



**WiMAX Forum<sup>®</sup> Network Architecture**  
Architecture, Detailed Protocols and Procedures  
WiMAX<sup>®</sup> - 3GPP EPS Interworking

**WMF-T37-009-R020v01**

WMF Approved  
(2011-11-14)

**WiMAX Forum Proprietary**

Copyright © 2011 WiMAX Forum. All Rights Reserved.

1 **Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability**

2  
3 Copyright 2011 WiMAX Forum. All rights reserved.

4  
5 The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for  
6 download from the WiMAX Forum and may be duplicated for internal use by the WiMAX Forum members, provided that all  
7 copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be  
8 duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

9  
10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance  
11 of the following terms and conditions:

12  
13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**  
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND**  
15 **STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**  
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**  
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**  
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**

19  
20 Any products or services provided using technology described in or implemented in connection with this document may be  
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely  
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all  
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable  
24 jurisdiction.

25  
26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**  
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**

29  
30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**  
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**

33  
34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any  
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any  
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual  
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,  
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,  
39 technologies, standards, and specifications, including through the payment of any required license fees.

40  
41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**  
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**  
43 **INTO THIS DOCUMENT.**

44  
45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**  
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**  
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**  
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**  
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**  
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**

51  
52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is  
53 solely responsible for determining whether this document has been superseded by a later version or a different document.

54  
55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the  
56 WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks of the WiMAX Forum. All  
57 other trademarks are the property of their respective owners.

58

1	<b>Table of Contents</b>	
2	<b>1. INTRODUCTION AND DOCUMENT SCOPE .....</b>	<b>6</b>
3	<b>2. ABBREVIATIONS AND DEFINITIONS .....</b>	<b>7</b>
4	2.1 Abbreviations .....	7
5	2.2 Terms & Definitions .....	7
6	<b>3. REFERENCES.....</b>	<b>8</b>
7	<b>4. GENERAL REQUIREMENTS AND PRINCIPLES.....</b>	<b>10</b>
8	<b>5. INTERWORKING NETWORK REFERENCE MODEL.....</b>	<b>11</b>
9	5.1 Non-Roaming Architecture .....	11
10	5.2 Roaming Architecture.....	12
11	5.3 Reference point mapping.....	15
12	<b>6. PDN-GW SELECTION.....</b>	<b>16</b>
13	<b>7. ACCESS NETWORK DISCOVERY AND SELECTION.....</b>	<b>17</b>
14	7.1 Access Network Discovery and Selection Function (ANDSF) .....	17
15	7.1.1 Architecture for ANDSF.....	17
16	7.1.2 ANDSF Management Objects.....	17
17	<b>8. INITIAL ATTACH TO 3GPP EPC VIA WIMAX® ASN.....</b>	<b>18</b>
18	8.1 Initial Attach Procedure with PMIP6 on S2a.....	18
19	8.2 Initial Attach Procedure with CMIP4 on S2a.....	20
20	<b>9. DETACH PROCEDURE .....</b>	<b>22</b>
21	9.1 MS/UE initiated detach procedure.....	22
22	9.1.1 MS/UE initiated detach procedure using PMIP6.....	22
23	9.1.2 MS/UE initiated detach procedure using CMIP4.....	24
24	9.2 Network initiated detach procedure.....	26
25	9.2.1 ASN-GW/BS initiated detach procedure using PMIP6.....	26
26	9.2.2 HSS/AAA initiated detach procedure using PMIP6.....	29
27	9.2.3 ASN-GW/BS initiated detach procedure using CMIP4.....	30
28	9.2.4 HSS/AAA initiated detach procedure using CMIP4.....	32
29	<b>10. AUTHENTICATION AND SECURITY .....</b>	<b>33</b>
30	10.1 Use of EAP-AKA' – Initial Authentication.....	33
31	10.2 Use of EAP-AKA' – Fast Re-Authentication.....	33
32	10.3 Key derivation from EMSK.....	33
33	<b>11. IP ADDRESS ALLOCATION.....</b>	<b>34</b>
34	11.1 IP Address Allocation in WiMAX® Networks using CMIP4 on S2a.....	34
35	11.2 IP Address Allocation in WiMAX using PMIP6 on S2a.....	34
36	<b>12. IP MOBILITY MODE SELECTION.....</b>	<b>35</b>
37	<b>13. HANDOVER .....</b>	<b>36</b>

1	13.1	WiMAX® to 3GPP access handover procedures .....	36
2	13.1.1	WiMAX® to E-UTRAN over GTP based S5/S8 .....	36
3	13.1.2	WiMAX® to E-UTRAN over PMIP6 based S5/S8 .....	36
4	13.1.3	WiMAX® to UTRAN/GERAN over GTP based S5/S8 .....	36
5	13.1.4	WiMAX® to UTRAN/GERAN over PMIP6 based S5/S8 .....	36
6	13.2	3GPP access to WiMAX® .....	37
7	13.2.1	Handover from 3GPP to WiMAX® with PMIP6 .....	37
8	13.2.2	Handover from 3GPP to WiMAX® with CMIP4 .....	38
9	<b>14.</b>	<b>RESOURCE DEACTIVATION PROCEDURES .....</b>	<b>41</b>
10	14.1	PDN GW initiated Resource Deactivation using PMIP6 .....	41
11	<b>15.</b>	<b>POLICY AND CHARGING CONTROL .....</b>	<b>42</b>
12	15.1	ASN-GW requirements for 3GPP PCC Release 9 .....	42
13	15.2	Gxa interface requirements .....	42
14	15.3	PCC procedures and flows .....	43
15	15.3.1	Network-initiated dynamic PCC procedure .....	43
16	15.3.2	MS-initiated dynamic PCC procedure .....	44
17	15.3.3	Allocation and retention priority support .....	45
18	15.3.4	Intra WiMAX BBERF relocation for PMIPv6 .....	45
19	15.3.5	Intra WiMAX BBERF relocation for MIPv4 FACoA .....	47
20	15.3.6	PCRF discovery and selection .....	48
21	15.4	Message and Parameter definitions .....	49
22	15.4.1	Event trigger support list .....	49
23	15.4.2	Mapping Gxa Parameters between 3GPP and WiMAX .....	50
24	<b>16.</b>	<b>MS/UE IMPLICATIONS .....</b>	<b>57</b>
25	16.1	MS/UE Identities .....	57
26	16.2	CMIP4 security key derivation .....	57
27	<b>17.</b>	<b>AAA IMPLICATIONS .....</b>	<b>58</b>
28	17.1	3GPP AAA (Informative) .....	58
29	17.2	WiMAX AAA Proxy Requirements .....	58
30	17.2.1	Bi-directional translation between STa and STa+ .....	58
31	17.2.2	STa Support .....	58
32	17.2.3	Accounting .....	58
33	<b>18.</b>	<b>ACCOUNTING IMPLICATIONS .....</b>	<b>59</b>
34	18.1	Charging requirements - no PCC framework .....	59
35	18.2	PCC Charging Requirements at the ASN-GW .....	59
36	<b>19.</b>	<b>WNAADA+ DESCRIPTION .....</b>	<b>60</b>
37	19.1	General .....	60
38	19.2	Diameter Capability Negotiation .....	60
39	19.3	WNAADA+ Access Authentication and Authorization .....	60
40	19.3.1	General .....	60
41	19.3.2	Handling WiMAX Subscriber QoS Profile Information .....	61
42	19.3.3	WNAADA+ WiMAX® Diameter-EAP-Request/Answer Commands .....	62
43	19.3.4	WiMAX AAA Proxy/Server STa to STa+ Translation Requirements .....	64
44	19.4	Commands for WNAADA+ HSS/AAA Initiated Detach .....	67
45	19.4.1	Abort-Session-Request (ASR) Command .....	67
46	19.4.2	Abort-Session-Answer (ASA) Command .....	67

1	19.4.3	Session-Termination-Request (STR) Command .....	68
2	19.4.4	Session-Termination-Answer (STA) Command .....	68
3	19.5	Commands for Re-Authentication and Re-Authorization Procedure .....	68
4	19.5.1	Re-Auth-Request (RAR) Command.....	68
5	19.5.2	Re-Auth-Answer (RAA) Command .....	68
6	19.5.3	AA-Request (AAR) Command.....	69
7	19.5.4	AA-Answer (AAA) Command .....	69
8			
9			

1 **List of Figures**

2 FIGURE 5-1 – 3GPP-WIMAX NON-ROAMING ARCHITECTURE ..... 11  
3 FIGURE 5-2 – 3GPP-WIMAX® ROAMING ARCHITECTURE - HOME ROUTED ..... 12  
4 FIGURE 5-3 – 3GPP-WIMAX® ROAMING ARCHITECTURE (CHAINED PMIP-BASED S8 + S2A) - HOME  
5 ROUTED ..... 13  
6 FIGURE 5-4 – 3GPP-WIMAX® ROAMING ARCHITECTURE– LOCAL BREAKOUT ..... 14  
7 FIGURE 7-1 – ARCHITECTURE FOR ANDSF ..... 17  
8 FIGURE 8-1 – INITIAL ATTACHMENT WITH 3GPP EPC OVER S2A (PMIP6) ..... 18  
9 FIGURE 8-2 – INITIAL ATTACHMENT WITH 3GPP EPC OVER S2A (CMIP4) ..... 20  
10 FIGURE 9-1 – MS/UE INITIATED DETACH PROCEDURE OVER S2A (PMIP6) ..... 22  
11 FIGURE 9-2 – MS/UE INITIATED DETACH PROCEDURE OVER S2A (CMIP4) ..... 24  
12 FIGURE 9-3 – ASN-GW/BS INITIATED DETACH PROCEDURE OVER S2A (PMIP6) ..... 26  
13 FIGURE 9-4 – HSS/AAA INITIATED DETACH PROCEDURE OVER S2A (PMIP6) ..... 29  
14 FIGURE 9-5 – ASN-GW/BS INITIATED DETACH PROCEDURE OVER S2A (CMIP4) ..... 30  
15 FIGURE 9-6 – HSS/AAA INITIATED DETACH PROCEDURE OVER S2A (CMIP4) ..... 32  
16 FIGURE 13-1 – HANDOVER FROM 3GPP ACCESS TO WIMAX® WITH PMIP6 ON S2A ..... 37  
17 FIGURE 13-2 – 3GPP IP ACCESS TO WIMAX® HANDOVER WITH CMIP4 ON S2A ..... 39  
18 FIGURE 14-1 – PDN-GW INITIATED RESOURCE DEACTIVATION (PMIP6) ..... 41  
19 FIGURE 15-1 – NETWORK-INITIATED DYNAMIC PCC PROCEDURE ..... 43  
20 FIGURE 15-2 – MS-INITIATED DYNAMIC PCC PROCEDURE ..... 44  
21 FIGURE 15-3 – INTRA WIMAX BBERF RELOCATION FOR PMIPV6 ..... 46  
22 FIGURE 15-4 – INTRA WIMAX BBERF RELOCATION FOR CMIPV4 ..... 47  
23 FIGURE 19-1 – WIMAX QOS PROFILE RETRIEVAL FROM THE WIMAX AAA PROXY SERVER ..... 61  
24

---

## 1. Introduction and Document Scope

3GPP Technical Specification 23.402 [4] specifies the stage 2 service description for providing IP connectivity using non-3GPP IP accesses (e.g. WLAN, WiMAX, HRPD etc.) to the 3GPP EPS. TS 23.402 [4] covers both roaming and non-roaming scenarios and covers all aspects related to the usage of non-3GPP IP accesses, including mobility between 3GPP and non-3GPP wireless access networks, policy control and charging, and authentication.

This document specifies Stage 2 & 3 specifications for interworking between Mobile WiMAX® and Release 9 3GPP Evolved Packet System (EPS). The purpose of this document is to identify the requirements and impacts to the WiMAX network for interworking with 3GPP EPS and not to duplicate the content of TS 23.402 [4].

This specification assumes that the mobile terminal can operate in dual-radio mode i.e. both radios can transmit and receive simultaneously. Single-Radio operation will be covered in a separate specification. This specification also assumes that a dual mode mobile terminal is connected to a common 3GPP Core (EPC) via WiMAX ASN. Scenario where dual mode mobile terminal is connected to a common WiMAX Core (CSN) via 3GPP access is not supported.

---

## 2. Abbreviations and Definitions

### 2.1 Abbreviations

For the purposes of the present document, following abbreviations apply

4	PMIP6	Proxy Mobile IP version 6
5	EPC	Evolved Packet Core
6	EPS	Evolved Packet System
7	S-GW	Serving Gateway
8	PDN-GW	PDN Gateway
9	ANID	Access Network Identity
10	MAG	Mobile Access Gateway
11	UE	User Equipment
12	PLMN	Public Land Mobile Network
13	IP-CAN	IP Connection Access Network
14	PCC	Policy and Charging Control
15	PCRF	Policy and Charging Rule Function
16	PCEF	Policy and Charging Enforcement Function
17	hPCRF	home PCRF
18	vPCRF	visited PCRF
19	BBERF	Bear Binding and Event Report Function
20	DRA	Diameter Routing Agent
21	MCC	Mobile Country Code
22	MNC	Mobile Network Code
23	CDR	Charging Data Record
24		

### 2.2 Terms & Definitions

**Dual Radio Handover:** In dual radio handovers *both* radios can be ON (can be simultaneously receiving and transmitting) at any given time during the handover process.

---

## 3. References

- 1 [1] WMF-T33-001-R016v01, WiMAX Forum® Network Architecture Detailed Protocols and Procedures,  
2 Base Specification.
- 3 [2] WMF-T33-109-R016v01, WiMAX Forum® Network Architecture Detailed Protocols and Procedures,  
4 Policy and Charging Control
- 5 [3] 3GPP TS 23.401, 3rd Generation Partnership Project, Technical Specification Group Services and System  
6 Aspects, "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio  
7 Access Network (E-UTRAN) access (Release 9)".
- 8 [4] 3GPP TS 23.402, 3rd Generation Partnership Project, Technical Specification Group Services and System  
9 Aspects, "Architecture Enhancements for non-3GPP accesses (Release 9)".
- 10 [5] 3GPP TS 33.402, 3rd Generation Partnership Project, Technical Specification Group Services and System  
11 Aspects, "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses; (Release  
12 9)".
- 13 [6] IETF RFC 3344, "IP Mobility Support for IPv4".
- 14 [7] IETF RFC 3775, "Mobility Support in IPv6".
- 15 [8] 3GPP TS 23.203, 3rd Generation Partnership Project, Technical Specification Group Services and System  
16 Aspects, "Policy and Charging Control Architecture (Release 9)".
- 17 [9] 3GPP TS 24.302, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
18 Terminals, "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3  
19 (Release 9)".
- 20 [10] 3GPP TS 23.003, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
21 Terminals, "Numbering, Addressing and Identification".
- 22 [11] IETF RFC 3748, "Extensible Authentication Protocol (EAP)".
- 23 [12] 3GPP TS 24.312, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
24 Terminals, "Access Network Discovery and Selection Function (ANDSF) Management Object (MO);  
25 (Release 9)".
- 26 [13] IETF RFC 5826, "Binding Revocation for IPv6 Mobility".
- 27 [14] 3GPP TS 29.273, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
28 Terminals, Evolved Packet System (EPS), "3GPP EPS AAA interfaces (Release 9)".
- 29 [15] IETF RFC 2794, "Mobile IP network Access Identifier Extension for IPv4".
- 30 [16] IETF RFC 5448, "Improved Extensible Authentication Protocol Method for 3rd Generation  
31 Authentication and Key Agreement (EAP-AKA)".
- 32 [17] IETF RFC 4005, "Diameter Network Access Server Application"
- 33 [18] IETF RFC 4006, "Diameter Credit-Control Application"
- 34 [19] 3GPP TS 29.212, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
35 Terminals, "Policy and Charging Control over Gx reference point; (Release 9)".
- 36 [20] 3GPP TS 29.061, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
37 Terminals, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based  
38 services and Packet Data Networks (PDN)"
- 39

- 1 [21] 3GPP TS 29.213, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
2 Terminals, “Policy and Charging Control signalling flows and QoS parameter mapping; (Release 9)”.
- 3 [22] 3GPP TS 29.214, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
4 Terminals, “Policy and Charging Control over Rx reference point”
- 5 [23] 3GPP TS 29.229, 3rd Generation Partnership Project, Technical Specification Group Core Network, “Cx  
6 and Dx interfaces based on the Diameter protocol”
- 7 [24] 3GPP TS 29.272, 3rd Generation Partnership Project, Technical Specification Group Core Network and  
8 Terminals, Evolved Packet System (EPS), “Mobility Management Entity (MME) and Serving GPRS  
9 Support Node (SGSN) related interfaces based on Diameter protocol”
- 10 [25] 3GPP TS 32.240, 3rd Generation Partnership Project, Technical Specification Group Services and System  
11 Aspects, Telecommunication management, Charging management, “Charging architecture and principles:  
12 (Release 9)”.
- 13 [26] 3GPP TS 32.251, 3rd Generation Partnership Project, Technical Specification Group Services and System  
14 Aspects, Telecommunication management, Charging management, “Packet Switched (PS) domain  
15 charging: (Release 9)”.
- 16 [27] 3GPP TS 32.299, 3rd Generation Partnership Project, Technical Specification Group Services and System  
17 Aspects, Telecommunication management, Charging management, “Diameter charging applications”
- 18 [28] 3GPP2 X.S0057, 3rd Generation Partnership Project 2, “E-UTRAN - eHRPD Connectivity and  
19 Interworking: Core Network Aspects”
- 20 [29] WMF-T33-001-R020v01, WiMAX Forum Network Architecture Detailed Protocols and Procedures, Base  
21 Specification.
- 22 [30] IETF RFC 3588, “Diameter Base Protocol”.
- 23 [31] RFC 4072, Diameter Extensible Authentication Protocol (EAP) Application.
- 24 [32] RFC 5779, Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction  
25 with Diameter Server.
- 26 [33] 3GPP TS 24.303, 3rd Generation Partnership Project, Technical Specification Group Services and System  
27 Aspects, “Mobility management based on Dual-Stack Mobile IPv6 (Release 9)”.
- 28

---

## 1 **4. General Requirements and Principles**

2 General concepts for interworking between 3GPP accesses and WiMAX® networks as specified in section 4.1.2 of  
3 TS 23.402 [4] shall apply.

4 General principle for handovers with optimizations between 3GPP Accesses and Mobile WiMAX as specified in  
5 section 10.1.1 (General Principles) of TS 23.402 [4] shall also apply.

6 Note: The ASN-GW may generate accounting records when interworking with 3GPP EPC. For the accounting  
7 requirements and functions, please refer to section 18.

## 5. Interworking Network Reference Model

This section defines the Network Reference Model for the interworking the 3GPP Evolved Packet System (EPS) with the Mobile WiMAX® system defined in the TS 23.402 [4] as a Trusted Non-3GPP IP Access system.

The WiMAX ASN may be deployed directly by the 3GPP operator or by a WiMAX Operator which has a Contractual Agreement with the 3GPP operator to provide the ASN.

