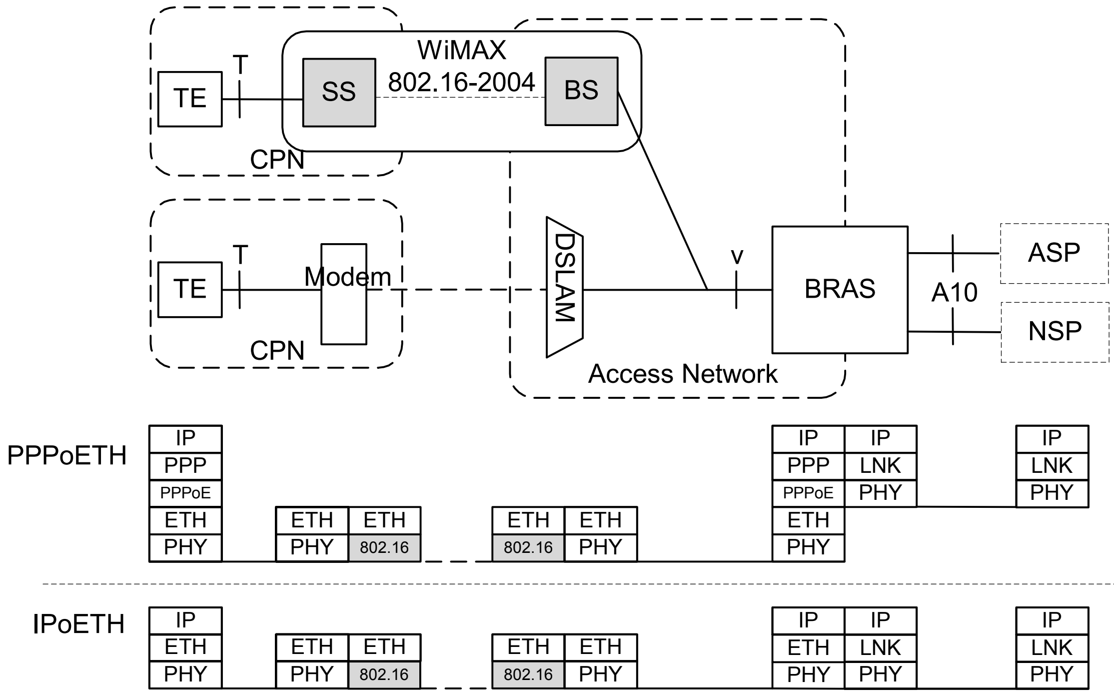


Figure 2 - WiMAX IEEE 802.16 FWA Deployment in a DSL Network

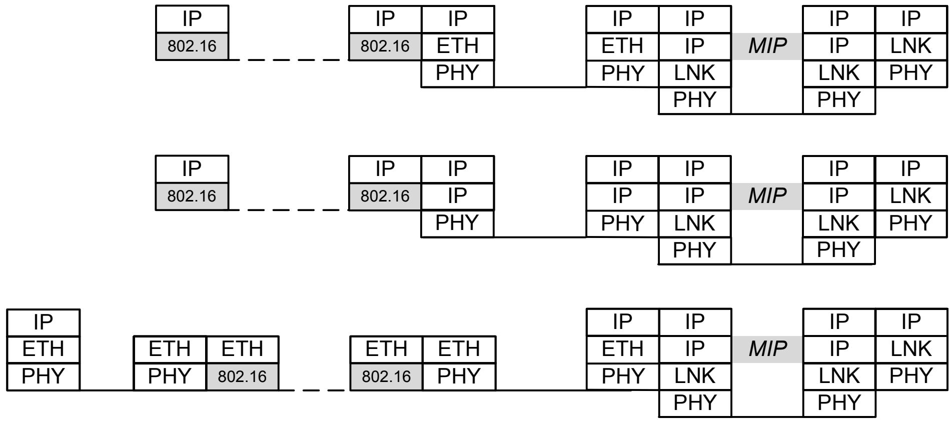
While [1] nicely fits into DSL architectures, [2] and its mobile WiMAX network architecture introduces a number of new network functions.

1.3 Interworking of Mobile WiMAX with DSL Services (A10 Interworking)

The mobile WiMAX network architecture describes a whole network with a two-layer mobility management structure and additional network elements to control mobility and enhanced security of terminals moving in a large area wireless network. Instead of PPP the enhanced 802.16 security sub layer PKMv2 and DHCP are used for terminal configuration and link control and management.

For mobile applications requiring MIP based mobility management provided by R3 between ASN and CSN the WiMAX network is assumed to integrate with the services provides by a DSL core via an IP interface between the CSN and the DSL core. The IWU as shown in the Figure 3 below mediates the R5 interface of WiMAX to an A10 conformant interface for integration with the services provided by the DSL core. The IWU may also co-locate a DHCP relay to access a DHCP server in the regional broadband network.