### 5.1 Non-Roaming Architecture

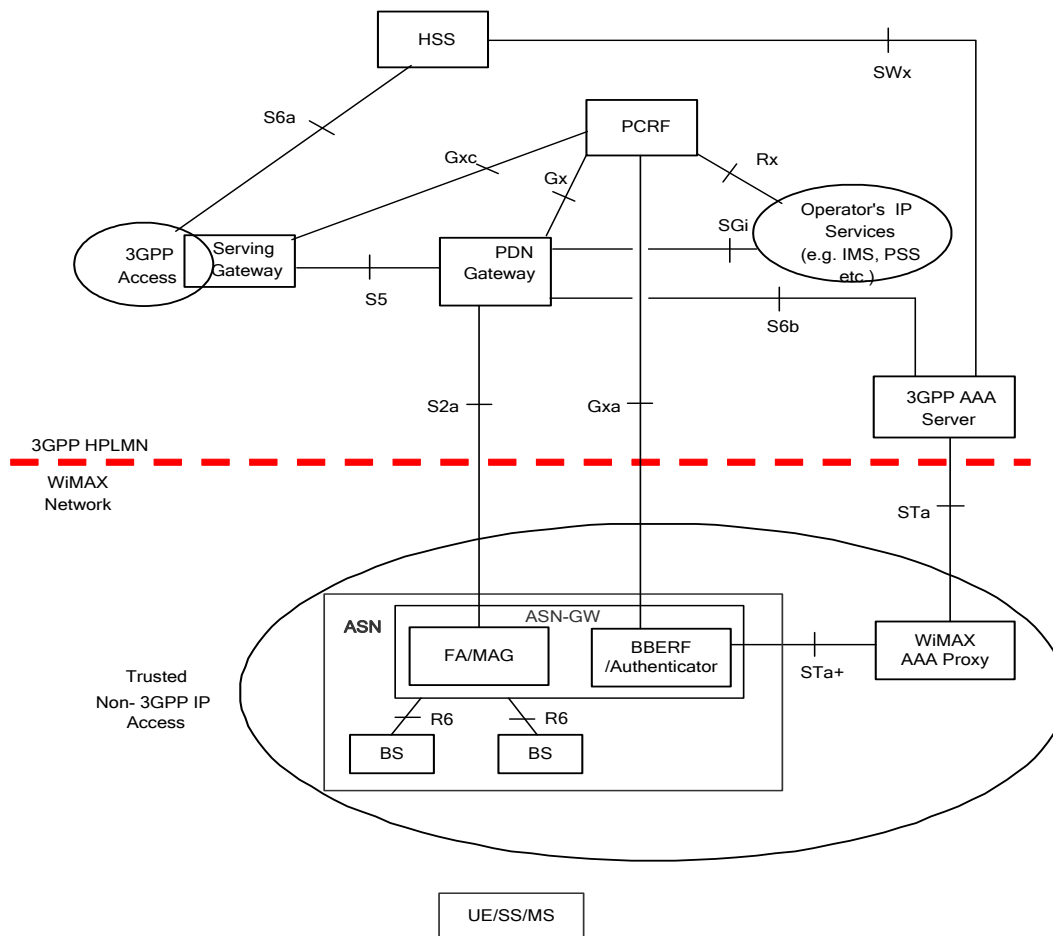
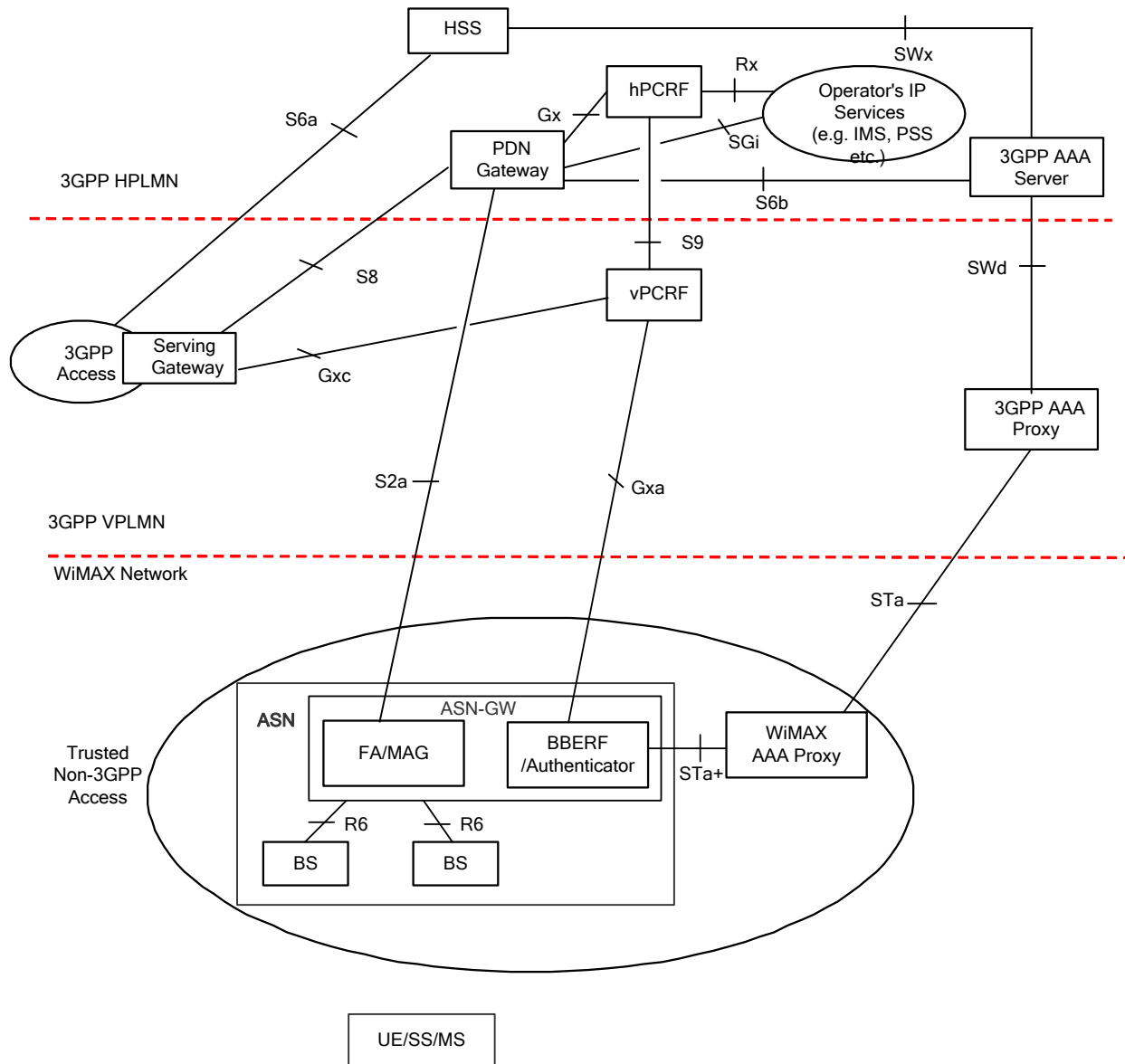


Figure 5-1 – 3GPP-WiMAX Non-Roaming Architecture

1 **5.2 Roaming Architecture**

2

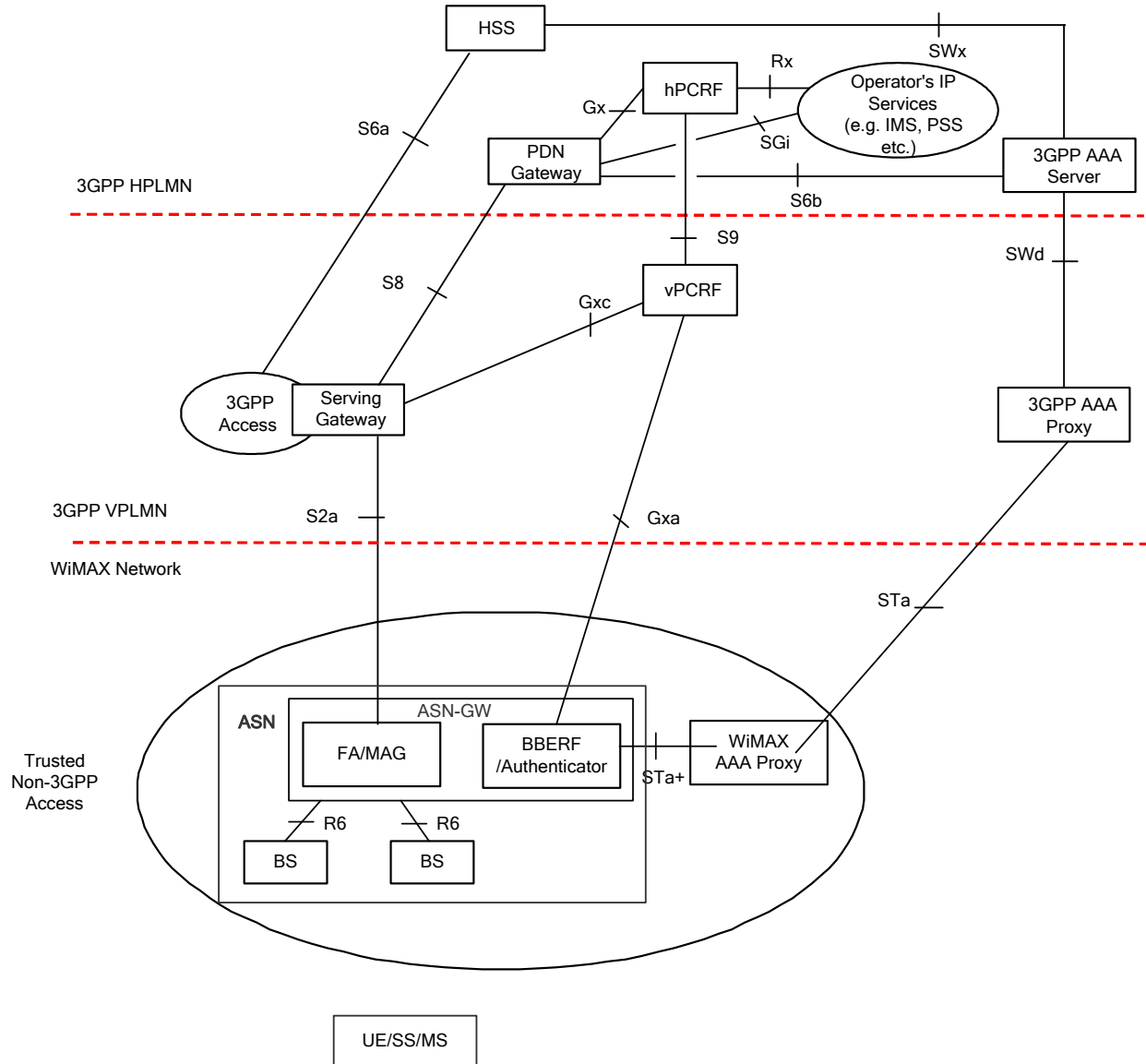


3

4

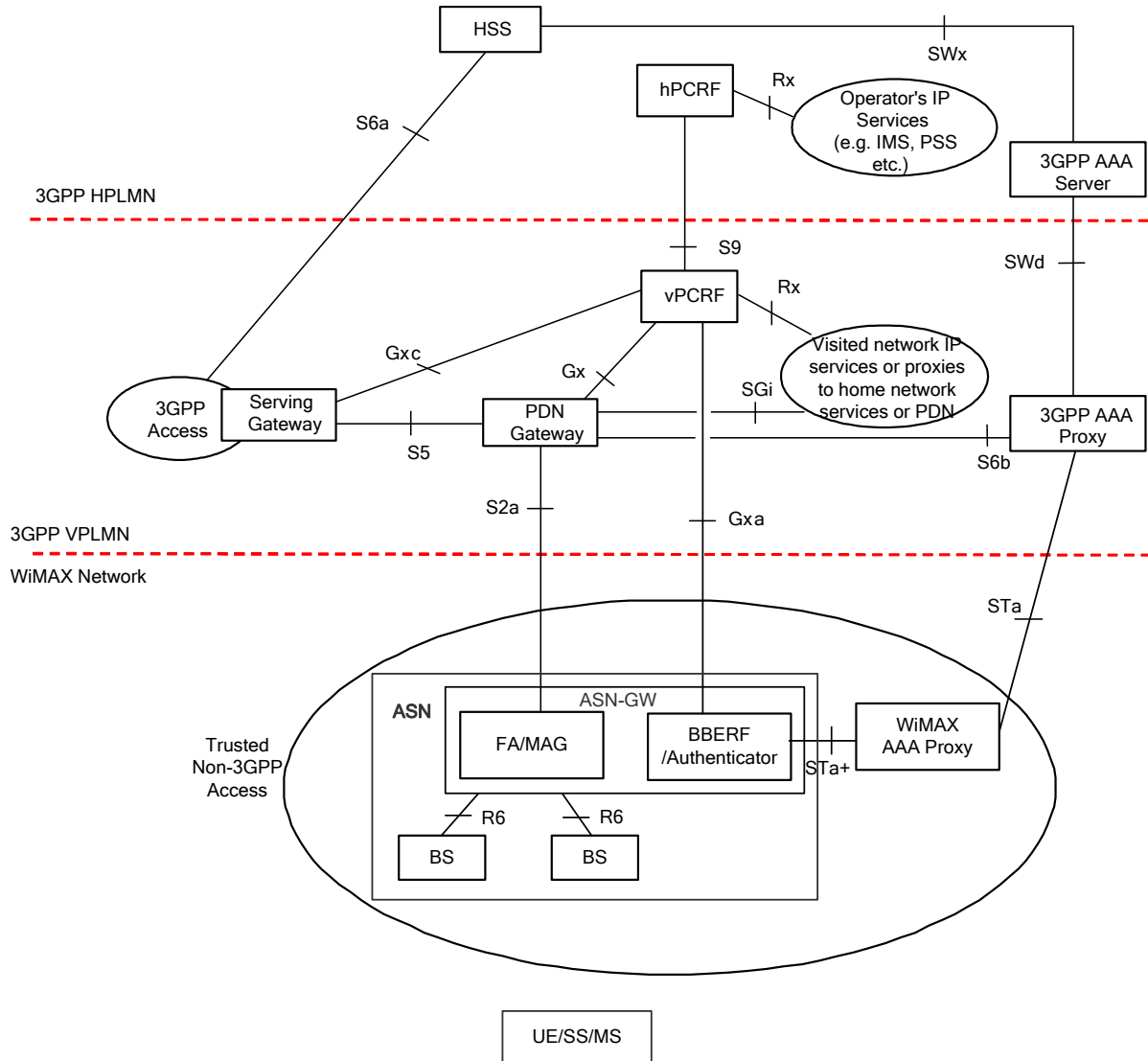
**Figure 5-2 – 3GPP-WiMAX® Roaming Architecture - Home Routed**

5



1  
 2  
 3

**Figure 5-3 – 3GPP-WiMAX® Roaming Architecture (Chained PMIP-based S8 + S2a) - Home Routed**



1

2

3

**Figure 5-4 – 3GPP-WiMAX® Roaming Architecture– Local Breakout**

4 Notes: In the above roaming and non-roaming scenarios and during the course of the WiMAX session, the S2a and  
 5 the Gxa Reference Points may terminate at two different ASN-GWs typically after MS/UE handovers where the  
 6 FA/MAG and the Anchor Authenticator/BBERF are separated.

### 5.3 Reference point mapping

The reference points relevant for interworking between the WiMAX® networks and 3GPP networks are described below:

S2a: This reference point provides the user plane and the related mobility management procedures between the WiMAX access network and 3GPP core network. It is defined between the Mobile Access Gateway (MAG) in WiMAX ASN-GW and 3GPP PDN Gateway. In the case when Mobile IPv4 is used as the S2a protocol, then the WiMAX side of this reference point SHALL be terminated by the MIP4 Foreign Agent function. This reference point is specified in 3GPP TS 23.402 [4].

The S2a reference point corresponds to the PMIP6 part of R3 reference point of WiMAX NRM [1].

Note: For Chained PMIP-based S8+S2a case as shown in Figure 5-3, the S2a interface is between WiMAX ASN-GW and 3GPP Serving GW. This scenario is shown in Figure 5-3 for reference but not supported in this version.

Gxa: This reference point is defined between the Policy and Charging Rule Function (PCRF) in the 3GPP EPC and the BBERF in the WiMAX ASN-GW. The PCRF provides QoS rules to the BBERF and receives event reports from the BBERF via this reference point. For roaming scenarios, this reference point is between the vPCRF and the BBERF. In WiMAX access network, this reference point is terminated at the ASN-GW containing the Anchor Authenticator and BBERF. The Gxa reference point specifications and requirements are provided in TS 23.203 [8] and TS 29.212 [19].

STa: This reference point is defined between the WiMAX AAA Proxy and the 3GPP AAA Server/Proxy function in the 3GPP Evolved Packet Core. It is used to carry the access authentication, authorization, QoS, and mobility information related to a specific subscriber. Stage 2 for STa reference point is defined in 3GPP TS 23.402 [4]. Stage 3 for STa reference point is defined in TS 29.273 [14].

STa+: This reference point is defined between the Anchor Authenticator function in the WiMAX ASN and the WiMAX AAA Proxy function. It is used to carry WiMAX specific attributes in addition to 3GPP AAA attributes define in STa [14]. The STa+ reference point is defined in section 19.

---

## 6. PDN-GW Selection

Note: This release of the specification only supports a single PDN connection – the default PDN connection. The PDN Type could be IPv4, IPv6 or IPv4v6.

The WiMAX® ASN shall be responsible for PDN-GW selection for the default PDN connection. The PDN-GW selection mechanism is defined in TS 23.402 [4], section 4.5.1 with following modification. The PDN-GW selection is based on the following information received from the AAA/HSS:

- PDN-GW identifier information in the UE's subscription record for the default APN, which could be a logical name (FQDN) or IP address.

If the PDN-GW identifier is available and the value is an IP address, the WiMAX ASN shall use this IP address received from AAA/HSS as part of access authentication as the PDN-GW's IP address for the default PDN connection.

If the PDN-GW identifier is available and it is a FQDN, the WiMAX ASN shall perform DNS resolution using that FQDN for PDN-GW address selection.

- APN information in the UE's subscription record if there is no PDN-GW identifier information present for the default APN.

If the PDN-GW identifier is not available, the WiMAX ASN shall perform DNS based PDN-GW address resolution for the default APN.

If the UE's subscription allows it to have a PDN-GW assignment in VPLMN, the HSS record shall indicate that to the WiMAX ASN. If allowed, the WiMAX ASN can select a PDN-GW in the VPLMN. This selection can be based on static configuration in the WiMAX ASN or using APN. If the WiMAX ASN cannot derive a PDN-GW address in the VPLMN, it shall use the APN information to resolve a PDN-GW address in the HPLMN.

---

## 7. Access Network Discovery and Selection

### 7.1 Access Network Discovery and Selection Function (ANDSF)

The ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data as per operator's policy. The ANDSF is able to initiate data transfer to the MS/UE, based on network triggers, and respond to requests from the MS/UE.

The detailed functionality for ANDSF is defined in section 4.8.2 of TS 23.402 [4]. ANDSF discovery shall be done as per section 4.8.4 of TS 23.402 [4].

#### 7.1.1 Architecture for ANDSF

The following architecture shall be used for access network discovery and selection using ANDSF. Details of communication over S14 are specified in section 6.8 of TS 24.302 [9].

Note: ANDSF is a 3GPP Rel-8 specified network element that exists in the hPLMN of the 3GPP EPC.



Figure 7-1 – Architecture for ANDSF

#### 7.1.2 ANDSF Management Objects

General ANDSF Management Objects parameters and Management Objects for WiMAX® networks are defined in 3GPP TS 24.312 [12].

## 8. Initial Attach to 3GPP EPC via WiMAX® ASN

### 8.1 Initial Attach Procedure with PMIP6 on S2a

Initial Attach Procedure with PMIP6 over S2a for home routed (anchoring at PDN-GW) and non-roaming, roaming, and local break-out are defined in Section 6.2.1 of TS 23.402 [4]. The initial attach procedure with PMIP6 on chained S2a and PMIP based S8 is defined in Section 6.2.4 of TS 23.402 [4]. WiMAX® specific triggers and procedures for home routed PMIP6 on S2a are highlighted below.

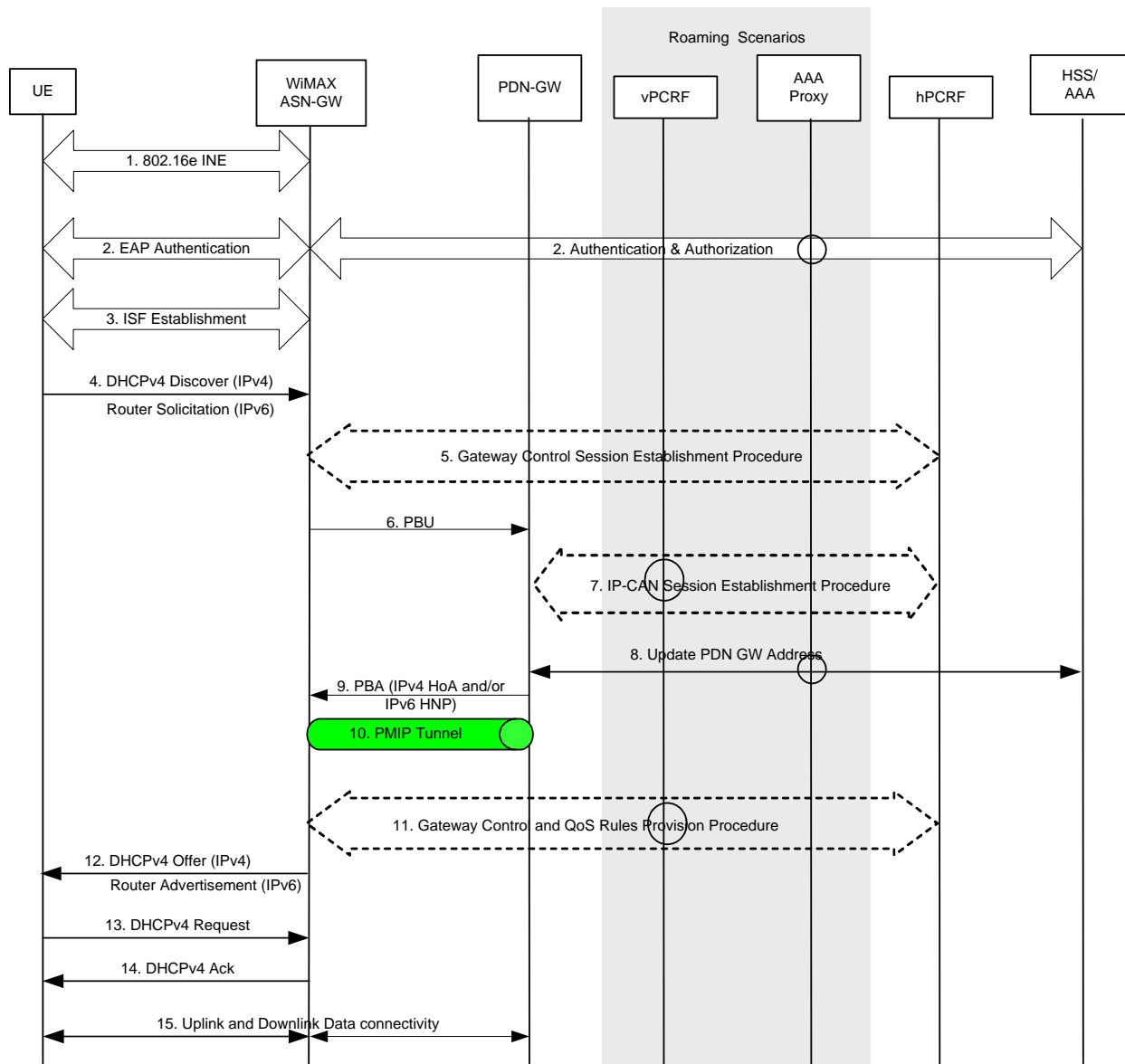


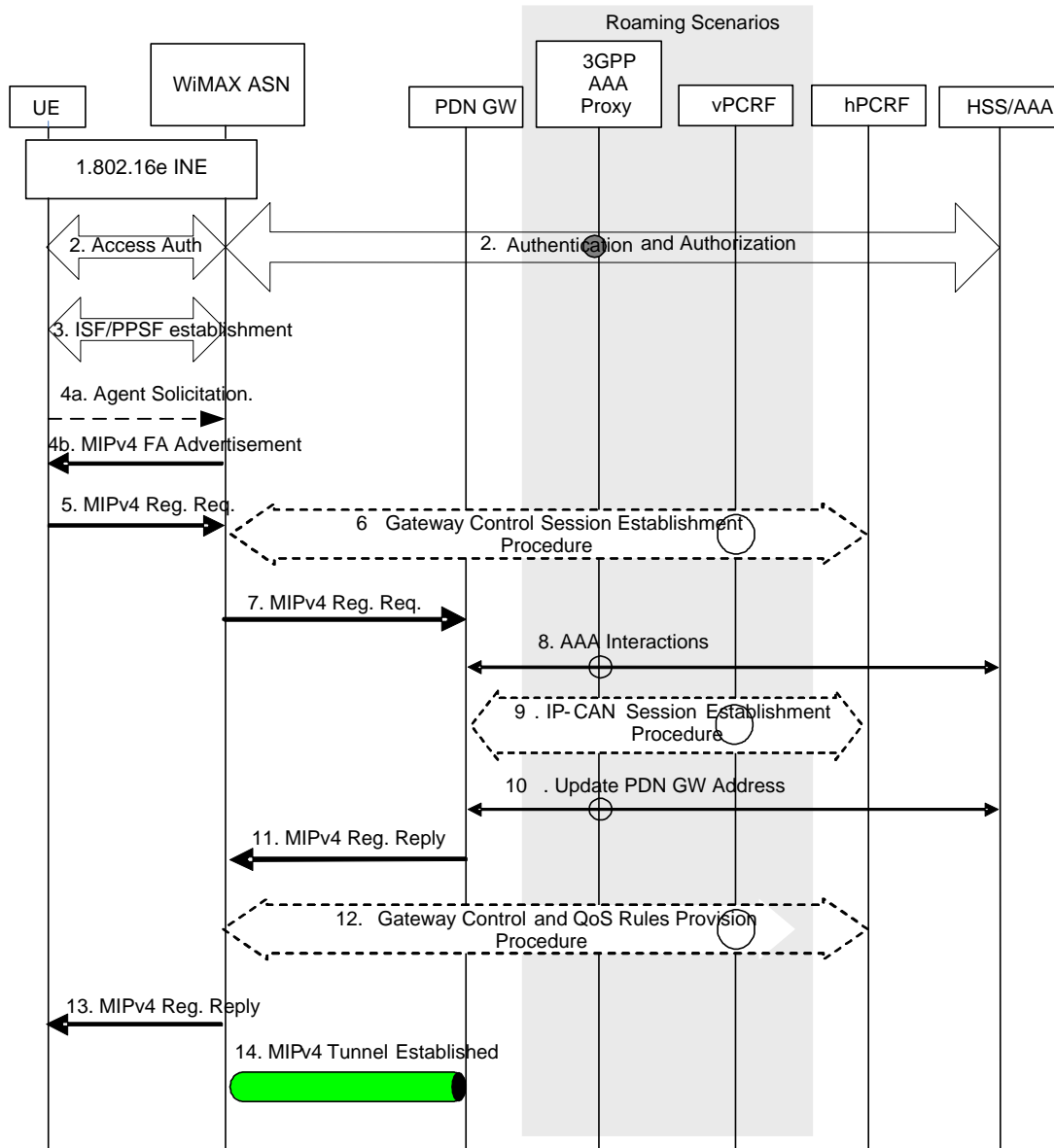
Figure 8-1 – Initial attachment with 3GPP EPC over S2a (PMIP6)

- 1 The optional interaction steps (5, 7, 11) between the ASN and PDN gateways and the PCRF in the procedures only  
2 occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in each gateway.  
3 The vPCRF and the AAA-Proxy are only involved in roaming and local break-out scenarios.
- 4 1) The initial WiMAX network entry procedures are performed up to the point where EAP authentication is  
5 triggered as defined in WiMAX NWG specification [1].
  - 6 2) The EAP authentication procedure is initiated and performed involving the MS/UE. Details of EAP based  
7 access authentication procedure is specified in section 10.1. The PDN Gateway address is determined at this  
8 point as described in section 4.5.1 of TS 23.402.
- 9 Note: ASN-GW knows that it is connecting to 3GPP EPC based on static pre-configuration
- 10 Note: Device Authentication based on X.509 certificates is not applicable.
- 11 3) After successful authentication and authorization, the ASN will try to establish the Initial Service Flow(s) to  
12 the MS/UE according to the authorized PDN type downloaded during access authentication. If IPv4v6 is  
13 authorized, the ASN will try to establish one IPv4 ISF and one IPv6 ISF. The MS/UE may reduce the ISFs to  
14 only the PDN type, IPv4 or IPv6 it supports.
  - 15 4) The MS/UE initiates either DHCPv4 for IPv4 or RS for IPv6 addressing or both for default PDN connection.  
16 The attach will always be treated as “Initial Attach”.
  - 17 5 -11) Steps 5 to 11 are the same as defined under section 6.2.1 of TS 23.402 [4] with following additional  
18 clarification. The PDN Type sent in PBU will be set to the type of ISFs established between the ASN and the  
19 MS/UE in step 4, i.e., IPv4, IPv6 or IPv4v6. The requested IP address type will be set corresponding to the  
20 PDN Type. If the PDN Type is IPv4, the requested IP address is IPv4 HoA. If PDN Type is IPv6, the  
21 requested IP address is IPv6 HNP. If the PDN Type is IPv4v6, both IPv4 HoA and IPv6 HNP are requested.  
22 In Step 8 the PDN-GW authorizes the user with the AAA in addition to updating its address.
- 23 The protocol configuration parameters in PCO are set and used according to the following clarification:
- 24 If the ASN is configured to support DHCP proxy, the PCO in PBU will contain additional protocol  
25 configuration parameters necessary for MS/UE IP stack configuration. These parameters may include DNS  
26 server or P-CSCF server, depending on what MS/UE has asked for in DHCPDISCOVER message. The  
27 ASN is also responsible to translate the configuration parameters received from PCO in PBA sent by the  
28 PDN-GW, into the DHCPOFFER and DHCPACK messages sent to the MS/UE. For IPv6 MS/UE, these  
29 parameters need to be sent in PCO even if they are not received in RS. IPv6 MS/UE will use stateless  
30 DHCPv6 for parameter configuration after it has configured IPv6 address using SLAAC. In this case, the  
31 ASN is responsible to translate the configuration parameters received from PCO into the DHCPv6 Reply  
32 message.
- 33 If the ASN is configured to support DHCP relay, configuration parameters need not be included in PCO.  
34 They are provided by the PDN-GW after PMIP tunnel establishment, when the ASN will relay the DHCP  
35 message to the PDN-GW. The PDN-GW acts as a DHCP server and provides all requested configuration  
36 parameters.
- 37 Step 5, 7 and 11 are performed if PCC is deployed. DRA function may be involved for PCRF discovery  
38 and selection in step 5 and 7 to ensure the same PCRF will be selected by the ASN-GW/BBERF and PDN-  
39 GW as described in section 15.3.6.
- 40 12) ASN-GW sends the DHCPv4 offer to MS/UE with assigned MN-HoA or RA with assigned IPv6 HNP.
  - 41 13 - 14) MS/UE complete the DHCP procedure configuring the previously offered IP address. Steps 13 and 14  
42 apply for IPv4 address allocation case only.
  - 43 15) IP connectivity between the MS/UE and the PDN-GW for default PDN connection is set for uplink and  
44 downlink directions.

1 **8.2 Initial Attach Procedure with CMIP4 on S2a**

2 Initial Attach Procedure with CMIP4 over S2a is defined in Section 6.2.3 of TS 23.402 [4]. WiMAX specific  
3 triggers and procedures are highlighted below.

4



5

6 **Figure 8-2 – Initial attachment with 3GPP EPC over S2a (CMIP4)**

7

8 When the Attach procedure occurs in the Non-Roaming case, the vPCRF is not involved. The optional interaction  
9 steps (6, 9, 12) between the ASN & PDN gateways and the PCRF in the procedures only occur if dynamic policy  
10 provisioning is deployed. Otherwise policy may be statically configured with the each gateway.

- 11 1) The initial WiMAX network entry procedures are performed up to the point where EAP authentication is  
12 triggered as defined in WiMAX NWG specification [1].

- 1       2) The EAP authentication procedure is performed as per section 10.1. The PDN-GW information is returned  
2       from the 3GPP AAA Server to the Authenticator at this point. The 3GPP AAA Server also returns to the  
3       Authenticator the MN NAI (permanent IMSI based MN NAI) to be used to identify the UE in Gateway  
4       Control Session Establishment messages (step 6).
- 5       After the successful authentication, both UE and AAA derive the MIP-RK, SPI, and other mobility keys such  
6       as FA-RK, MN-FA, MN-HA-CMIP4 that will be used for the security protection in CMIP4 registration  
7       messages.
- 8       3) After successful authentication and authorization, an Initial Service Flow (ISF) and/or the Pre-provisioned  
9       Service Flows (PPSF) are established for the MS/UE within the ASN.
- 10      4) The FA in WiMAX ASN sends a Foreign Agent Advertisement (FAA) message to the MS/UE. The FAA  
11      message includes the Care-of Address (CoA). The MS/UE sends an Agent Solicitation to FA if the MS/UE  
12      doesn't receive FAA message after successful ISF establishment.
- 13      5) The MS/UE sends a Registration Request (RRQ) message to the FA as specified in RFC 3344 [6]. The NAI  
14      included in the RRQ shall be a permanent IMSI based MN NAI. The MS/UE sets the HA address field to  
15      ALL\_ZERO\_ONE address and it is updated when the Registration Reply is received from the FA.
- 16      The Authentication Extension in the RRQ should be calculated using keys derived in the step 2.
- 17      6-12) Steps 6 to 12 are exactly same as defined under section 6.2.3 of TS 23.402 [4].
- 18      Note: The selected PDN-GW obtains Authentication and Authorization information from the AAA/HSS at  
19      step 8.
- 20      Step 6, 9 and 12 are performed if PCC is deployed. DRA function may be involved for PCRF discovery and  
21      selection in step 6 and 9 to ensure the same PCRF will be selected by the ASN-GW/BBERF and PDN-GW as  
22      described in section 15.3.6.
- 23      13)The FA processes the RRP (MN-NAI, Home Address, Home Agent Address) according to RFC 3344 [6] and  
24      sends a corresponding RRP message to the MS/UE.
- 25      14) IP connectivity from the MS/UE to the PDN-GW is now setup. A MIP tunnel is established between the FA  
26      in the ASN-GW and the PDN-GW.

## 9. Detach Procedure

### 9.1 MS/UE initiated detach procedure

#### 9.1.1 MS/UE initiated detach procedure using PMIP6

Figure 9-1 presents MS/UE initiated detach procedure over S2a (PMIP6). The optional interactions between PCRF and PCEF/BBERF only occur if the PCC is deployed.

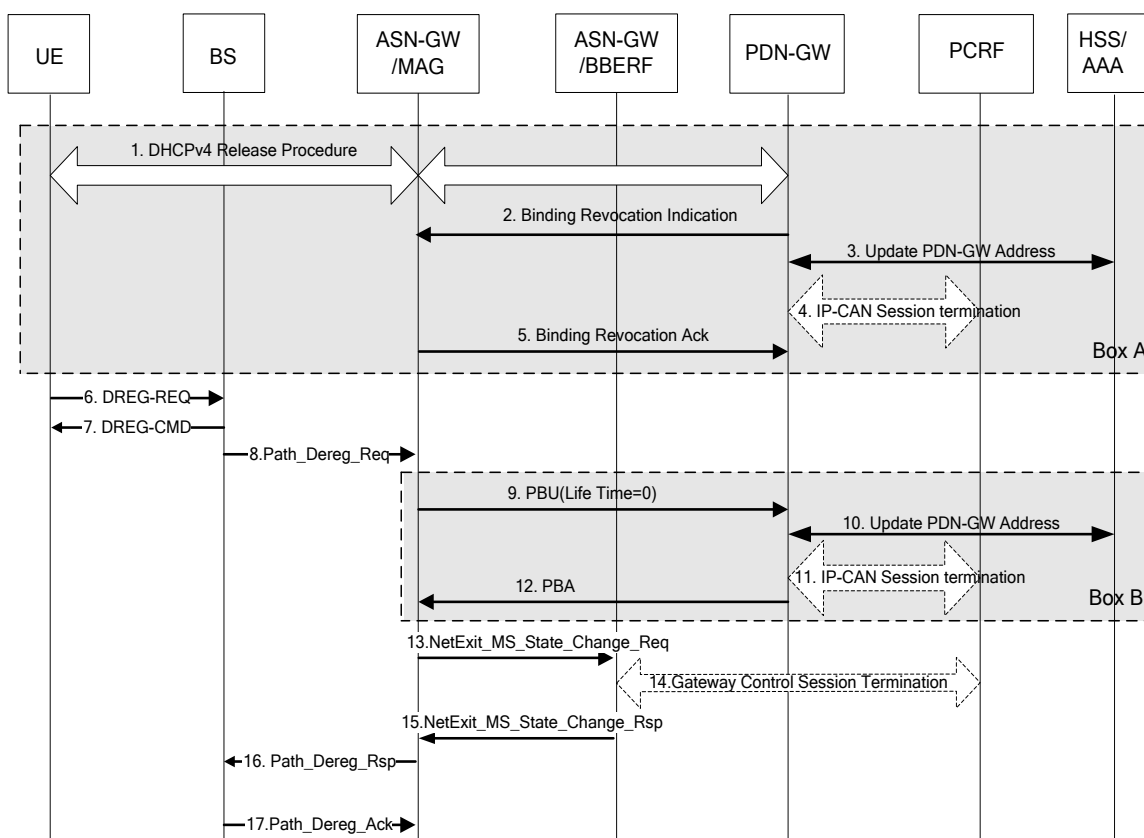


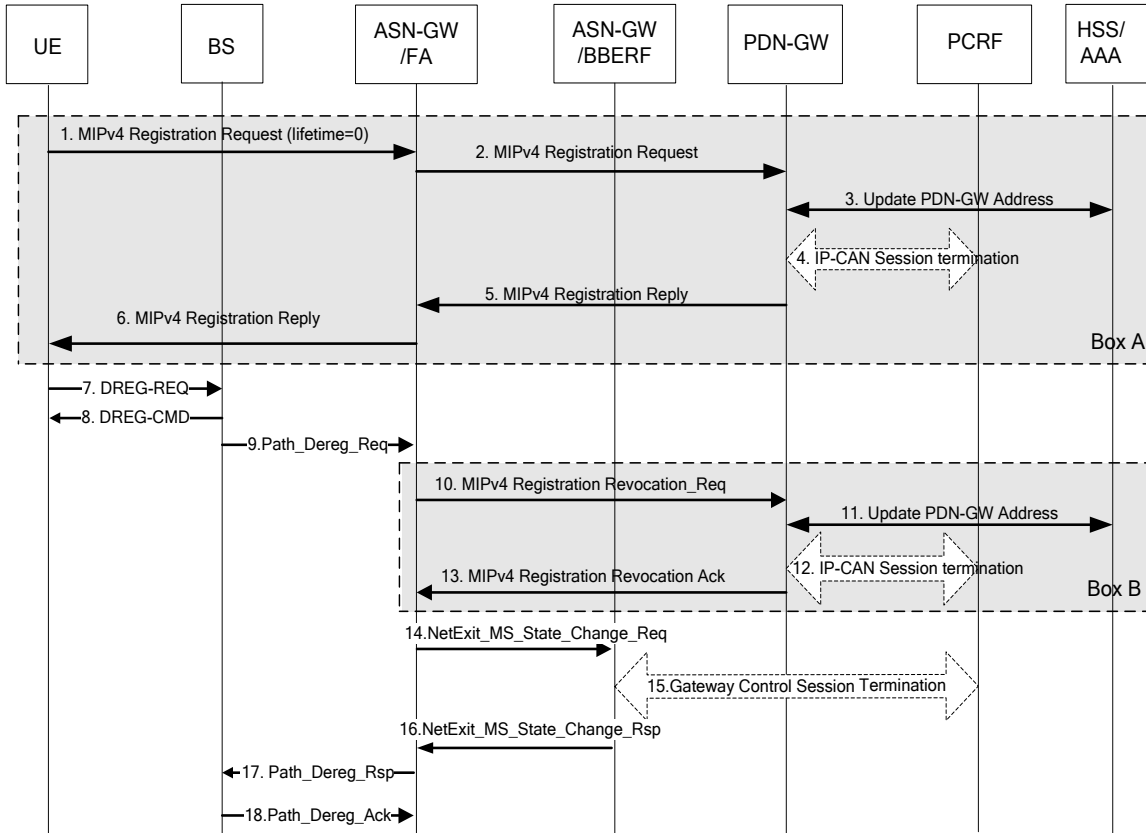
Figure 9-1 – MS/UE Initiated Detach Procedure over S2a (PMIP6)