The use of EAP over RADIUS is presumed for AAA over R5 to enable authentication of mobile WiMAX users accessing DSL services.



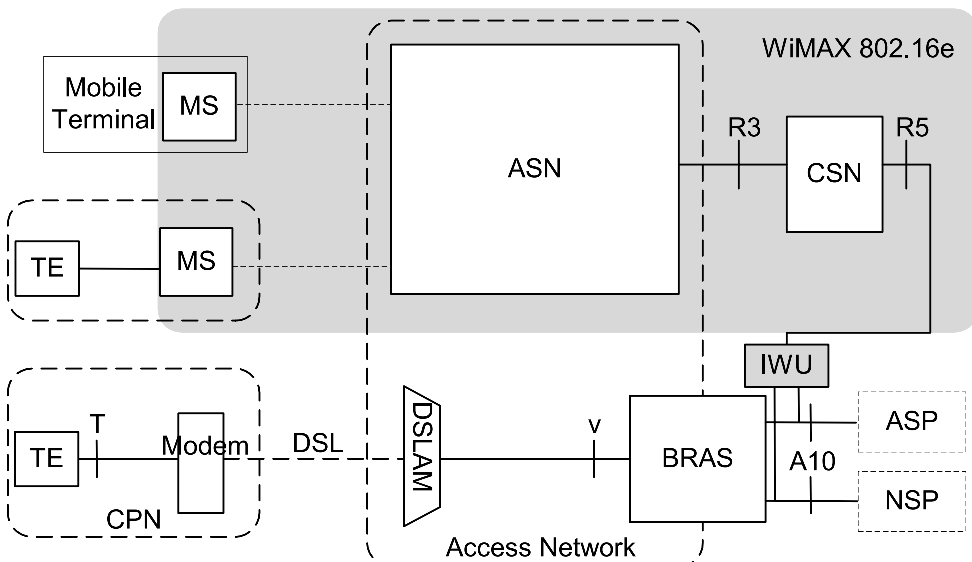


Figure 3 - WiMAX Integration with DSL Services

1.4 Interworking of Mobile WiMAX with DSL Access Networks (V Interworking)

For mainly fixed and nomadic WiMAX applications exposing the T reference point of the DSL architecture to the customers, the solution presented above is not suitable due to the unavailability of Ethernet bridging over R3 towards CSN.

When Ethernet bridging is available over the air (ETH CS) and within the ASN, Ethernet packets can be forwarded to the V aggregation point at the BRAS by a direct link between the ASN and the Ethernet aggregation point in the DSL access network. In this case the Ethernet-enabled ASN can be reused to bridge PPPoE packets across a single ASN bypassing the functions of the R3 reference point .While user data is carried directly to the V aggregation point, there is still a need for a mobile WiMAX network compliant control plane for establishing the bridging connectivity across the air. As user authentication is performed within PPPoE, device authentication and the PKMv2 security framework should be applied for the bridging MS to establish the 802.16e link. The appropriate forwarding configuration inside the ASN is established during the service discovery phase of PPPoE when the client detects the MAC address of the BRAS offering the wanted service.

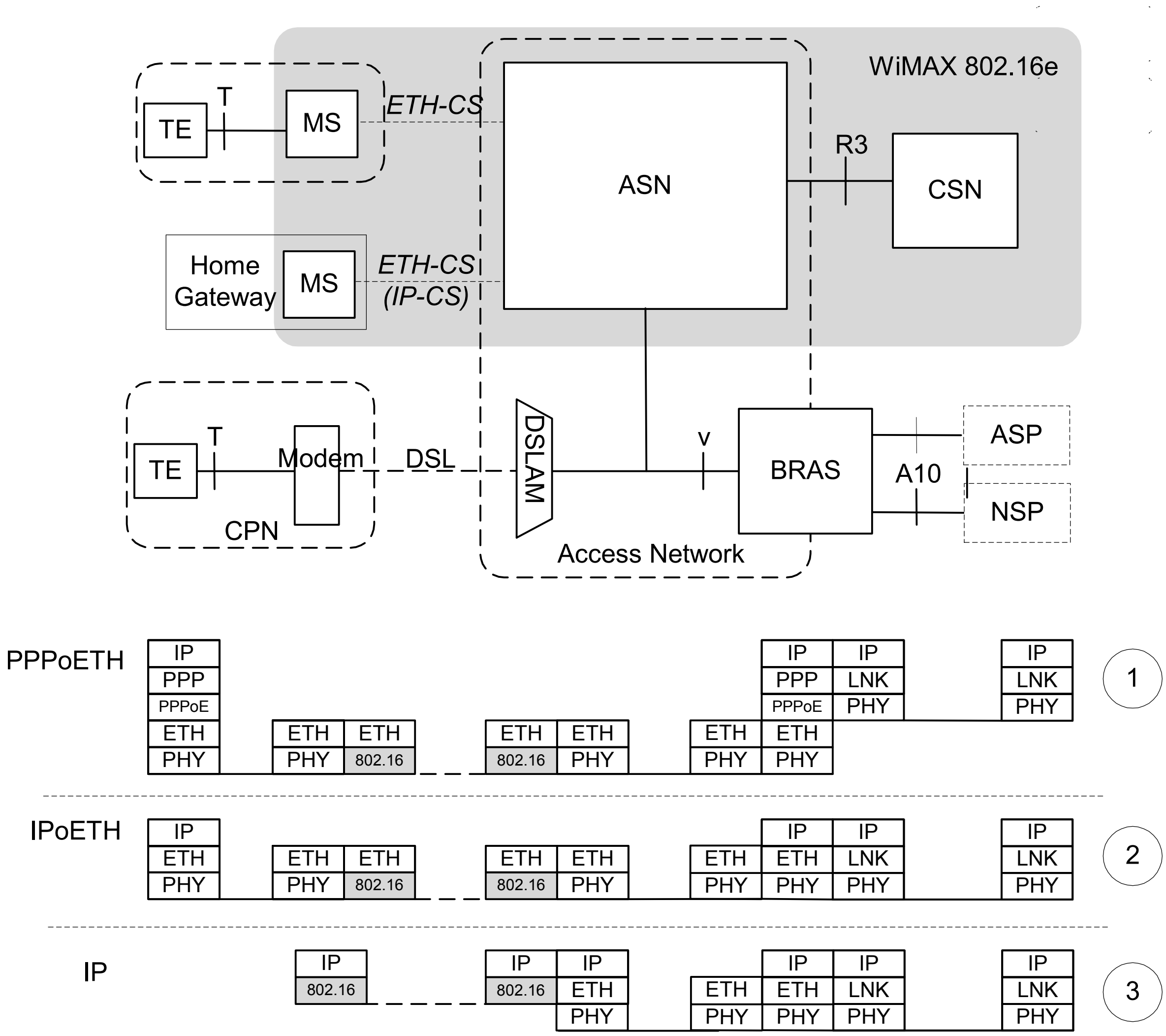


Figure 4 - WiMAX Integration with DSL Access Networks

This allows the integration of a mobile WiMAX network with a DSL network for offering DSL-like network interfaces for cases when WiMAX mainly replaces the wire usually required for DSL services. Option 1 in the protocol layering drawing at the bottom of Figure 4 shows the case for PPPoE.

While this kind of integration lacks the wide-area mobility management service it still remains the enhanced radio resource management, load balancing and security features of [2].

Also the IP over Ethernet DSL case can be integrated with an Ethernet based implementation of a mobile WiMAX network as shown for option 2 in the protocol layering drawing in the Figure 4 above. In that case, applying the PKMv2 security framework ensures security.

When Ethernet binding is available in the ASN but not over the air, as IP CS is used, uplink IP packets over 802.16 frames can be encapsulated at the BS in Ethernet frames and forwarded northbound to the V aggregation point at the BRAS by a direct link between the ASN and the Ethernet aggregation point in the DSL access network. This is depicted by the option 3 in the protocol layering drawing in the picture below. In this case, the user plane in the ASN allows for forwarding of Ethernet frames. As in the previous case, applying the PKMv2 security framework ensures the security.

Attachment 4-7

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[3GPP – WiMAX Interworking]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[3GPP – WiMAX Interworking]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

TABLES

1. Internetworking with 3GPP

1.1 Introduction and Scope

3GPP specifies how interworking with non-3GPP IP access networks (such as WiMAX ASNs) shall take place. Within the 3GPP Release 7 set of specifications, interworking with WLAN networks is specified in [TS23.234] and [T33.234] for security, where the following interworking scenarios are distinguished:

- Scenario 1 is the simplest case which impacts neither 3GPP nor the interworking network architecture. This just means a transparency for the subscriber in its relationship with his/her operator: the subscriber will be charged on the same bill for usage of both 3GPP and non-3GPP services, and custom care will be ensured without dependency on the connecting platform.
- In Scenario 2 (or Direct IP access), a subscriber MAY use the non-3GPP access network to access e.g. the Internet, but AAA operations are handled by the 3GPP platform.
- Scenario 3 (or 3GPP IP access) allows the operator to extend 3GPP system Packet Switched (PS) based services to the non-3GPP network. In this scenario, an authenticated 3GPP subscriber can access to 3GPP PS services through a non-3GPP access network interworking with its 3GPP PLMN (non roaming case) or with a visited 3GPP PLMN (roaming case).