- 1) MS/UE may initiate DHCPv4 Release Procedure in case of PMIP6 connection setup with DHCPv4. For IPv6 case, there is no DHCPv6 release procedure for the case of PMIP6 connection setup with stateless auto-configuration.
- 2) If the DHCPv4 Release is performed in step 1, the PDN-GW sends a Binding Revocation Indication message with Revocation Trigger field set to “8” i.e. User Initiated Session(s) Termination to Mobile Access Gateway (MAG) as defined in RFC 5826 [13].
- 3) Then the PDN-GW updates the PDN GW identity information corresponding to the UE's PDN connection in the AAA Server/HSS. This identity information is de-registered from the HSS as described in subclause 6.4.1.1 of TS 23.402 step 4 [4].

- 1 4) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in clause 7.3 of  
2 TS 23.203 [8].
- 3 5) The MAG returns a *Binding Revocation Acknowledgement* message to the PDN GW.
- 4 Note: Steps 1 to 5 in Box A occur for the case ASN-GW acts as a DHCP Relay.
- 5 6) MS/UE initiates detach procedure by sending a *DREG\_REQ* message with De-Registration Request  
6 Code=0x00 to BS.
- 7 7) BS sends *DREG\_CMD* message to the MS/UE with Action code=0x04.
- 8 8) BS sends *Path\_Dereg\_Req* message over R6 to the ASN-GW.
- 9 9) Upon receipt of a *Path\_Dereg\_Req* message over R6, if the MS/UE did not already perform a DHCPv4  
10 Release procedure in step 1, then the ASN-GW SHALL trigger MIP tunnel Release procedure with the PDN-  
11 GW by sending a PBU message with lifetime value set to “0”.
- 12 10) The PDN GW informs the AAA Server/HSS to remove the PDN GW identity information as described in  
13 step 3.
- 14 11) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as described in step 4.
- 15 12) The PDN GW deletes all existing entries implied in the *Proxy Binding Update (PBU)* message from its  
16 Binding Cache and sends a *Proxy Binding Ack (MN NAI, lifetime=0)* message to the MAG.
- 17 Note: Steps 9 to 12 in Box B occur for the case ASN-GW acts as a DHCP Proxy.
- 18 13) The ASN-GW/MAG sends a *NetExit\_MS\_State\_Change\_Req* message to notify the ASN-GW/Anchor  
19 Authenticator to delete the MS/UE contexts.
- 20 14) The ASN-GW/BBERF/Anchor Authenticator initiates the gateway control session termination procedure as  
21 defined in clause 7.7.2 of TS 23.203 [8].
- 22 15) The ASN-GW/Anchor Authenticator responds to the ASN-GW/MAG with a *NetExit MS State Change\_Rsp*  
23 message.
- 24 16) The ASN-GW sends a *Path\_Dereg\_Rsp* message over R6 to the BS.
- 25 17) BS sends *Path\_Dereg\_Ack* over R6 to the ASN-GW.

### 9.1.2 MS/UE initiated detach procedure using CMIP4

Figure 9-2 presents MS/UE initiated detach procedure over S2a (CMIP4).



**Figure 9-2 – MS/UE Initiated Detach Procedure over S2a (CMIP4)**

- 1) MS/UE may perform MIPv4 Registration Request (lifetime=0).

Note: Step 1 is expected to be performed by the MS/UE however in some cases the MS/UE may directly execute step 7 by sending *DREG-REQ*.

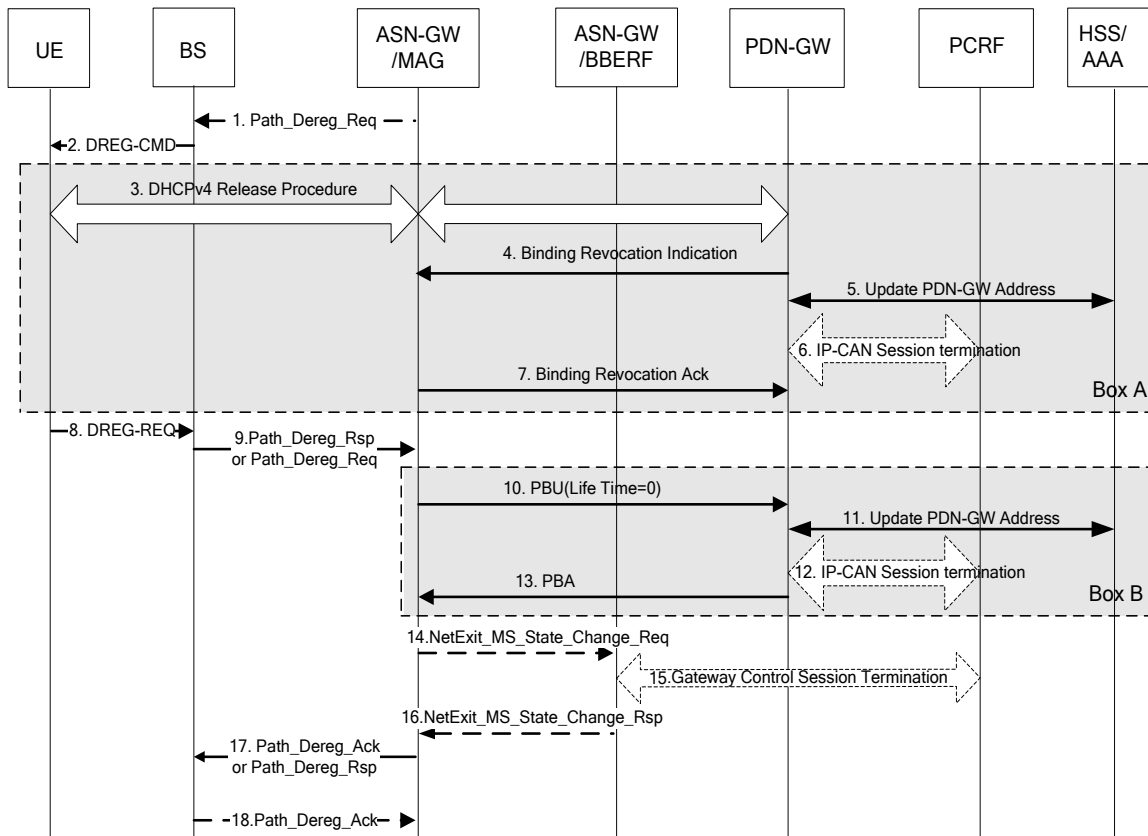
- 2) ASN-GW sends MIPv4 Registration Request (lifetime=0) over S2a to PDN-GW.
- 3) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to the UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS23.402 [4].
- 4) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in clause 7.3 of TS 23.203 [8].
- 5) The PDN-GW deletes all existing entries implied in the Registration Request message from its Binding Cache and sends a Registration Reply to the ASN-GW.
- 6) The ASN-GW sends a Registration Reply (lifetime=0) to the MS/UE.
- 7) MS/UE initiates a detach procedure by sending a DREG\_REQ message with De-Registration Request Code=0x00 to BS.
- 8) BS sends DREG\_CMD message to the MS/UE with Action code=0x04.
- 9) BS sends *Path\_Dereg\_Req* message over R6 to the ASN-GW.

- 1       10) Upon receipt of a *Path\_Dereg\_Req* message over R6, if the MS/UE did not already perform MIP De-  
2       registration procedure in step 1, then the ASN-GW performs a MIP Revocation procedure (as shown under  
3       step 10 to 13 in Box B) by sending a Registration Revocation Req message to the PDN-GW.
- 4       11) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in  
5       step 3.
- 6       12) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as described in step 4.
- 7       13) The PDN-GW deletes all existing entries implied in the Registration Revocation Req message from its  
8       Binding Cache and sends a Registration Revocation Ack message to the ASN-GW.
- 9       14) The ASN-GW/FA sends *NetExit\_MS\_State\_Change\_Req* message to notify the ASN-GW/Anchor  
10       Authenticator to delete the MS/UE contexts.
- 11       15) The ASN-GW/ BBERF/Anchor Authenticator initiates the gateway control session termination procedure  
12       as defined in clause 7.7.2 of TS 23.203 [8].
- 13       16) The ASN-GW/Anchor Authenticator responds to the ASN-GW/FA with *NetExit\_MS\_State\_Change\_Rsp*  
14       message.
- 15       17) ASN-GW sends a *Path\_Dereg\_Rsp* message over R6 to the BS.
- 16       18) BS sends *Path\_Dereg\_Ack* over R6 to the ASN-GW.

## 9.2 Network initiated detach procedure

### 9.2.1 ASN-GW/BS initiated detach procedure using PMIP6

Figure 9-3 presents ASN-GW or BS initiated detach procedure over S2a (PMIP6). The ASN/ASN-GW typically initiates the detach procedure during administration graceful shutdown. The BS may initiate the detach procedure when it determines a loss of the link with the MS/UE.



**Figure 9-3 – ASN-GW/BS Initiated Detach Procedure over S2a (PMIP6)**

- 1) ASN-GW/MAG determines that MS/UE detach is required (i.e. administration reasons) and then initiates data path deregistration procedure by sending *Path\_Dereg\_Req* message over R6 to BS with Action Code TLV set to indicate MS/UE detach from the network.

Note: This step is only needed in case of ASN-GW initiated Detach.

Note: Alternate network exit procedure is also allowed using *NetExit\_MS\_State\_Change\_Req/Rsp* message from ASN-GW/Anchor Authenticator as specified in section 4.5.2.1.2.4 of NWG Stage 3 specification [1]. In this case, the ASN-GW/MAG sends *Path\_Dereg\_Req* message to the BS after receiving the trigger message from the ASN-GW/Anchor Authenticator.

- 2) BS sends DREG\_CMD message to the MS/UE including Action Code=0x00.

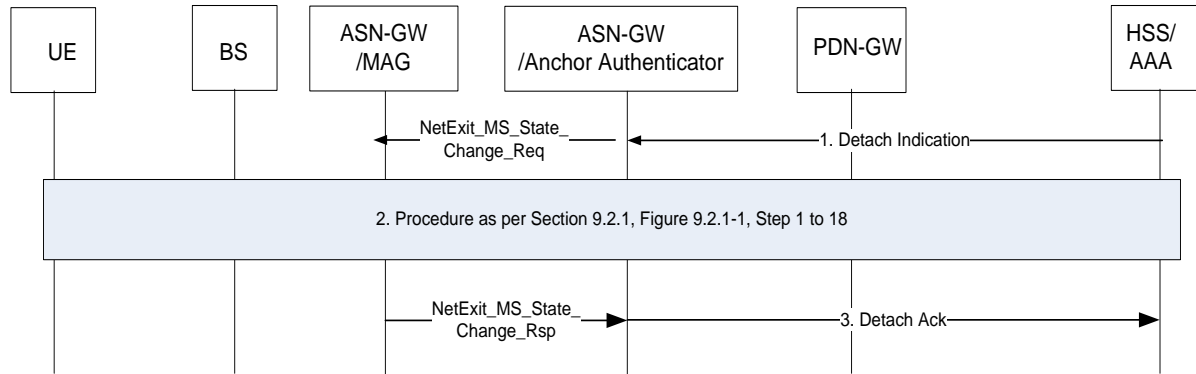
- 1 Note: This is the first step in the case of a BS initiated Detach.
- 2 3) The MS/UE may initiate DHCPv4 Release Procedure in case of PMIP6 connection setup with DHCPv4. For  
3 IPv6 case, there is no DHCPv6 release procedure for the case of PMIP6 connection setup with stateless auto-  
4 configuration.
- 5 4) If the DHCPv4 Release is performed in step 3, the PDN-GW sends a *Binding Revocation Indication* message  
6 with Revocation Trigger field set to “8” i.e. User Initiated Session(s) Termination to Mobile Access Gateway  
7 (MAG) as defined in RFC 5826 [13].
- 8 5) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to  
9 the UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS  
10 23.402 [4].
- 11 6) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in subclause 7.3  
12 of TS 23.203 [8].
- 13 7) The MAG returns a Binding Revocation Acknowledgement message to the PDN-GW.
- 14 Note: Steps 3 to 7 in the Box A occur in case ASN-GW acts as a DHCP Relay.
- 15 8) The MS/UE sends a *DREG\_REQ* message with De-Registration Request Code=0x02 to the BS.
- 16 9) For ASN-GW initiated Detach procedure, the BS sends *Path\_Dereg\_Rsp* message over R6 to the ASN-  
17 GW/MAG. Otherwise, for BS initiated Detach, the BS sends *Path\_Dereg\_Req* message over R6 to the ASN-  
18 GW in order to start tearing down the R6 data path.
- 19 10) Upon receiving either a *Path\_Dereg\_Rsp* or *Path\_Dereg\_Req* message over R6, if the MS/UE did not  
20 already perform DHCPv4 Release procedure in step 3, the ASN-GW triggers MIP tunnel Release procedure  
21 with the PDN-GW by sending PBU message with lifetime value set to “0”.
- 22 11) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in  
23 step 4 in subclause 6.4.1.1 of [4].
- 24 12) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in subclause 7.3  
25 of TS 23.203[7].
- 26 13) The PDN-GW deletes all existing entries implied in the Proxy Binding Update (PBU) message from its  
27 Binding Cache and sends a Proxy Binding Ack (MN NAI, lifetime=0) message to the MAG.
- 28 Note: The steps 10 to 13 in Box B occur when the ASN-GW acts as DHCP Proxy.
- 29 14) The ASN-GW/MAG sends *NetExit\_MS\_State\_Change\_Req* message to notify the ASN-GW/Anchor  
30 Authenticator to delete the MS/UE contexts. If the network detachment is initiated by the ASN-GW/Anchor  
31 Authenticator with *NetExit\_MS\_State\_Change\_Req* message as the first step (See step 1), the ASN-  
32 GW/MAG sends *NetExit\_MS\_State\_Change\_Rsp* message in this step to the ASN-GW/Authenticator as a  
33 response.
- 34 15) The ASN-GW containing the BBERF/Anchor Authenticator initiates a Gateway Control Session  
35 Termination procedure as defined in subclause 7.7.2 of TS 23.203 [8].
- 36 16) The ASN-GW/Anchor Authenticator responds to the ASN-GW/MAG with *NetExit\_MS\_State\_Change\_Rsp*  
37 message. This step is skipped if the network detachment is initiated by the ASN-GW/Anchor Authenticator  
38 (see step 1).
- 39 17) For ASN-GW initiated Detach, the ASN-GW/MAG sends a *Path\_Dereg\_Ack* message over R6 to the BS.  
40 Otherwise, for BS initiated Detach, the ASN-GW/MAG sends a *Path\_Dereg\_Rsp* message over R6 to the BS.
- 41 18) For BS initiated Detach, the BS sends a *Path\_Dereg\_Ack* message over R6 to the ASN-GW/MAG.

- 1 Note: For idle mode ungraceful network exit, step 10-16 in this figure are needed, and additional steps as described
- 2 in section 4.5.2.2.1 in stage 3 [1].

1 **9.2.2 HSS/AAA initiated detach procedure using PMIP6**

2 Figure 9-4 presents HSS/AAA initiated detach procedure over S2a (PMIP6). The HSS can initiate the procedure  
3 when the user's subscription is removed or access blocked and the 3GPP AAA Server can initiate the procedure per  
4 instruction from the O&M system or re-authentication timer expiry.

5



6

7 **Figure 9-4 – HSS/AAA Initiated Detach Procedure over S2a (PMIP6)**

8

9 1) The HSS/AAA sends a Detach Indication message to the Authenticator in the ASN-GW to detach a specific  
10 MS/UE.

11 Authenticator sends a *NetExit\_MS\_State\_Change\_Req* message over R4 to the MAG (Mobile Access  
12 Gateway)/Anchor DPF. The MAG/Anchor DPF initiates the Data Path termination and MIP de-registration  
13 corresponding to the MS/UE's connections.

14 If the Anchor Authenticator is located in the same ASN-GW with the MAG/Anchor DPF, the Anchor  
15 Authenticator can send a *Path\_Dereg\_Req* message over R6 to the BS directly.

16 2) This includes step 1 to 18 as in Figure 9-3.

17 3) The MAG/Anchor DPF of the ASN-GW responds to the Anchor Authenticator by sending a  
18 *NetExit\_MS\_State\_Change\_Rsp* message to confirm the Data Path termination and MIP de-registration. The  
19 Anchor Authenticator sends a *Detach Ack* message to the HSS/AAA.

20 If the Anchor Authenticator is located in the same ASN-GW with the MAG/Anchor DPF, the BS sends a  
21 *Path\_Dereg\_Rsp* message over R6 to the Anchor Authenticator directly.