Table 1 - WiMAX-3GPP Interworking Scenarios (Based on Table 3 of 3GPP TR 22.934)

	Scenarios		
Service and operational Capabilities:	**Scenario 1: Common Billing and Customer Care**	**Scenario 2: 3GPP system based Access Control and Charging**	**Scenario 3: Access to 3GPP system PS based services**
Common Billing	X	X	X
Common Customer Care	X	X	X
3GPP System Based Access Control		X	X
3GPP System Based Access Charging		X	X
Access to 3GPP System PS Based Services from WiMAX			X

In this document *WiMAX-3GPP interworking* is specified based on the I-WLAN architecture described in [TS23.234] and [T33.234] by 3GPP. The solution covers both Direct IP access ("scenario 2") and 3GPP IP access ("scenario 3"), denoted *WiMAX Direct IP access* and *WiMAX 3GPP IP access* in the context of this specification.

This solution does not modify [TS23.234] and [TS33.234] in any way, but builds on top of it by providing missing interworking functionality from the WiMAX perspective, within the WiMAX CSN. The motivation for this is to make available an interworking solution in the time frame of the WiMAX NWG Release 1 architecture as well as the 3GPP Release 7 timeframe that is focused on scenarios 2 and 3.

It is, however, understood that for future releases, a more advanced and integrated interworking solution between WiMAX networks and 3GPP networks is under development as part of the 3GPP SAE (system architecture evolution) effort. The interworking solution specified in this document does not limit such future architectures.

Additional considerations for IPv6 related to scenario-3 interworking are out-of-scope for this release of the document.

1.2 Control Plane Protocols and Procedures

This section provides the detailed description of WiMAX-3GPP interworking

1.2.1 WiMAX specifics in direct and 3GPP IP access

Due to a number of features that are specific to the WiMAX NWG architecture but are not available for WLAN networks covered by the 3GPP I-WLAN specification, WiMAX-3GPP interworking requires a set of additional functions to support these features, for enabling standard operation within the WiMAX part of the interworking architecture.

WiMAX networks as specified by [NWG Stage-3] allow access to IP services for users subscribed to a WiMAX CSN operator. For gaining access to WiMAX network resources, the user's MS has to perform an initial network entry procedure as specified in [NWG Stage-3, section 5.5]. During initial network entry, the following major steps need to be performed:

- Network discovery and selection
- User/Device Authentication
- QoS and Service Flow establishment
- Mobile IP registration and tunnel establishment

This document details how these steps shall be performed for the WiMAX-3GPP interworking case.

For access to WiMAX networks, security for the 802.16-2005 wireless link needs to be established. Hence, for WiMAX 3GPP IP access, WiMAX Direct IP access shall be performed first to establish appropriate key material in the ASN Authenticator for initiating protection of the R1 wireless link (PKMv2). This is required to allow access to the WiMAX ASN/CSN resources and initiate the final establishment of the secure Wu tunnel for WiMAX-3GPP IP access (according to [TS23.234] I-WLAN 3GPP IP access).

1.2.2 Detailed Solution

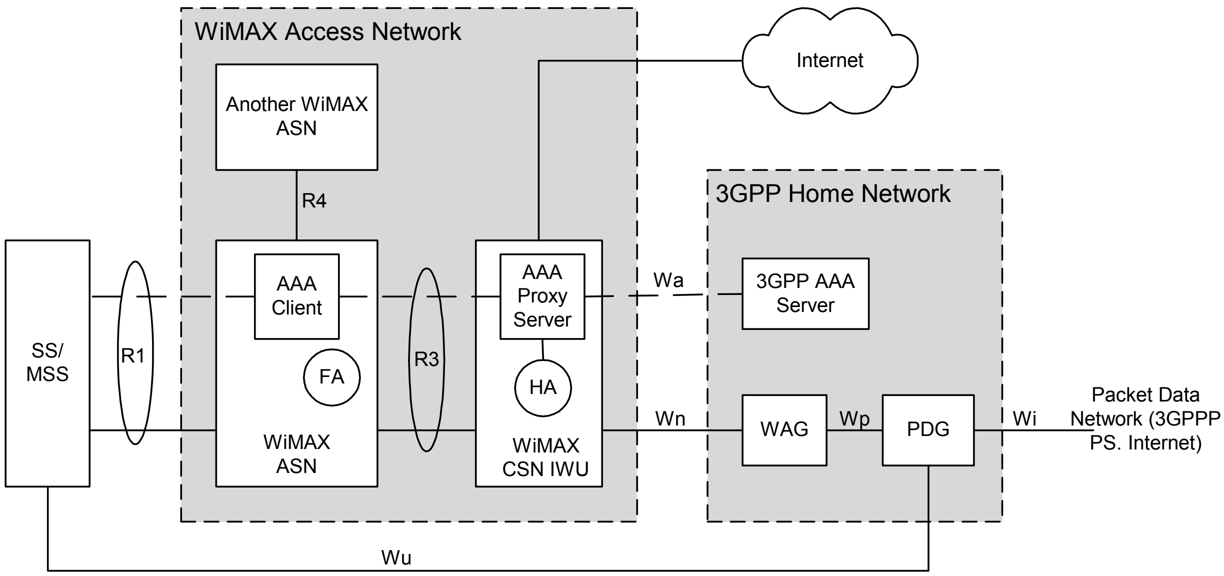


Figure 1- WiMAX-3GPP Interworking (Non-Roaming Case)

Figure 1 represents the WiMAX-3GPP Interworking architecture and the appropriate Reference Points.

Unless otherwise mentioned, all the content of [TS23.234] and [T33.234] shall be applied to the WiMAX Interworking case. This includes the specification of the Wa, Wn and Wu inter-technology interfaces.

The WiMAX ASN and CSN networks provide standard WiMAX functionality as specified in [NWG stage-3]. Accordingly, Internet connectivity, Mobile IP and IP address management are provided by the WiMAX CSN (except those aspects covered by the Wu tunnel for WiMAX-3GPP IP access).

Based on this, the following sections specify functionality required in the WiMAX ASN and CSN to support interworking with 3GPP networks for roaming 3GPP subscribers using a WiMAX MS or WiMAX-enabled 3GPP UE (which is for brevity also denoted a MS in this specification).

1.2.2.1 General Requirements to the WiMAX Network

The WiMAX ASN supporting WiMAX-3GPP interworking shall support PMIP operation for any WiMAX-3GPP interworking MS in compliance with [NWG stage-3], section 5.8.

The WiMAX CSN shall provide an interworking AAA proxy/server that is in the path of the AAA signaling between the Authenticator of the ASN and the 3GPP AAA server responsible for user authentication in the 3GPP home network (Wa interface to the 3GPP core network). It is responsible for:

- Generating PMIP keys
- Distributing these keys to the involved entities of the WiMAX network (HA and PMIP client).
- Handling the RADIUS attributes that are WiMAX-specific or needed for Mobile IP

1.2.2.2 Network Discovery and Selection

Once the MS has detected the available ASNs and corresponding CSN that provides WiMAX-3GPP interworking support in a given area by the means of methods described in [NWG stage-3], the selection of the 3GPP PLMN shall be done accordingly to TS 23.234.

1.2.2.3 User/Device Authentication

For WiMAX-3GPP interworking, the WiMAX user authentication shall be based on EAP-SIM or EAP-AKA. Device authentication is not supported by 3GPP AAA servers. If device and user authentication (double EAP) is performed, the device authentication is performed within the WiMAX network. A 3GPP AAA server does not support the WiMAX-specific authentication mode of combined device/user authentication (using single-EAP) or device-only authentication, so these authentication modes are not supported with 3GPP interworking.

Hence, the MS shall not run a combined device/user authentication using single-EAP (AuthMode {4}). The AAA proxy may reject an unsupported authentication mode by checking the provided NAI that encodes the authentication mode as decoration .

User-only Authentication:

A single EAP authentication run takes place between MS and the 3GPP AAA server, with the CSN interworking AAA proxy/server in the path. If the authentication is successful (EAP-Success), the interworking AAA proxy/server forwards the resulting MSK key to the AAA client in compliance with the common WiMAX and 3GPP procedures.

A number of AAA attributes used within the WiMAX AAA architecture are WiMAX defined VSAs not known to, or provided by, the 3GPP AAA server.

For this, the following RADIUS WiMAX VSAs are added by the interworking AAA proxy/server to support standard WiMAX operation in the path of user authentication, to the RADIUS Access-Accept message that is sent by the 3GPP AAA server to the Authenticator after successful user authentication:

- WiMAX-Capability (type 26/1)
- Framed-IP Adress (HoA)
- AAA-Session ID (type 26/4)
- MSK (type 26/5), carries the MSK received from the 3GPP AAA server
- RADIUS VSAs between ASN and HAAA for bootstrapping mobility service as specified in [NWG-stage-3] table [tbd].
- RADIUS attributes between ASN and HAAA for DHCP relay as specified in [NWG-stage-3] table [tbd] in case DHCP relay is supported.
- For Mobile IP, the interworking AAA proxy/server adds the RADIUS attributes and values that are required for WiMAX operation of Mobile IP but that are not supported by the 3GPP AAA server. It shall add this HA address in the same way as a WiMAX AAA server would do.