### 9.2.3 ASN-GW/BS initiated detach procedure using CMIP4

Figure 9-5 presents an ASN-GW or BS initiated detach procedure over S2a (CMIP4). The ASN-GW typically initiates the detach procedure during administration graceful shut down. The BS initiates the detach procedure when it determines a loss of a link with the MS/UE.

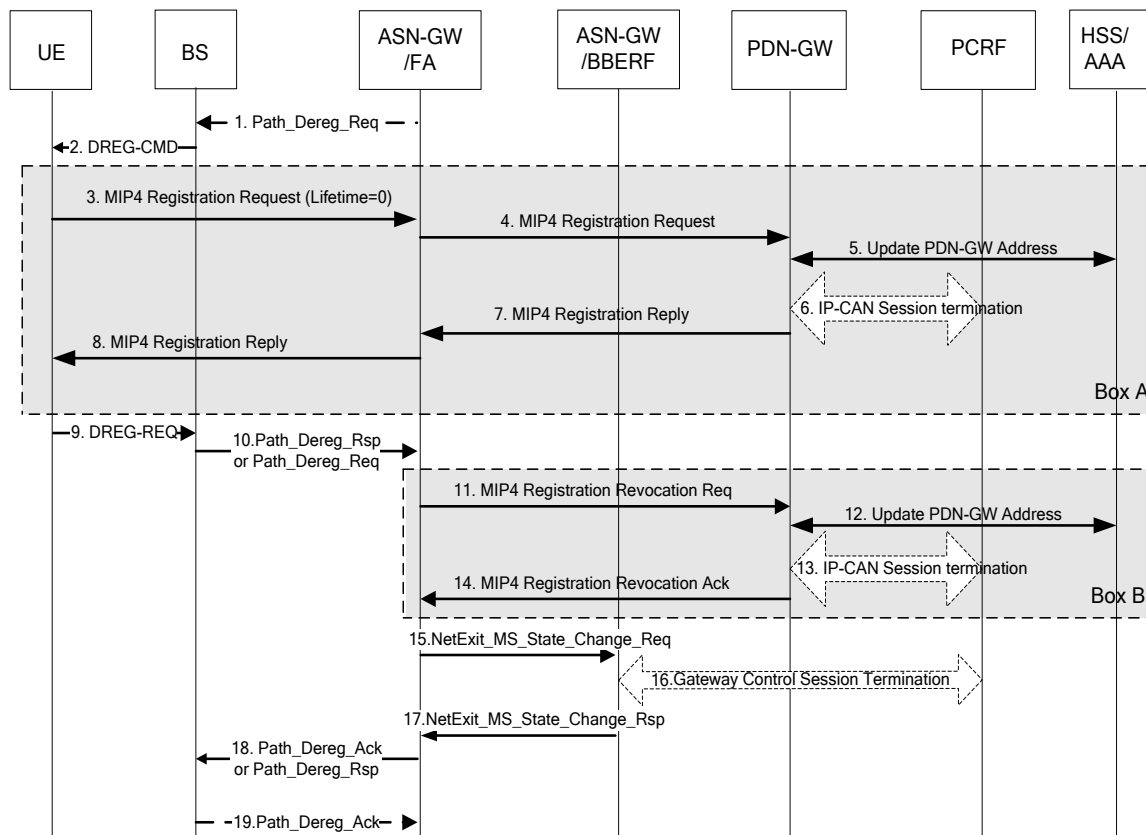


Figure 9-5 – ASN-GW/BS Initiated Detach Procedure over S2a (CMIP4)

- 1) The ASN-GW/FA determines that an MS/UE detach is required (e.g. administration reasons) and initiates data path deregistration procedure by sending *Path\_Dereg\_Req* message over R6 to the BS with Action Code TLV set to indicate MS/UE detach from the network.

Note: This step is only needed in case of ASN-GW initiated Detach.

Note: Alternate network exit procedure is also allowed using *NetExit\_MS\_State\_Change\_Req/Rsp* message from the ASN-GW/Anchor Authenticator as specified in subclause 4.5.2.1.2.4 of NWG Stage 3 specification [1]. In this case, the ASN-GW/FA sends a *Path\_Dereg\_Req* message to the BS after receiving the trigger message from the ASN-GW/Anchor Authenticator.

- 2) Either the BS determined that an MS/UE detach is required or triggered by the ASN-GW *Path\_Dereg\_Req* message, the BS sends a *DREG\_CMD* message to the MS/UE including Action Code=0x00.

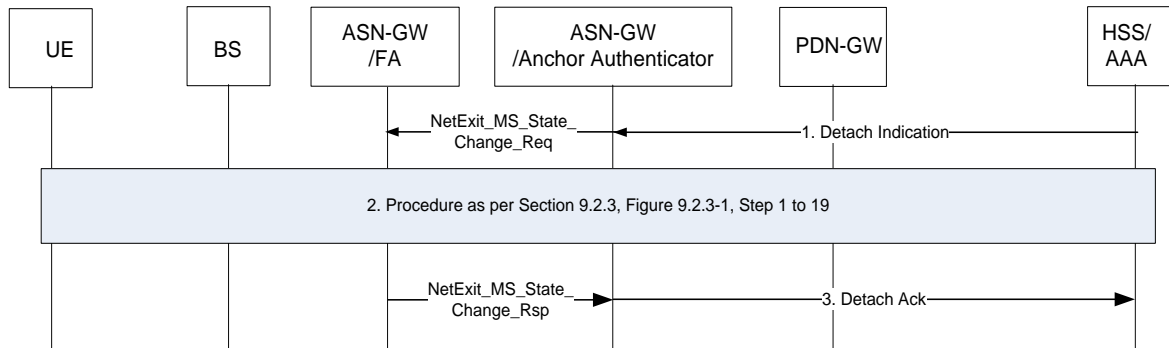
Note: This is the first step in the case of BS initiated Detach.

- 1 3) In the case of the illustrated Box A, the MS/UE performs Release Procedure by sending a *MIPv4 Registration*  
2 *Request* (lifetime=0) message.
- 3 4) The ASN-GW sends the *MIPv4 Registration Request* (lifetime=0) over S2a to PDN-GW.
- 4 5) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information corresponding to the  
5 UE's PDN connection. This information is de-registered from the HSS as described in clause 12 of TS  
6 23.402[4].
- 7 6) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in subclause 7.3 of  
8 TS 23.203 [8].
- 9 7) The PDN-GW deletes all existing entries implied in the Registration Request message from its Binding Cache  
10 and sends a Registration Reply to the ASN-GW.
- 11 8) The ASN-GW sends a *MIPv4 Registration Reply* (lifetime=0) to the MS/UE.
- 12 Note: Step 3 is expected to be performed by the MS/UE however in some cases the MS/UE may directly send a  
13 *DREG-REG* message as shown in step 9.
- 14 9) The MS/UE sends a *DREG\_REQ* message with De-Registration Request Code=0x02 to BS.
- 15 10) For ASN-GW initiated Detach, the BS sends a *Path\_Dereg\_Rsp* message over R6 to the ASN-GW. Otherwise,  
16 for BS initiated Detach, the BS sends a *Path\_Dereg\_Req* message over R6 to the ASN-GW in order to start  
17 tearing down the R6 data path.
- 18 11) Upon receipt of a *Path\_Dereg\_Req* or *Path\_Dereg\_Rsp* message over R6, if the MS/UE didn't already perform  
19 a MIPv4 De-registration procedure in step 3, then the ASN-GW performs a MIPv4 Revocation procedure (steps  
20 11 to 13 in Box B) by sending a *MIPv4 Registration Revocation Req* message to the PDN-GW.
- 21 12) The PDN-GW informs the AAA Server/HSS to remove the PDN-GW identity information as described in step  
22 5 and clause 12 of [4].
- 23 13) The PDN-GW initiates the IP-CAN session termination procedure with the PCRF as defined in subclause 7.3 of  
24 [8].
- 25 14) The PDN-GW deletes all the existing entries implied in the Registration Revocation Req message from its  
26 Binding Cache and sends a *MIPv4 Registration Revocation Ack* message to the ASN-GW.
- 27 15) The ASN-GW/FA sends *NetExit\_MS\_State\_Change\_Req* message to notify the ASN-GW/Anchor  
28 Authenticator to delete the MS/UE contexts. If the network detachment is initiated by the ASN-GW/Anchor  
29 Authenticator with *NetExit\_MS\_State\_Change\_Req* as the first step, the ASN-GW/FA sends  
30 *NetExit\_MS\_State\_Change\_Rsp* message in this step to the ASN-GW/Authenticator as a response.
- 31 16) The ASN-GW containing the BBERF and Anchor Authenticator initiates the gateway control session  
32 termination procedure as defined in subclause 7.7.2 of TS 23.203 [8].
- 33 17) The ASN-GW/Anchor Authenticator responds to the ASN-GW/FA with a *NetExit\_MS\_State\_Change\_Rsp*  
34 message. This step is skipped if the network detachment is initiated by ASN-GW/Anchor Authenticator.
- 35 18) For ASN-GW initiated Detach, the ASN-GW/FA sends a *Path\_Dereg\_Ack* message over R6 to the BS.  
36 Otherwise, for BS initiated Detach, the ASN-GW/FA sends a *Path\_Dereg\_Rsp* message over R6 to the BS.
- 37 19) For BS initiated Detach, the BS sends a *Path\_Dereg\_Ack* message over R6 to the ASN-GW/FA.
- 38 Note: For idle mode ungraceful network exit, step 11-17 in this figure are needed, and additional steps as described  
39 in section 4.5.2.2.1 in stage 3 [1].

1 **9.2.4 HSS/AAA initiated detach procedure using CMIP4**

2 Figure 9-6 presents HSS/AAA initiated detach procedure over S2a (CMIP4). The HSS can initiate the procedure  
 3 when the user's subscription is removed and the 3GPP AAA Server can initiate the procedure when instructed by the  
 4 O&M system or upon re-authentication/re-authorization timer expiry.

5



6

7 **Figure 9-6 – HSS/AAA Initiated Detach Procedure over S2a (CMIP4)**

8

- 9 1) The HSS/AAA sends a Detach Indication message to the Anchor Authenticator in ASN-GW to detach a  
 10 specific MS/UE. The NAI and APN are included. The MN NAI identifies the MS/UE required to  
 11 detach. The APN is needed in order to determine which PDN-GW to deregister the MS/UE from, as  
 12 some PDN-GWs may support multiple PDNs.

13 Authenticator sends a *NetExit\_MS\_State\_Change\_Req* message over R4 to the FA/Anchor DPF. The  
 14 FA/Anchor DPF initiates the Data Path termination and MIP de-registration corresponding to the  
 15 MS/UE's PDN connections.

16 If the authenticator is located in the same ASN with the FA/Anchor DPF, the authenticator can send a  
 17 *Path\_Dereg\_Req* message to the BS over R6 directly.

- 18 2) This includes step 1 to 19 as in Figure 9-5.

- 19 3) The FA/Anchor DPF responds to the Authenticator by sending a *NetExit\_MS\_State\_Change\_Rsp*  
 20 message to confirm the Data Path termination and MIP de-registration. The Authenticator sends a  
 21 Detach Ack message to the HSS/AAA.

22 If the authenticator is located in the same ASN with the FA/Anchor DPF, the BS sends a  
 23 *Path\_Dereg\_Rsp* message over R6 to the Authenticator directly.

24

---

## 10. Authentication and Security

This section defines the authentication process for Access Control to the 3GPP core network, i.e. to permit or deny a subscriber to attach to and use the resources of a WiMAX® IP access which is interworked with the EPC network.

WiMAX access authentication signaling is executed between the MS/UE and the 3GPP AAA server/HSS.

3GPP based access authentication is executed across the STa reference point as per section 5. The MS/UE shall have a permanent ID that is an IMSI-based NAI as defined in TS 23.003 [10] for the initial authentication.

The WiMAX-3GPP dual mode device shall support EAP-AKA' [16] for the purpose of interworking with 3GPP.

### 10.1 Use of EAP-AKA' – Initial Authentication

For initial authentication, both MS/UE and 3GPP AAA/HSS SHALL execute the EAP-AKA' protocol [16] as specified in subclause 6.2 (Authentication and key agreement for trusted access) of TS 33.402 [5]. For execution of this protocol, both MS/UE and the 3GPP AAA/HSS SHALL set the ANID value to "WIMAX".

### 10.2 Use of EAP-AKA' – Fast Re-Authentication

EAP-AKA' Fast Re-Authentication shall be supported per IETF RFC 5448 [16]. Use of EAP-AKA' Fast Re-Authentication shall be as per 3GPP TS 33.402 [5].

### 10.3 Key derivation from EMSK

Key derivation from EMSK shall be as per 3GPP TS 33.402 [5].

---

1 **11. IP Address Allocation**

2 **11.1 IP Address Allocation in WiMAX® Networks using CMIP4 on S2a**

3 IP Address allocation in WiMAX using CMIP4 on S2a shall be as per RFC 3344 [6].

4 **11.2 IP Address Allocation in WiMAX using PMIP6 on S2a**

5 IP address allocation in WiMAX® networks using PMIP6 on S2a shall be as per section 4.7.2 of TS 23.402 [4].

6 Note: DHCP relay which is collocated in ASN-GW needs to be stateless, so ASN-GW will not send PBU with  
7 lifetime=0, as per section 4.7.2 of 3GPP TS 23.402 [4].

8

---

## 12. IP Mobility Mode Selection

IP Mobility Mechanism is statically configured in the MS/UE and network if operator plans to deploy a network with single mobility mechanism. For network supporting multiple mobility mechanism (PMIP6 & MIP4 FA-CoA), IP Mobility Mode is selected by HSS/AAA based on the information it has regarding the MS/UE, local/home network capabilities and local/home network policies. Support of CMIP4 and/or PMIP6 at WiMAX® ASN is known to HSS/AAA through static pre-configuration.

For WiMAX® ASN and EPC supports multiple protocols following principle applies:

- During initial attach over WiMAX, PMIP6 is used for providing connectivity. WiMAX ASN shall not send Agent Advertisement to MS/UE. If AAA/HSS indicates PMIP6 is not allowed, then the WiMAX ASN uses MIP4 and sends Agent Advertisements to MS/UE.
- During handover from 3GPP to WiMAX, PMIP6 is used for providing connectivity over WiMAX. WiMAX ASN shall not send Agent Advertisement to MS/UE. If AAA/HSS indicates PMIP6 is not allowed, then the WiMAX ASN uses MIP4 and sends Agent Advertisements to MS/UE.

---

## 1 **13. Handover**

### 2 **13.1 WiMAX® to 3GPP access handover procedures**

#### 3 **13.1.1 WiMAX® to E-UTRAN over GTP based S5/S8**

4 General procedure for handover from WiMAX access to E-UTRAN access over GTP based S5/S8 interface is  
5 specified in section 8.2.1.1 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after  
6 handover to E-UTRAN is as defined in Section 14.

#### 7 **13.1.2 WiMAX® to E-UTRAN over PMIP6 based S5/S8**

8 General procedure for handover from WiMAX access to E-UTRAN access over PMIP6 based S5/S8 interface is  
9 specified in section 8.2.1.2 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after  
10 handover to E-UTRAN is as defined in Section 14.

#### 11 **13.1.3 WiMAX® to UTRAN/GERAN over GTP based S5/S8**

12 General procedure for handover from WiMAX access to UTRAN/GERAN access over GTP based S5/S8 interface  
13 is specified in section 8.2.1.3 of TS 23.402 [4]. The resource release procedure in the WiMAX access system after  
14 handover to UTRAN/GERAN is as defined in Section 14.

#### 15 **13.1.4 WiMAX® to UTRAN/GERAN over PMIP6 based S5/S8**

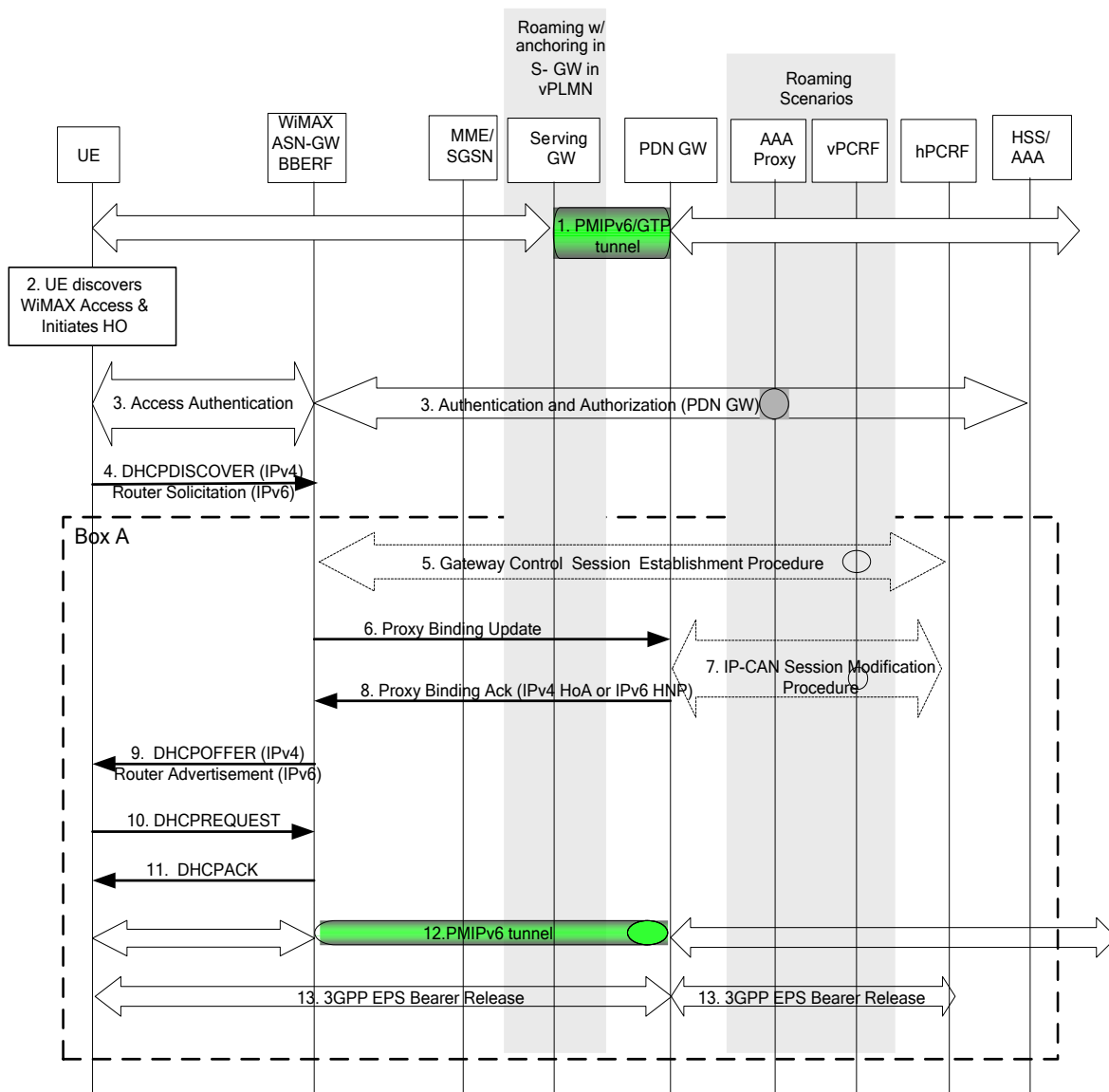
16 General procedure for handover from WiMAX access to UTRAN/GERAN access over PMIP6 based S5/S8  
17 interface is specified in section 8.2.1.4 of TS 23.402 [4]. The resource release procedure in the WiMAX access  
18 system after handover to UTRAN/GERAN is as defined in Section 14.