The keys for MIP are added. They are derived from MIP-RK' using the derivation defined in section 5.3.5. MIP-RK' is created by the interworking AAA proxy/server. It is internal to the interworking AAA proxy/server how to create MIP-RK'. This can be a random number (MIP-RK' = RAND). RAND shall be a random number created for each user authentication by a cryptographically strong random number generator. The interworking AAA proxy/server also generates HA-RK according to the rules given in section 5.3.5 of [NWG-stage-3].

The interworking AAA proxy/server acts as AAA proxy during the network access authentication. Once receiving the EAP-Success message from the 3GPP AAA server, it stores the NAI of the authenticating user (marked as authenticated) and creates and stores the associated MIP-RK' and HA-RK keys for this session (used later for bootstrapping the Mobile IP HA).

Device and User Authentication (Double EAP):

Device authentication may be performed in advance to user authentication, if user authentication terminates in the 3GPP AAA server. If device authentication is performed during WiMAX-3GPP interworking, it must terminate in the WiMAX network (ASN or CSN). Subsequent user authentication is performed as described above.

NAI Considerations:

3GPP 33.234 requires that the (outer) NAI used for EAP-SIM/AKA contains either a pseudonym allocated to the WLAN-UE in previous authentication or, in the case of first authentication, the IMSI, if user identity privacy is used. The NAI construction as specified for [RFC4186] and [RFC4187] with the additional considerations given in [TS33.234] shall be used, with the following exception:

- The Authentication Mode preceding the user part of the WiMAX NAI shall be added by the MS for WiMAX-3GPP interworking.

The WiMAX-3GPP interworking AAA proxy shall remove the WiMAX authentication mode from the NAI when forwarding AAA messages to the 3GPP AAA server, and shall add the same value for AAA messages sent back to the AAA client.

1.2.2.4 Mobile IP registration support

The Mobile IP keys are created by the interworking AAA proxy/server in the CSN. These keys are distributed to the involved entities of the WiMAX network (i.e., HA and Authenticator). Distribution of these key happens in compliance with the mechanisms specified in section 5.3.5 of [NWG-stage-3], where the interworking AAA proxy/server (instead of the 3GPP AAA server that is not assumed to be WiMAX MIP-aware) interfaces with the HA in the CSN, and adds the PMIP keys to the RADIUS Access-Accept message of the 3GPP AAA server during user authentication, such that the Authenticator in the ASN receives the keys required for PMIP operation for this specific MS.

The interworking AAA proxy/server acts as AAA proxy during the network access authentication. When it receives the EAP-Success message from the 3GPP AAA server, it shall store the NAI of the authenticating user (marked as authenticated) and create and store the MIP-RK’ and HA-RK keys for this session. MIP-RK’ is generated as described in section 1.2.2.3 above. This generation of MIP-RK’ is specific to WiMAX-3GPP interworking: The 3GPP AAA server does not provide MIP keys, and it does not export the EMSK key that would be needed for regular MIP-RK derivation as described in section 5.3.1 of [NWG Stage-3]. As the MIP_RK’ generation is internal to the WiMAX network it can only be used for PMIP. A 3GPP interworking MS shall not use CMIP.

When the Interworking PMIP client sends the MIP-RRQ message to the assigned HA, the HA requests the MIP keys from the interworking AAA proxy/server as described in [NWG-stage-3]. The interworking AAA proxy/server checks stored NAIs and returns the associated MIP keys when a matching entry for the NAI is available. These keys are derived from MIP-RK’ that was generated and stored during the preceded network access authentication for the same NAI.

The key derivation of MIP keys from MIP-RK’ is done as defined in section 5.3.5 of [NWG Stage-3]. The AAA proxy shall return an Access-Reject if no corresponding user session state (containing NAI and corresponding MIP-RK’) can be found.

1.2.2.5 Detailed Requirements to the MS

The MS shall not register with CMIP when using a subscription with a 3GPP operator for network access. If the WiMAX CSN receives a CMIP registration attempt by a 3GPP subscriber using WiMAX direct IP access, this registration attempt will fail due to wrong CMIP keys.

When using a 3GPP subscription for user authentication, the MS shall use EAP-SIM or EAP-AKA as EAP method.

For the outer NAI that is used in the EAP identity exchange, the NAI shall be constructed as specified in [TS23.234] for 3GPP-WLAN interworking, with the following exception: The authentication mode indication preceding the user part of the WiMAX authentication method “{n}” should be added by the MS for WiMAX-3GPP interworking.

The MS shall not run a combined device/user authentication using single-EAP (AuthMode {4}). This is due to the fact that a 3GPP AAA server cannot be assumed to support this WiMAX-specific Authentication Mode. If a terminal attempts to authenticate using this specific authentication mode, the interworking AAA proxy/server will respond with an error message, and the MS will not be able to gain access to the WiMAX network.

It is, however, possible to perform device authentication in addition to user authentication for a roaming 3GPP user, if device authentication terminates in the WiMAX network (ASN or CSN).

1.2.3 Limitations of this specification

- WiMAX-3GPP IP access based on the Wu Reference point IPsec tunnel might not allow the WiMAX terminal to enter the idle mode for power consumption saving due to the maintenance of the IPsec connection in an active state. Further development with 3GPP SA2 is required to enable idle terminals.

- WiMAX provides powerful and flexible QoS handling which is transparent to Direct IP access but can't be fully utilized within WiMAX-3GPP IP access. 3GPP SA2 is currently extending the specification for utilizing QoS-enabled IP-based access networks.
- Handoff capability from 3GPP network to WiMAX network is usually referred as scenario 4 (intersystem mobility) and 5 (seamless intersystem mobility). These scenarios are out of scope of release 1, but they will be addressed in future releases.
- CMIP operation, due to the fact that:
    - a 3GPP AAA server cannot be assumed to derive WiMAX-specific mobility keys from the EMSK, and
    - the (visited) WiMAX network and roaming 3GPP subscribers cannot be assumed to have pre-shared mobility keys,

  is not supported by this WiMAX release.

1.3 Reference Point Mapping and Security

1.3.1 Reference Points Linking the WiMAX Access Network to the 3GPP System

This section lists the relevant 3GPP reference points as specified by [TS23.234], and provides their mapping to WiMAX-3GPP interworking.

- Wa is the reference point transporting all AAA messages between the interconnected WiMAX and 3GPP networks. At the WiMAX side, it is terminated by a AAA proxy/server. At the 3GPP side, it is terminated by either the 3GPP AAA server, or an optional AAA proxy/server in the 3GPP network that is interconnected with the 3GPP AAA server. In cases where the WiMAX and 3GPP AAA infrastructure speak different AAA protocols, RADIUS/Diameter translation needs to be done at one side of the Wa interface. For co-existence of RADIUS and Diameter, the considerations given in [TS33.234], annex A.3.2 apply.
- Wn links the WiMAX Access network and the WAG (WLAN Access Gateway). The WAG is a gateway toward which the data coming from the WiMAX Access Network SHALL be routed. It is used to enforce the routing of packets through the appropriate PDG. WAG functionalities are described in details in [TS23.234].
- Wu refers to tunnel establishment and tear down between MS and the appropriate PDG (Packet Data Gateway), as well as user data packet transmission through this tunnel. PDG functionalities are described in details in [23.234]. The 3GPP technical solution for 3GPP IP access in [TS23.234] shall apply.
- Ww: connects the MS to the WiMAX Access Network; this reference point maps to the WiMAX NWG R1 reference point.

1.3.2 Reference Point Security

For reference point security of affected WiMAX network reference points, the recommendations and profiles given in [NWG stage-2], section [tbd] and [NWG stage-3], section [tbd] apply as specified. For securing reference points between the WiMAX network and the 3GPP networks, the following considerations shall apply:

- Wa: Interface between AAA proxy/server in the WiMAX CSN and 3GPP AAA server responsible for interworking.
  If the interface is based on RADIUS, protection is achieved by means of RADIUS standard procedures. In particular, the attribute MS-MPPE-Recv-Key [RFC 2548] provides protection of the MSK key derived in the 3GPP AAA server. If the interface is based on Diameter (i.e., a RADIUS/Diameter translation gateway is at the WiMAX side of the reference point), IPsec shall be used if there is no physical protection for this reference point (the support of IPsec for Diameter is mandatory as stated in [RFC3588]).
- Wn: It shall be possible to protect the integrity and confidentiality of IP packets sent through a tunnel between the WiMAX side and the 3GPP side of this reference point.
- Wu: The technical solution chosen by 3GPP for WLAN 3GPP IP access security [TS33.234] shall apply. With this, all data transferred through this tunnel is secured by IPsec.

- Ww: wireless MAC layer security is provided in compliance with [NWG-stage3] and [802.16-2005] through PKMv2. Device and user authentication are based on EAP methods. For WiMAX-3GPP interworking, EAP-SIM or EAP-AKA shall be used as EAP methods.

Attachment 4-8

End-to-End Network Systems Architecture

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)
[3GPP2 – WiMAX Interworking]

Release 1.1.0

WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[3GPP2 – WiMAX Interworking]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

1. Internetworking with 3GPP2

Note: See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

1.1 Integration of WiMAX Access Network in the 3GPP2 X.S0011-C model

This section describes the interaction between WiMAX Access Network and the 3GPP2 packet data network architecture. Since both the 3GPP2 PDSN (Packet Data Serving Node) and the WiMAX ASN-GW provide mobile IP foreign agent (FA) functionality, this is the simplest point for interworking. To support Interworking, the FA and HA shall support the following IETF RFC's:

- RFC 2003 – 2006
- RFC 3344 [43]
- RFC 3024 (reverse tunnelling) [29]
- RFC 2794 (NAI extension) [22]

In configuring the Mobile IP HA – FA Authentication Extension in the mobile IP registration messages there are three methods for deriving the Security Associations.