1 **13.2 3GPP access to WiMAX®**

2 **13.2.1 Handover from 3GPP to WiMAX® with PMIP6**

3 The steps involved in the handover from a 3GPP access network connected to the EPC to a WiMAX access network  
 4 connected via PMIP6 tunnel to the same EPC over the S2a interface are depicted below for the case of non-roaming,  
 5 roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway  
 6 in the VPLMN. It is assumed that while the MS/UE is served by the 3GPP Access, a PMIP6 or GTP tunnel is  
 7 established between the S-GW and the PDN-GW in the Evolved Packet Core. For Dual Radio handover, the MS/UE  
 8 is in WiMAX active mode during handover procedure.

9



10

11

12

**Figure 13-1 – Handover from 3GPP Access to WiMAX® with PMIP6 on S2a**

- 1 The optional interaction steps between the gateways and the PCRF in Figure 13-1 only occur if dynamic policy  
2 provisioning is deployed. Otherwise policy may be statically configured with the gateway.
- 3 1) The MS/UE is connected to the 3GPP access network and has a PMIP6 or GTP tunnel on the S5 interface.
  - 4 2) The MS/UE discovers the WiMAX access system and determines to transfer its current sessions (i.e.  
5 handover) from the currently used 3GPP access network to the discovered WiMAX access network. The  
6 mechanisms that aid the MS/UE to discover the WiMAX access system are specified in chapter 8 (Access  
7 Network Discovery and Selection).
  - 8 3) The MS/UE performs access authentication and authorization in the WiMAX access system. The 3GPP AAA  
9 server authenticates and authorizes the MS/UE for access in the trusted non-3GPP system. The 3GPP AAA  
10 server queries the HSS and returns the PDN-GW address to the WiMAX access system at this step (upon  
11 successful authentication and authorization).
- 12 Note: Device authentication based on X.509 certificates is not applicable.
- 13 PDN-GW address selection is as described in the section 4.5.1 of 3GPP TS 23.402 [4].
- 14 4) After successful authentication and authorization, the DHCP DISCOVER (for IPv4) or Router Solicitation  
15 (for IPv6) procedure is triggered. The Router Solicitation message will be optional if the attach type was  
16 known at step 3.
- 17 5-8) Steps 5-8 in Box A are described as steps 5-8 subclause 8.2.2 in 3GPP TS 23.402 [4] and subclause 7.7 in  
18 TS 23.203 [8].
- 19 Note: Steps 5-6 can happen anytime after step 3.
- 20 Note: In absence of “Attach Type” received over WiMAX access, if a PDN-GW for the default APN is  
21 returned to the WiMAX access during access authentication in step 3, the Handover Indicator in PBU (step 6)  
22 shall be set to “\”4” – Handover state unknown. Otherwise, Handover Indicator shall be set to “1” – attach  
23 over new interface.
- 24 9) The ASN-GW sends the DHCP OFFER to the MS/UE with assigned MN-HoA or Router Advertisement with  
25 assigned IPv6 HNP.
  - 26 10-11) For IPv4 case, the MS/UE configures the previously offered IPv4 address via DHCPv4 signalling.
  - 27 12) The PMIP6 tunnel is set up between the WiMAX ASN-GW and the PDN-GW. At this point, the MS/UE can  
28 send and receive IP packets through the WiMAX network.
  - 29 13) Step 13 in box A is described as steps 12 in subclause 8.2.2 in 3GPP TS 23.402 [4].

30

### 31 **13.2.2 Handover from 3GPP to WiMAX® with CMIP4**

32

33 The steps involved in the handover from a 3GPP access network connected to the EPC to a WiMAX® access  
34 network connected via CMIP4 to the same EPC over the S2a interface are depicted below for the case of non-  
35 roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving  
36 Gateway in the VPLMN. It is assumed that while the MS/UE is served by the 3GPP Access, a PMIP6 or GTP tunnel  
37 is established between the S-GW and the PDN-GW in the Evolved Packet Core.

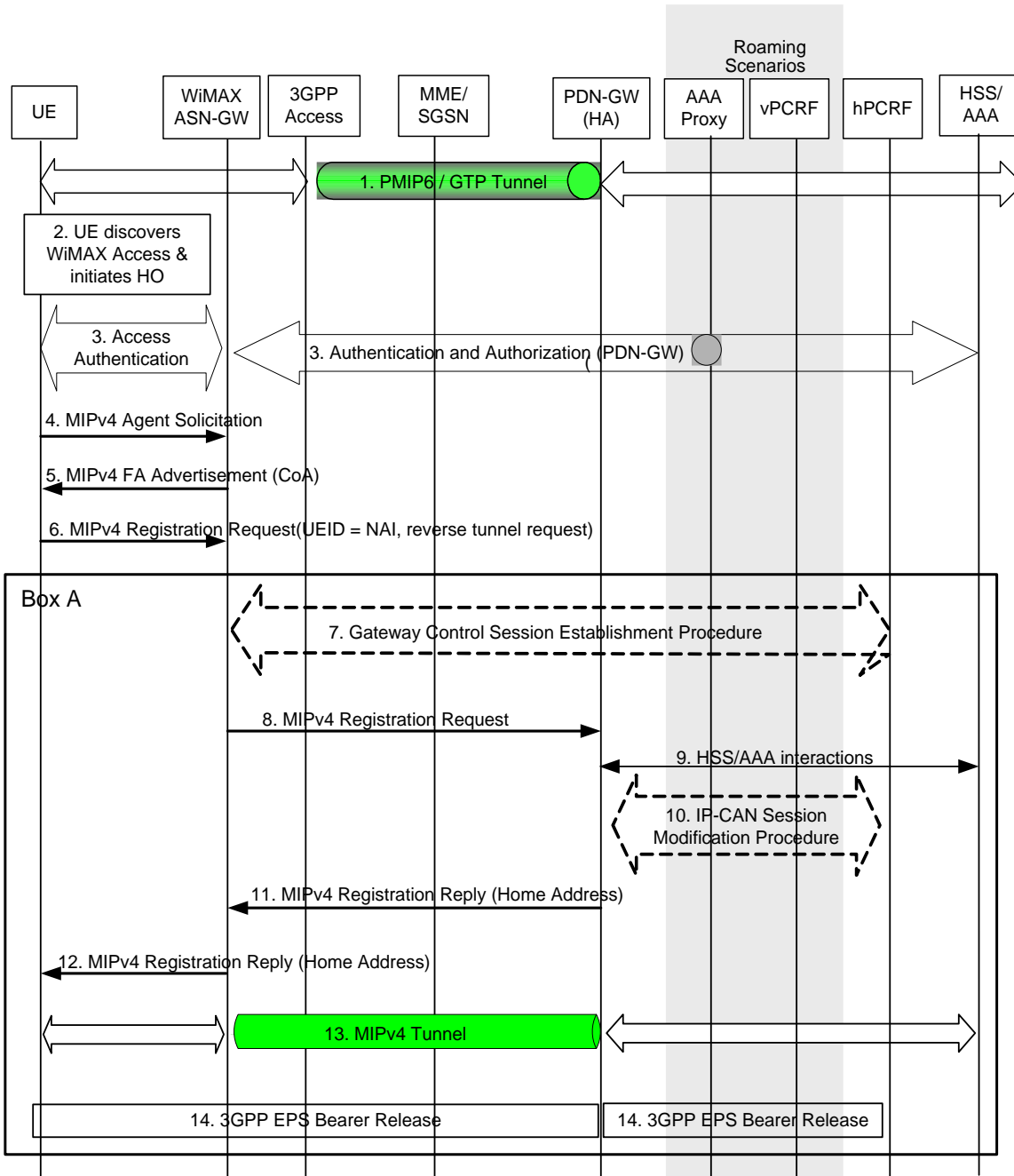


Figure 13-2 – 3GPP IP Access to WiMAX® Handover with CMIP4 on S2a

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

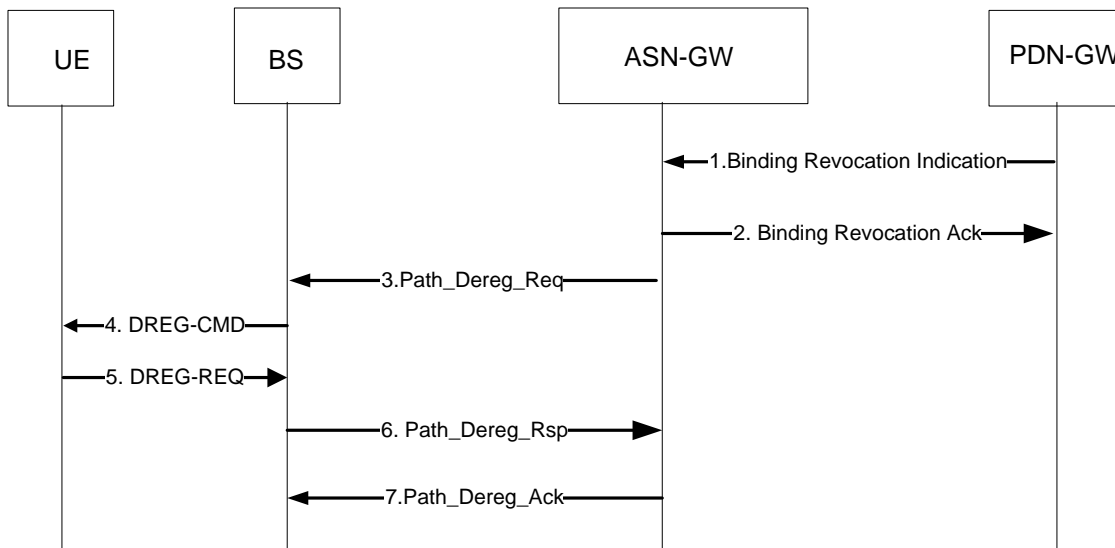
- 1) The MS/UE is connected to the 3GPP access network and has a PMIP6 or GTP tunnel on the S5 interface.
- 2) The MS/UE discovers the WiMAX access system and determines to transfer its current sessions (i.e. handover) from the currently serving 3GPP access network to the discovered WiMAX access network. The

- 1 mechanisms that aid the MS/UE to discover the WiMAX access network are specified in chapter 8 (Access  
2 Network Discovery and Selection).
- 3 3) The MS/UE performs access authentication and authorization in the WiMAX access system. The 3GPP AAA  
4 server authenticates and authorizes the MS/UE for access in the WiMAX system. The 3GPP AAA server  
5 queries the HSS and returns the PDN-GW address to the ASN at this step (upon successful authentication  
6 and authorization).
- 7 After the successful authentication, both MS/UE and AAA derive the MIP-RK, SPI, and other mobility keys  
8 such as FA-RK, MN-FA, MN-HA-CMIP4 that will be used for the security protection in CMIP4 registration  
9 messages.
- 10 4) The MS/UE may send an Agent Solicitation message (AS) RFC 3344 [6] to trigger the Handover procedure.
- 11 5) The FA sends a Foreign Agent Advertisement message (FAA) (RFC 3344 [6]) to the MS/UE. The FAA  
12 message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. The number of times  
13 this message is sent can be configured.
- 14 6) The MS/UE sends a Registration Request (RRQ) (MN-NAI, lifetime) message as defined in RFC 3344 [6] to  
15 the FA as specified in RFC 3344 [6]. Reverse Tunnelling shall be requested. This ensures that all traffic will  
16 go through the PDN-GW. The RRQ message shall include the NAI-Extension RFC 2794 [15]. The MS/UE  
17 may not indicate a specific Home Agent address in the RRQ message, in which case the FA uses the PDN-  
18 GW address as received in step 3. The MS/UE then receives the IP address of the PDN Gateway in step 12 as  
19 part of the Registration Reply (RRP) message. The MS/UE should then include the PDN Gateway address in  
20 the Home Agent address field of subsequent RRQ messages.
- 21 The Authentication Extension in the RRQ should be calculated using keys derived in the step 3.
- 22 7-14) Steps 7-14 in Box A are described in subclause 8.3 in 3GPP TS 23.402 [4] and subclause 7.7 in TS 23.203  
23 [8].

## 14. Resource Deactivation Procedures

### 14.1 PDN GW initiated Resource Deactivation using PMIP6

The procedure described in this section is used for releasing of resources in WiMAX® system after handover to 3GPP access.



**Figure 14-1 – PDN-GW Initiated resource deactivation (PMIP6)**

- 1) PDN-GW initiates the Binding Revocation procedure by sending Binding Revocation Indication to the MAG as defined in RFC 5826 [13]. For Handover, Revocation trigger indicates Inter-MAG Handover over different Access Types.
- 2) MAG in ASN-GW sends Binding Revocation Ack to acknowledge the successful resource release procedure.
- 3) ASN-GW determines that MS/UE detach is required and then initiates data path deregistration procedure by sending *Path\_Dereg\_Req* message over R6 to BS with Action Code TLV set to indicate MS/UE detach from the network to release the connection.
- 4) BS sends DREG\_CMD message to the MS/UE including Action Code=0x00.
- 5) MS/UE sends a DREG\_REQ message with De-Registration Request Code=0x02 to BS.
- 6) BS sends *Path\_Dereg\_Rsp* message over R6 to the ASN-GW.
- 7) ASN-GW sends a *Path\_Dereg\_Ack* message over R6 to the BS.

Note: For idle mode ungraceful network exit initiated by PDN-GW, step 1-2 in this figure are needed, and additional steps as described in section 4.5.2.2.1 in stage 3 [1].

---

## 15. Policy and Charging Control

This section describes the functions associated with policy and charging which is part of 3GPP EPC – WiMAX Connectivity and Interworking architecture (see Figure 5-1, Figure 5-2, Figure 5-3 and Figure 5-4).

Per TS 23.401 [3] and TS 23.402 [4], a 3GPP EPS needs to support both PCEF/BBERF and PCRF functionality to enable dynamic policy and charging control by means of installation of PCC rules and QoS rules based on user and service flow dimensions. However, a 3GPP EPS may only support PCRF and PCEF functionality and no BBERF functionality in which case it shall support dynamic policy and charging control in 3GPP EPC side.

The procedures and call flows defined in this specification assume that deployment of dynamic policy and charging control (PCC) as defined in TS 23.402[4] and TS 23.203 [8], will be consistent throughout the network.

The ASN-GW implements the Bearer Binding and Event Reporting Function (BBERF) needed to interwork 3GPP EPC with WiMAX (see Figure 5-1, Figure 5-2, Figure 5-3 and Figure 5-4).

### 15.1 ASN-GW requirements for 3GPP PCC Release 9

- The BBERF in the ASN-GW shall follow the framework defined in TS 23.402 [4] for QoS policy control.
- The ASN-GW/BBERF shall perform bearer binding to associate the QoS rule to an appropriate IP-CAN bearer (i.e. a WiMAX SF) within the IP-CAN session. The bearer binding mechanism on the ASN-GW/BBERF is defined in 3GPP TS 23.203 subclause 6.1.1.4 [8].
- The ASN-GW/BBERF shall support event trigger mechanism defined in TS 23.203 [8]. When receiving the event trigger list from the PCRF, the ASN-GW/BBERF shall obtain the associated information and send these parameters to the PCRF via a response message. When one or more of the subscribed event triggers happen, the ASN-GW/BBERF shall inform the PCRF the occurrences of these events and update the PCRF with the associated parameters. The association of Gxa parameters to each event trigger is described in 3GPP TS 29.212 subclause 5.3.7[19].
- Full policy and charging enforcement functionality with service-aware end-user charging shall be located only in the PDN-GW. The BBERF shall communicate with the PCRF in the EPC using the Gxa interface as defined in TS 23.203 [8].

### 15.2 Gxa interface requirements

In order to enable bearer binding and event reporting functions, the ASN-GW/BBERF SHALL communicate with the 3GPP PCRF using the Gxa reference point.

The Gxa reference point, when terminated at the ASN-GW, shall satisfy the following architectural principles of TS 23.402 [4] :

- Gxa shall support transfer of QoS parameters and related rules.
- Gxa shall support event reporting.

The supported event triggers are listed in Table 15-1, and the supported Gxa parameters are listed in Table 15-2.

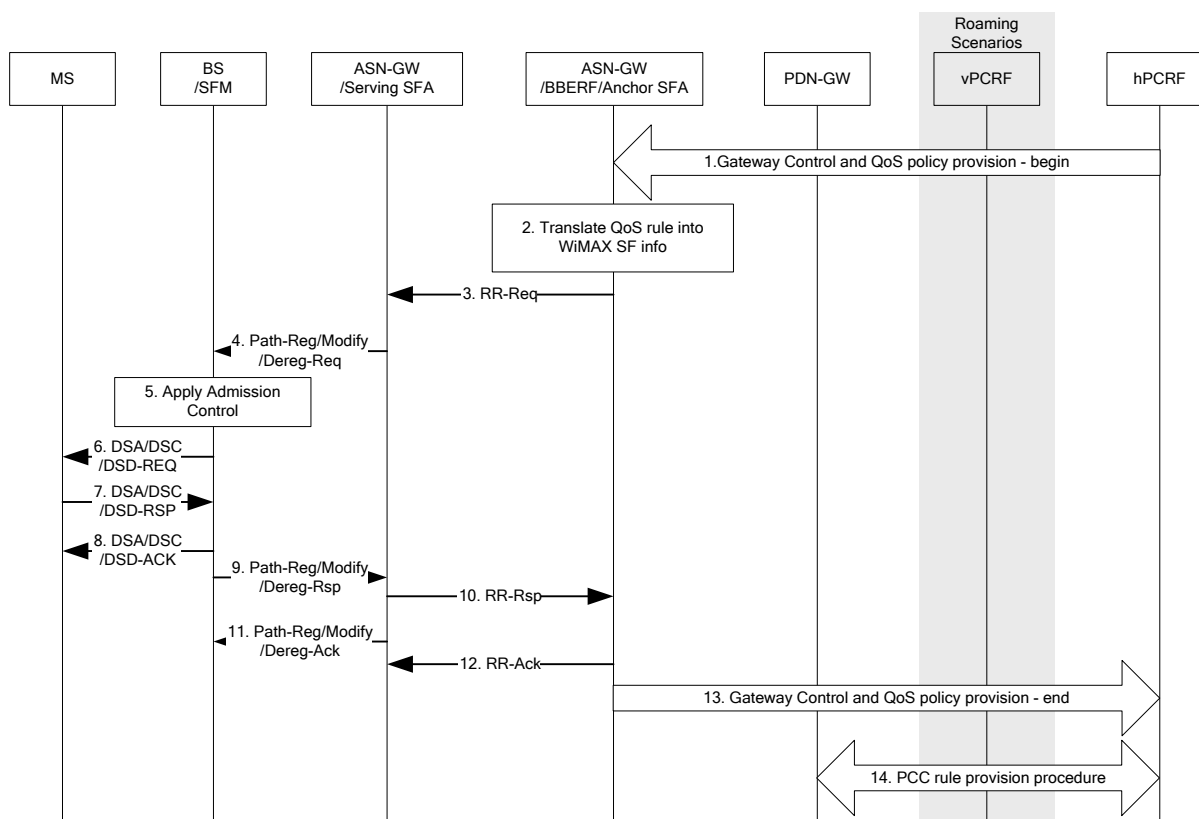
The service flow level QoS parameters are conveyed in QoS rules and their definition and usage are discussed in TS 23.203 [8] and TS 23.402 [4]. The service flow level QoS parameters shall consist of:

- QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP) for both Guaranteed Bit-Rate and non-Guaranteed Bit Rate bearers.
- Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR) parameters for Guaranteed Bit Rate bearers, and MBR for non-GBR bearers.

## 1 15.3 PCC procedures and flows

### 2 15.3.1 Network-initiated dynamic PCC procedure

3 The PCRF may initiate QoS rule provisioning to the BBERF to control the resource allocation in non-3GPP access  
4 network as defined in section 6.6 in 3GPP TS 23.402 [4]. The procedure of Network-initiated QoS rule provisioning  
5 and enforcement in WiMAX access network is shown in Figure 15-1. The vPCRF only exist in roaming scenarios  
6 and forwards messages between hPCRF and BBERF.

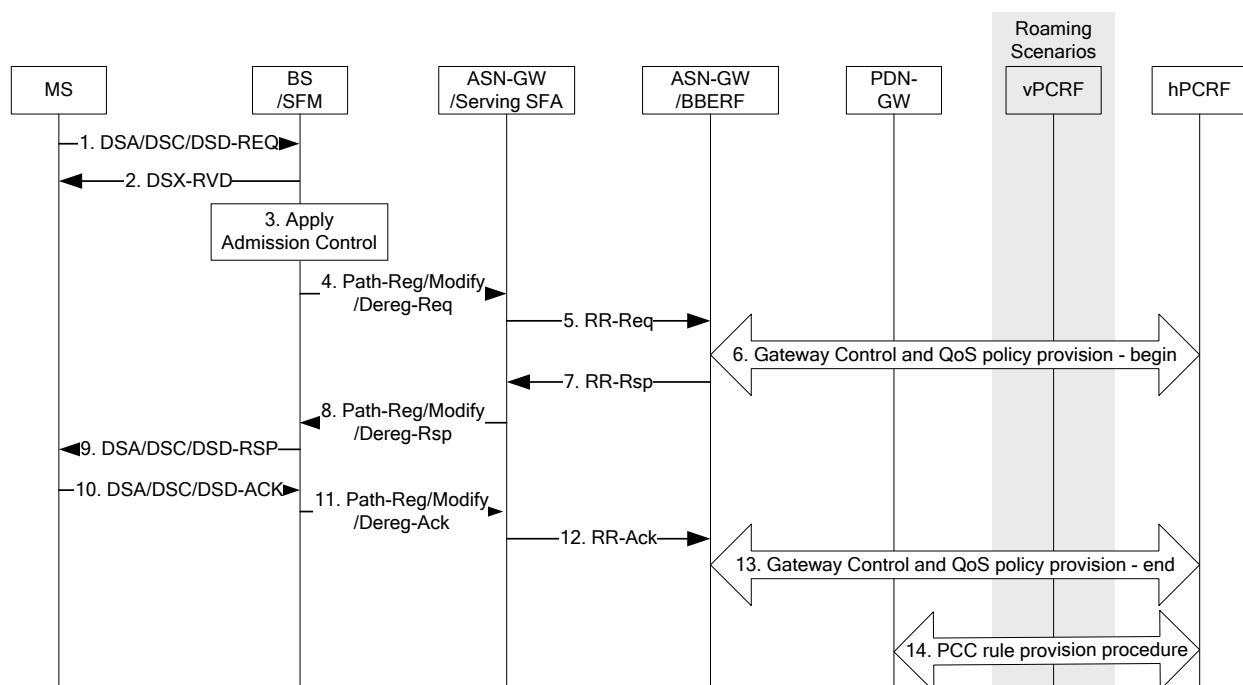


7  
8 **Figure 15-1 – Network-initiated dynamic PCC procedure**

- 9
- 10 1) The PCRF sends a *RAR* message with the QoS rules and event triggers to the BBERF as defined in TS  
11 23.203 [8].
  - 12 2) After received the QoS rules, the BBERF translates the QoS rules into WiMAX SF Info parameters. The  
13 mapping relationship between QoS rule and SF Info is shown in Table 15-2.
  - 14 3) The BBERF invokes the co-located Anchor SFA to initiate dynamic service flow management procedure  
15 by sending a *RR-Req* message to the Serving SFA.
  - 16 4) The Serving SFA sends a *Path-Reg/Modify/Dereg-Rsp* message to the BS/SFM to initiate corresponding  
17 data path operation.
  - 18 5) If new air resources are required, the BS/SFM performs admission control for the requirement.
  - 19 6) If the requested resource can be satisfied at the BS, the BS sends *DSA/DSC/DSD-REQ* message to the MS.
  - 20 7) The MS/UE responds to the BS/SFM with a *DSx-RSP* message.
  - 21 8) The BS/SFM sends a *DSx-ACK* message to the MS/UE to complete the QoS transaction in the airlink.

- 1 9) The BS/SFM sends a *Path-Reg/Modify/Dereg-Rsq* message to the Serving SFA to confirm the reservation.
- 2 10) The Serving SFA sends a *RR-Rsp* message sent to the BBERF/Anchor SFA.
- 3 11) The Serving SFA sends a *Path-Reg/Modify/Dereg-Ack* message to the BS/SFM.
- 4 12) The BBERF/Anchor SFA returns a *RR-Ack* message to the Serving SFA.
- 5 13) The BBERF responds to the PCRF with a *RAA* message. This step can be performed in parallel with step
- 6 12.
- 7 14) The PCRF provisions the PCC rules at the PCEF in the PDN-GW as defined in TS 23.203 [8]. Step 14 may
- 8 occur before step 1 or performed in parallel with steps 1-13 if acknowledgement of resource allocation is
- 9 not required at the PCRF before it updates the PCC rules in the PCEF (as defined in TS 23.203 [8]).

### 10 15.3.2 MS-initiated dynamic PCC procedure



11

12

**Figure 15-2 – MS-initiated dynamic PCC procedure**

13

- 14 1) The MS/UE initiates dynamic service flow management by sending a *DSA/DSC/DSD-REQ* message to the
- 15 BS.
- 16 2) A *DSX-RVD* is sent from the BS to the MS/UE.
- 17 3) If new air resources are required, the BS/SFM performs admission control for the requirement.
- 18 4) If the MS's request is admitted in step 3, the BS starts the corresponding data path procedure. The BS sends
- 19 *Path-Reg/Modify/Dereg-Req* message to the Anchor DP which is co-located with Serving SFA.
- 20 5) The Serving SFA sends a *RR-Req* message to the Anchor SFA including the requested SF info.
- 21 6) The Anchor SFA invokes the co-located BBERF to start Gateway Control session modification and receive
- 22 the authorized QoS rule from the PCRF as defined in TS 23.203 [8].
- 23 7) The BBERF/Anchor SFA returns a *RR-RSP* message to the Serving SFA indicating the authorization
- 24 decision and optionally the authorized QoS parameters.

- 1 8) The Serving SFA sends *Path-Reg/Modify/Dereg-Rsp* message to the BS/SFM to confirm the reservation.
- 2 9) The SFM confirms the request of the MS/UE by sending a *DSx-RSP* message.
- 3 10) The MS/UE sends a *DSx-ACK* message to complete the QoS request.
- 4 11) The SFM sends a *Path-Reg/Modify/Dereg-Ack* message to the Serving SFA to inform the completion of the  
5 request.
- 6 12) The Serving SFA sends a *RR-Ack* message to the Anchor SFA/BBERF.
- 7 13) If the QoS enforcement result was required by the PCRF, the BBERF indicates to the PCRF whether the  
8 QoS Policy Rules enforcement was successful as defined in TS 23.203 [8].
- 9 14) The PCRF initiates the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [8] to  
10 update the PCC rules in the PDN GW. This step may be performed in parallel with steps 6-13 if  
11 acknowledgement of resource allocation is not required at the PCRF before the update of the PCC rules in  
12 the PCEF (as defined in TS 23.203 [8]).

### 13 **15.3.3 Allocation and retention priority support**

14 The Allocation-Retention-Priority (ARP) parameter may be included in the QoS rule to indicate the priority of  
15 allocation and retention, the pre-emption capability and pre-emption vulnerability for the bearers of the service  
16 flows as defined in 3GPP TS 29.212 [19].

17 When the BBERF receives a *CCA/RAR* message including ARP parameter from the PCRF or vPCRF, the  
18 BBERF/Anchor SFA shall:

- 19 1) set the Priority Indication field in the QoS Parameters of the SF Info structure with the ARP value in the  
20 received QoS rule based on the local policy, and
- 21 2) send the *RR\_Req* message with SF Info to the Serving SFA.

22 When the Serving SFA receives an *RR\_Req* message from the BBERF/Anchor SFA to create a new service flow, the  
23 Serving SFA forwards the Priority Indication field in SF Info in the *Path\_Reg\_Req* message to the Serving BS.

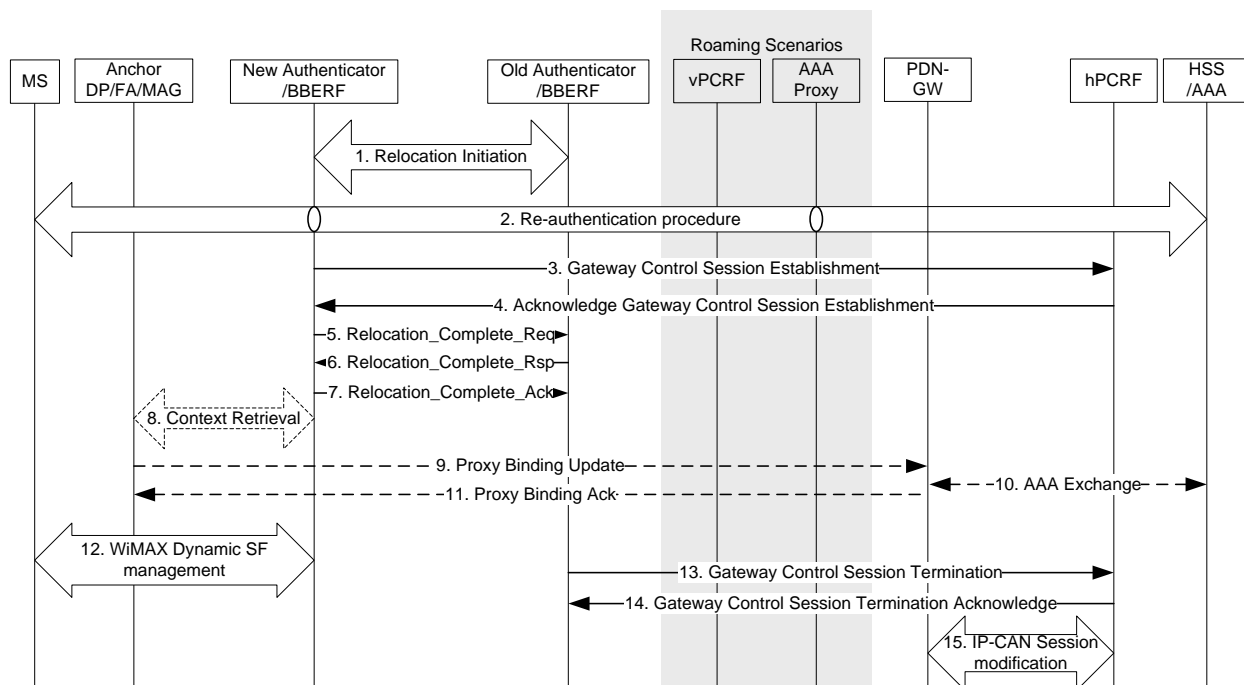
24 When the Serving SFA receives an *RR\_Req* message from the Anchor SFA to modify an existing service flow, the  
25 Serving SFA forwards the Priority Indication field in SF Info in the *Path\_Modification\_Req* message to the Serving  
26 BS.

27 Based on the received Priority Indication field, the ASN-GW and BS shall perform priority resource allocation and  
28 retention for the service flow as described in section 4.19.2 of Stage 3[1].

29 The sub-structure of the Priority Indication field and its association with the ARP parameters (Priority Level, Pre-  
30 emption Capability, Pre-emption Vulnerability) is described in the ETS section of the Network Release 2.0 Stage 3  
31 base document, section 4.19.1.4 [29].

### 32 **15.3.4 Intra WiMAX BBERF relocation for PMIPv6**

33 In the WiMAX functional decomposition, the BBERF is co-located with the Anchor Authenticator (AA). When the  
34 Anchor Authenticator is relocated from the source to the target ASN-GW, the BBERF shall be relocated with it at  
35 same time. The combined Authenticator/BBERF relocation procedure for the PMIPv6 case is shown in the  
36 following figure. The vPCRF and AAA proxy only exist in roaming scenarios.



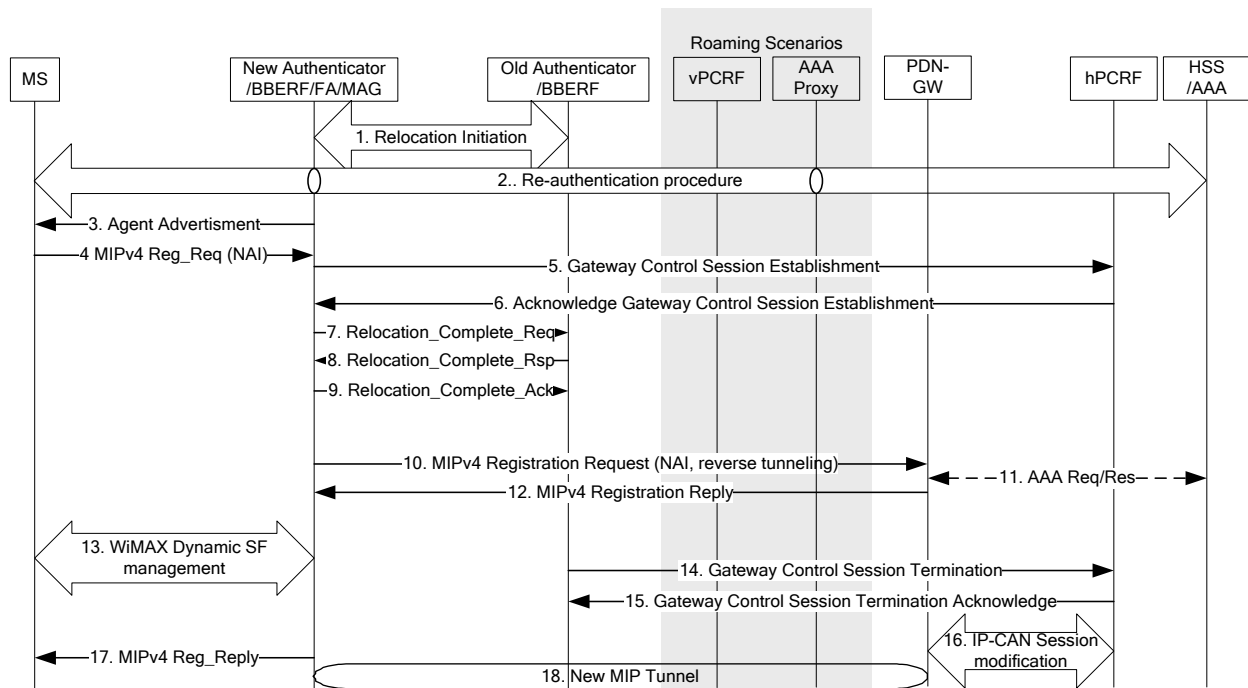
**Figure 15-3 – Intra WiMAX BBERF relocation for PMIPv6**

- 1) The Anchor Authenticator relocation is initiated by either the new or old authenticator as defined in section 4.4.1.5.5 or 4.21 in stage 3 [1].
- 2) The EAP phase and SA-TEK 3 Way Handshake (WHS) procedure are performed during the Re-authentication procedure. For optimized relocation case, the new Authenticator obtains MSK from the proxy AAA without performing full re-authentication in this step as defined in subclause 4.21 stage3 [1].
- 3) In case of EAP-Success (AA relocation success), the new target Authenticator triggers the collocated BBERF function to initiate Gateway Control Session Establishment with the PCRF as defined in subclause 7.7.1.2 in [8]. The new target BBERF does not include the Session-Linking-Indicator AVP or include the AVP with value 0, to inform the PCRF it needs to immediately link the new Gxa session with existing Gx session.
- 4) The PCRF responds to the target BBERF with Acknowledge Gateway Control Establishment message including the QoS rules and Event triggers as defined in subclause 7.7.1.2 in [8].
- 5-7) The new Authenticator and the old Authenticator complete relocation procedure as defined in section 4.4.1.5.5 in stage 3 [1].
- 8) The new Authenticator performs Authenticator Update Notification Procedure as defined in subclause 4.4.1.5.5.5 in stage 3 [1].  
Note: Step 8 is optional if the Anchor DP is co-located with the new target Authenticator/BBERF.
- 9) If the Anchor DP and AA are co-located in the same ASN-GW, and combined AnchorDP/Authenticator relocation is performed, the new Anchor DP/MAG initiates a Proxy Binding Update with the PDN-GW in this step.
- 10) Query and response exchange between the PDN-GW and the 3GPP AAA server following the S6b procedures defined in TS 23.402 [4], TS 29.273 [14] and TS 33.402 [5].
- 11) The PDN-GW responds to the ASN-GW/MAG with a Proxy Binding Ack message.

- 1 12) The QoS rules and event triggers received by the target BBERF in step 4 are deployed and the target
- 2 Authenticator/BBERF initiates dynamic service flow management process as shown in Figure 15-1 steps 3-
- 3 12. Note: If the authorized QoS parameters are the same as the ones in the old source
- 4 Authenticator/BBERF, the Data path management and airlink SF modification steps may be skipped.
- 5 13) The source Authenticator/BBERF sends a Gateway Control Session Termination to the PCRF to cease the
- 6 prior Gxa session. Step12-14 may occur in parallel with step 8-11.
- 7 14) The PCRF sends a Gateway Control Session Termination Acknowledge message to the source
- 8 Authenticator/BBERF acknowledging the termination of the control session.
- 9 15) The PCRF performs IP-CAN session modification procedure as defined in subclause 7.7.1.2 step 10 in [8].

### 10 15.3.5 Intra WiMAX BBERF relocation for MIPv4 FACoA

11 In the WiMAX functional decomposition, the BBERF is co-located with the Anchor Authenticator (AA). In this call  
12 flow when the A-DPF/FA is relocated from the source to the target ASN-GW, so is the Anchor Authenticator and  
13 the BBERF at same time. Simultaneous migration of the A\_DPF and AA is optional. The combined A-DPF,  
14 Authenticator/BBERF relocation procedure for the MIPv4 FACoA case is shown in the following figure. The  
15 vPCRF and AAA proxy only exist in roaming scenarios.