- Public Certificates (see Annex A and Annex B in 3GPP2 X.S0011-C)
- Dynamic IKE pre-shared secret distributed by the home AAA server
- Statically configured IKE pre-shared secret

Support of these capabilities and RFC's should allow for session mobility between 3GPP2 Packet Data networks and WiMAX networks for mobile clients.

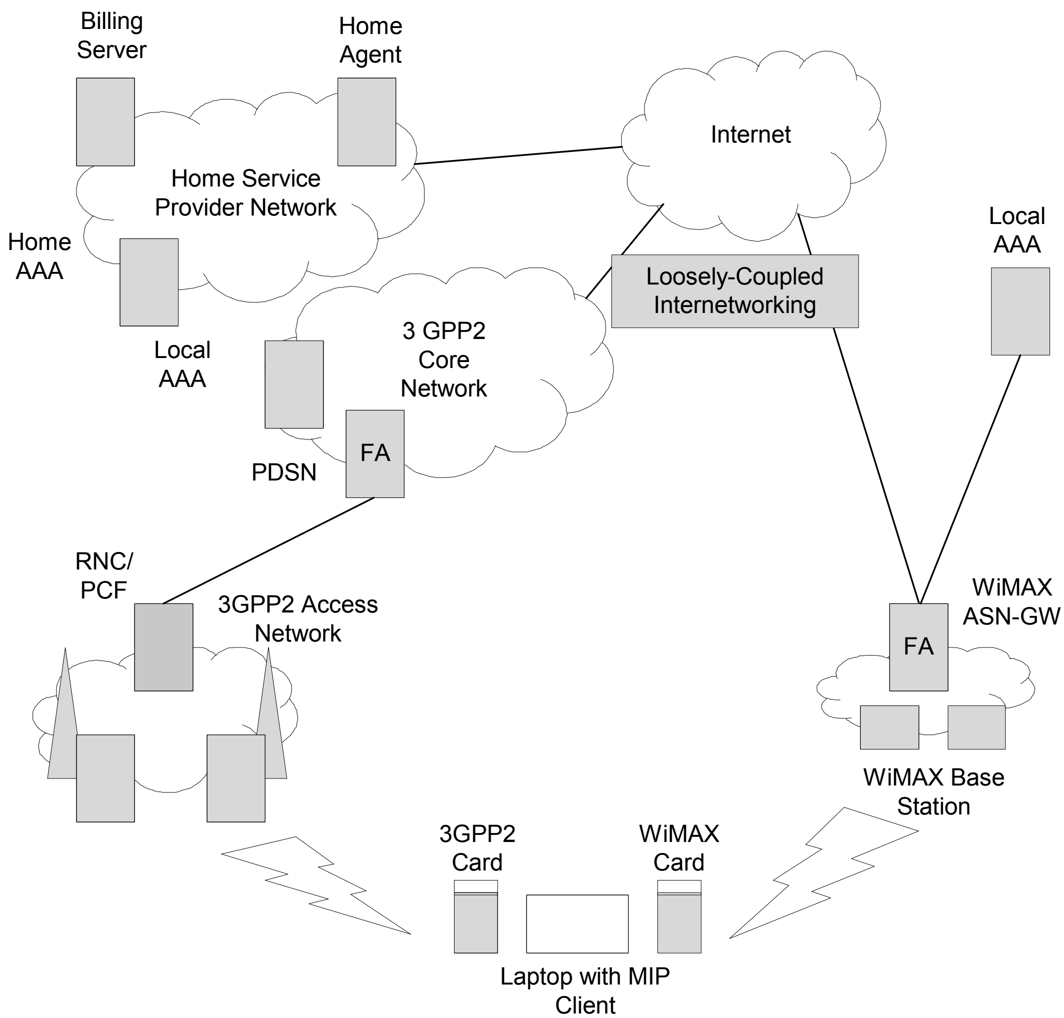


Figure 1 - Loosely-Coupled Interworking of WiMAX with 3GPP2

OFDMA Broadband Mobile Wireless Access System
(WiMAX™ applied in Japan)

ARIB STD-T94　Version 1.4

(1/2)

Version 1.0	December	12th	2007
Version 1.1	March	19th	2008
Version 1.2	June	6th	2008
Version 1.3	September	25th	2008
Version 1.4	March	18th	2009

Published　by
Association of Radio Industries and Businesses

11F, Nittochi Building,
1-4-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013,Japan
TEL　03-5510-8590
FAX　03-3592-1103

Printed in Japan