16  
17 **Figure 15-4 – Intra WiMAX BBERF relocation for CMIPv4**

- 18
- 19 1) Anchor-DPF and anchor authenticator relocation can be triggered by the network or by the MS. In the case
- 20 of network triggered relocation, step 1 above follows steps 1 through 4 as described in subclause 4.8.3.3.7.1
- 21 in stage 3 [1].
- 22 2) In case of MS/UE triggered relocation at re-registration renewal time, re-authentication takes place as
- 23 described in subclause 4.8.3.1 of stage 3 [1]. The EAP phase and SA-TEK 3 WHS procedure are
- 24 performed during the Re-authentication procedure. For optimized relocation case, the new Authenticator
- 25 obtains MSK from the Proxy AAA without performing full re-authentication in this step as defined in
- 26 subclause 4.21 stage3 [1].

- 1 3) In the case of network initiated relocation, the new A\_DPF/FA sends agent advertisement as described  
2 subclause 4.8.3.1 or 4.8.3.3.7.1 in stage 3 [1].
- 3 4) The MS/UE sends a Registration Request (RRQ) [6] message to the FA collocated with the A-DPF.  
4 Reverse tunneling is requested. This ensures that all traffic will go through the PDN-GW. The RRQ  
5 message includes the NAI and either the Home Agent address or a request for Home Agent assignment.
- 6 5) The new target Authenticator triggers the collocated BBERF function to initiate Gateway Control Session  
7 Establishment with the PCRF as defined in subclause 7.7.1.2 in [8]. The new target BBERF does not  
8 include the Session-Linking-Indicator AVP or include the AVP with value 0, to inform the PCRF it needs  
9 to immediately link the new Gxa session with existing Gx session. In case re-authentication was performed  
10 in step 2, this step proceeds only after EAP-Success (AA relocation success).
- 11 6) The PCRF responds to the target BBERF with Acknowledge Gateway Control Establishment message  
12 including the QoS rules and Event triggers as defined in subclause 7.7.1.2 in [8].
- 13 7-9) The new Authenticator and the old Authenticator complete relocation procedure as defined in subclause  
14 4.4.1.5.5 in stage 3 [1].  
15 Note: The new authenticator performs internal context update similar to the Authenticator Update  
16 Notification procedure defined in subclause 4.4.1.5.5.5 in stage 3 [1].
- 17 10) As the Anchor DP and AA are co-located in the same ASN-GW, and combined AnchorDP/Authenticator  
18 relocation is performed, the new Anchor DP/FA initiates a MIPv4 Registration Request with the PDN-GW  
19 in this step.
- 20 11) If the PDN-GW does not have a Mobile-Home Authentication Extension SPI that agrees with the one  
21 received in the RRQ from the MS, the PDN-GW sends an Authorization Request to the 3GPP AAA to  
22 obtain authorization and the mobility key.
- 23 12) The PDN-GW responses to the new ASN-GW/FA with a MIPv4 Registration Response message.
- 24 13) The QoS rules and event triggers received by the target BBERF in step 6 are deployed and the target  
25 Authenticator/BBERF initiates dynamic service flow management process as shown in Figure 15-1 steps 3-  
26 12.  
27 Note: If the authorized QoS parameters are the same as the ones in the old source Authenticator/BBERF,  
28 the Data path management and airlink SF modification steps may be skipped.
- 29 14) The source Authenticator/BBERF sends a Gateway Control Session Termination to the PCRF to cease the  
30 prior Gxa session. Step12-14 may occur in parallel with step 8-11.
- 31 15) The PCRF sends a Gateway Control Session Termination Acknowledge message to the source  
32 Authenticator/BBERF acknowledging the termination of the control session.
- 33 16) The PCRF performs IP-CAN session modification procedure as defined in subclause 7.7.1.2 step 10 in [8].
- 34 17) The A-DPF/FA processes the RRP message according to RFC3344 [6] and sends a corresponding RRP  
35 message to the MS.
- 36 18) A MIP tunnel is established between the new target FA and the PDN-GW.

### 37 **15.3.6 PCRF discovery and selection**

38 The PCRF discovery and selection shall be performed at the ASN-GW/BBERF before Gateway Control Session is  
39 established. According to the configuration of the operator, the ASN-GW/BBERF may select PCRF for a certain IP-  
40 CAN session based on the APN (Default APN) and realm information in MS's NAI.

41 If more than one PCRF exists in the Diameter realm, an additional DRA (Diameter Routing Agent) function is  
42 needed for PCRF discovery and selection. The DRA function maintains the PCRF assignment information (i.e. DRA  
43 binding) of the Diameter realm to ensure that all PCC-related Diameter sessions (Gx, Gxa, S9 and Rx) of a certain  
44 IP-CAN session reach the same PCRF. In this case, the ASN-GW/BBERF shall send the CCR message to the DRA  
45 function before Gateway Control Session establishment. After receiving the request message, the DRA may assign a  
46 new PCRF, or obtain the IP address of the assigned PCRF by searching the DRA binding with the MS's NAI and

- 1 APN in the request message. According to the various DRA mode defined in 3GPP TS29.213 [21], the ASN-  
 2 GW/BBERF shall establish Diameter session via the DRA (in PA1 mode), or with the selected PCRF directly after it  
 3 receives the address of the PCRF from the DRA (in redirect mode or PA2 mode).
- 4 If DRA was used during the PCRF selection, the ASN-GW/BBERF shall inform the DRA function to release the  
 5 stored PCRF assignment information of the IP-CAN session when the Gateway Control Session is terminated or  
 6 failed to be established.
- 7 The detailed call flows between the ASN-GW/BBERF and the DRA function are defined in section 7.4 in 3GPP TS  
 8 29.213 [21].
- 9 Note: In roaming scenario, only the v-PCRF needs to be selected by the BBERF. A v-DRA may be used for v-PCRF  
 10 selection.

## 11 15.4 Message and Parameter definitions

### 12 15.4.1 Event trigger support list

13 The event triggers over the Gxa interface are illustrated in Table 15-1 along with an indication whether an event is  
 14 supported by the WiMAX ASN-GW/BBERF. In WiMAX-3GPP interworking, these supported event triggers may  
 15 be used in the *CCA/RAR* messages by the PCRF to subscribe to event notifications, or be used in the *CCR/RAA*  
 16 messages by the ASN-GW/BBERF to report event occurrence along with the related parameters listed in Table 15-2  
 17 to the PCRF for a QoS rule decision. For further details refers to subclause 5.3.7 in [19].

18 **Table 15-1 Event trigger support list**

Event trigger value[a]	Supported by the ASN-GW /BBERF	Description
SGSN_CHANGE (0)	No	3GPP only
QOS_CHANGE (1)	Yes	Indicate the change of request QoS.
RAT_CHANGE (2)	No	Not applicable for WiMAX access network.[b]
TFT_CHANGE (3)	No	3GPP only
PLMN_CHANGE (4)	No	Not applicable for Gxx interface.
LOSS_OF_BEARER (5)	No	
RECOVERY_OF_BEARER (6)	No	
IP-CAN_CHANGE (7)	No	Not applicable for Gxx interface.
QOS_CHANGE_EXCEEDING_AUTHORIZATION (11)	No	Not applicable for Gxx interface.
RAI_CHANGE (12)	No	3GPP only
USER_LOCATION_CHANGE (13)	Yes	Indicate the change of user's location.
NO_EVENT_TRIGGERS (14)	Yes	Remove the event triggers on BBERF.
OUT_OF_CREDIT (15)	No	Not applicable for Gxx interface.
REALLOCATION_OF_CREDIT (16)	No	Not applicable for Gxx interface.
REVALIDATION_TIMEOUT (17)	Yes	Used for schedule the next CCR.

Event trigger value[a]	Supported by the ASN-GW /BBERF	Description
UE_IP_ADDRESS_ALLOCATE (18)	No	Not applicable for Gxx interface.
UE_IP_ADDRESS_RELEASE (19)	No	Not applicable for Gxx interface.
DEFAULT_EPS_BEARER_QOS_CHANGE (20)	No	3GPP only
AN_GW_CHANGE (21)	No	Not applicable for Gxx interface.
SUCCESSFUL_RESOURCE_ALLOCATION (22)	Yes	Indicate the resource for a QoS rule is allocated successfully.
RESOURCE_MODIFICATION_REQUEST (23)	Yes	Indicate a resource modification request initiated by the MS.
PGW_TRACE_CONTROL (24)	No	3GPP only
UE_TIME_ZONE_CHANGE (25)	Yes	Indicate the change of user's timezone.
TAI_CHANGE (26)	No	3GPP only
ECCI_CHANGE (27)	No	3GPP only
CHARGING_CORRELATION_EXCHANGE (28)	No	Not applicable for Gxx interface.
APN-AMBR_MODIFICATION_FAILURE (29)	Yes	Indicate the APN-AMBR modification have failed.
USER_CSG_INFORMATION_CHANGE (30)	No	Not support in this release.
USAGE_REPORT (33)	No	Not support in this release.
DEFAULT-EPS-BEARER-QOS_MODIFICATION_FAILURE (34)	No	3GPP only
USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE (35)	No	Not support in this release.
USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE (36)	No	Not support in this release.

1 Note [a]: The values not listed in the table may be added by 3GPP in future updates or releases.

2 Note [b]: The support of this event trigger depends on a future 3GPP change of the RAT-Type AVP (i.e. WiMAX  
3 addition is required).

#### 4 **15.4.2 Mapping Gxa Parameters between 3GPP and WiMAX**

5 The parameters used in Gxa interface are defined in 3GPP TS 29.212 [19]. In WiMAX-3GPP interworking, these  
6 AVPs may be used in CCR/RAA messages by the ASN-GW/BBERF to report information to the PCRF based on

- 1 the event triggers or requests from the PCRF, or be used in CCA/RAR messages by the PCRF to transfer the QoS
- 2 rules and event triggers to the ASN-GW/BBERF. The ASN-GW/BBERF shall perform mapping between WiMAX
- 3 parameters and Gxa AVPs for E2E QoS control.
- 4 The information received across the Gxa interface is illustrated in Table 15-2 along with an indication if it is
- 5 required and how it is used in WiMAX.

1

**Table 15-2 Mapping Gxa Parameters between 3GPP and WiMAX**

Attribute Name	Reference (29.212 [19] clause)	Description	Access Type	WiMAX Mapping	Need on Gxa for WiMAX access
3GPP-MS-TimeZone	3GPP TS 29.061 [20]	Indicate the offset between universal time and local time in steps of 15 minutes of where the MS/UE currently resides. The ASN-GW/BBERF uses this to report the MS's time zone to the PCRF.	All	No mapping required.	Yes
3GPP-SGSN-Address	3GPP TS 29.061 [20]	The IPv4 address of the SGSN.	3GPP-EPS	No mapping required.	No
3GPP-SGSN-IPv6-Address	3GPP TS 29.061 [20]	The IPv6 address of the SGSN.	3GPP-EPS	No mapping required.	No
AN-GW-Address	5.3.49	Carries the address of the ASN-GW/FA/MAG.	All	No mapping required.	Yes
3GPP-SGSN-MCC-MNC	3GPP TS 29.061 [20]	Carries the MCC/MNC information of the AN-GW.	All	No mapping required.	Yes[a]
3GPP-User-Location-Info	3GPP TS 29.061 [20]	Indicates details of where the UE is currently located (e.g. SAI or CGI)	3GPP-EPS	No mapping required.	No
3GPP2-BSID	3GPP2 X.S0057 [28]	The ASN-GW/BBERF reuse this to denote the WiMAX BSID of where the MS/UE is currently located.	3GPP2, Non-3GPP-EPS	No mapping required.	Yes
Access-Network-Charging-Identifier-Value	3GPP TS 29.214 [22]	Contains a charging identifier.	All	No mapping required. In WiMAX-3GPP interworking, the Charging-ID per PDN connection is carried in RRP/PBA message.	No
Allocation-and-Retention-Priority	5.3.32	Indicates a priority for accepting or rejecting a bearer establishment or modification request and dropping a bearer in case of resource limitations.	All	ASN-GW maps this to "Priority indication" TLV as defined in ETS section in NWG Rel 2.0 stage3 [1].	Yes
APN-Aggregate-Max-Bitrate-DL	5.3.39	Indicates the aggregate maximum bitrate for the downlink direction for all non-GBR bearers of the APN.	All	No mapping required.	Yes
APN-Aggregate-Max-Bitrate-UL	5.3.40	Indicates the aggregate maximum bitrate for the uplink direction for all non-GBR bearers of the APN.	All	No mapping required.	Yes

Attribute Name	Reference (29.212 [19] clause)	Description	Access Type	WiMAX Mapping	Need on Gxa for WiMAX access
Bearer-Control-Mode	5.3.23	Indicates the PCRF selected bearer control mode.	All	No mapping required. If the UE_ONLY mode is chosen by the PCRF, the ASN-GW/BBERF shall not initiate WiMAX QoS management procedure.	Yes
Called-Station-ID	IETF RFC 4005 [17]	The address the user is connected to (i.e. the PDN identifier).	All	No mapping required.	Yes
PDN-Connection-ID	5.3.58	The identification of PDN connection to the same APN.	All	No mapping required.	Yes[b]
CC-Request-Number	IETF RFC 4006 [18]	The number of the request for mapping requests and answers.	All	No mapping required.	Yes
CC-Request-Type	IETF RFC 4006 [18]	The type of the request (initial, update, termination).	All	No mapping required.	Yes
User-CSG-Information	3GPP TS 32.299 [27]	Indicates the user “Closed Subscriber Group” Information associated to CSG cell access.	3GPP-EPS	No mapping required.	No
Event-Trigger	5.3.7	Reports the event that occurred on the BBERF.	All	No mapping required. The event triggers supported by WiMAX are list in Table 15-1.	Yes
Flow-Description	3GPP TS 29.214 [22]	Defines the service flow filter parameters for a QoS rule.	All	The ASN-GW maps this to the classifier in “Packet Classification Rule” TLV including: IP Source/Destination Address and Mask, Source/Destination Port Range and Protocol.	Yes
Flow-Information	5.3.53	Defines the service flow filter parameters for a QoS rule and may include flow description, packet filter identifier, ToS/Traffic Class, SPI and Flow Label information. May also include an instruction as to whether signalling the information to the UE is to occur.	All	The ASN-GW maps this to the sub TLV of “SF Info”. See the mapping relationship of its sub-AVPs for detail.	Yes
Flow-Label	5.3.52	Defines the IPv6 flow label.	All	The ASN-GW maps this to the “IPv6 Flow Label” TLV.	Yes
Framed-IP-Address	IETF RFC 4005 [17]	The IPv4 address allocated for the user.	All	No mapping required.	Yes
Framed-IPv6-Prefix	IETF RFC 4005 [17]	The IPv6 prefix allocated for the user.	All	No mapping required.	Yes

Attribute Name	Reference (29.212 [19] clause)	Description	Access Type	WiMAX Mapping	Need on Gxa for WiMAX access
Guaranteed-Bitrate-DL	5.3.25	Defines the guaranteed bitrate for downlink.	All	The ASN-GW maps this to the “Minimum Reserved Traffic Rate” TLV.	Yes
Guaranteed-Bitrate-UL	5.3.26	Defines the guaranteed bitrate for uplink.	All	The ASN-GW maps this to the “Minimum Reserved Traffic Rate” TLV.	Yes
IP-CAN-Type	5.3.27	Indicates the type of Connectivity Access Network that the user is connected to. The ASN-GW/BBERF shall set this to “WIMAX(3)”.	All	No mapping required.	Yes
Max-Requested-Bandwidth-UL	3GPP TS 29.214 [22]	Defines the maximum authorized bandwidth for uplink.	All	The ASN-GW maps this to the “Maximum Sustained Traffic Rate” TLV.	Yes
Max-Requested-Bandwidth-DL	3GPP TS 29.214 [22]	Defines the maximum authorized bandwidth for downlink.	All	The ASN-GW maps this to the “Maximum Sustained Traffic Rate” TLV.	Yes
Packet-Filter-Content	5.3.54	Indicates the content of the packet filter.	All	The ASN-GW derives this from the “Packet Classification Rule” TLV in RR-Req.	Yes
Packet-Filter-Identifier	5.3.55	The identity of the packet filter.	All	The ASN-GW receives this from the PCRF and maps this to the “Classification Rule Index” TLV in RR-Req.	Yes
Packet-Filter-Information	5.3.56	Information related to the packet filters that the BBERF provides to the PCRF.	All	The ASN-GW derives this from the “Packet Classification Rule” TLV in RR-Req. See the sub-AVPs for detail.	Yes
Packet-Filter-Operation	5.3.57	Indicates the operation that the terminal is requesting over the packet filters provided by the Packet-Filter-Information AVPs.	All	The ASN-GW derives this from the “Classification Rule Action” TLV.	Yes
Packet-Filter-Usage	5.3.66	Indicates whether the UE shall be provisioned with the related traffic mapping information.	All	No mapping required.	Yes
Network-Request-Support	5.3.24	Indicates whether the UE and access network supports the network requested bearer control mode or not.	All	No mapping required.	Yes

Attribute Name	Reference (29.212 [19] clause)	Description	Access Type	WiMAX Mapping	Need on Gxa for WiMAX access
Precedence	5.3.11	Indicates the precedence of QoS rules or packet filters.	All	The ASN-GW maps this to the "Classification Rule Priority" TLV.	Yes
PCC-Rule-Status	5.3.19	Describes the status of one or a group of QoS rules.	All	No mapping required.	Yes
QoS-Class-Identifier	5.3.17	Identifies a set of IP-CAN specific QoS parameters	All	The ASN-GW maps this to the "QoS Parameters" TLV. See Annex D in [2] for detail.	Yes
QoS-Information	5.3.16	Defines the QoS information for a resource or QoS rule.	All	The ASN-GW maps this to the "QoS Parameters" TLV. See the sub-AVPs for detail.	Yes
Default-EPS-Bearer-QoS	5.3.48	Defines the QoS information of the default bearer	All	No mapping required.	No
RAI	3GPP TS 29.061 [20]	Contains the Routing Area Identity of the SGSN where the UE is registered	3GPP-EPS	No mapping required.	No
RAT-Type	5.3.31	Identifies the radio access technology that is serving the UE.	All	No mapping required.	No
Resource-Allocation-Notification	5.3.50	Indicates whether successful resource allocation notification for rules is needed or not.	All	No mapping required.	Yes
Rule-Failure-Code	5.3.38	Identifies the reason a QoS rule is being reported.	All	No mapping required.	Yes
Security-Parameter-Index	5.3.51	Defines the IPSec SPI.	All	No mapping required.	No
Session-Release-Cause	5.3.44	Indicate the reason of termination initiated by the PCRF. Only the reason code UNSPECIFIED_REASON is applicable for the PCRF-initiated Gxx session termination.	All	No mapping required.	Yes
Subscription-Id	IETF RFC 4006 [18]	The identification of the subscription (i.e. IMSI)	All	No mapping required.	Yes
Supported-Features	3GPP TS 29.229 [23]	If present, this AVP informs the destination host about the features that the origin host requires to successfully complete this command exchange.	All	No mapping required.	Yes
ToS-Traffic-Class	5.3.15	Defines the IPv4 ToS or IPv6 Traffic Class	All	The ASN-GW maps this to the IP TOS/DSCP Range and Mask TLV.	Yes
Trace-Data	3GPP TS 29.272 [24]	Contains trace control and configuration parameters, specified in 3GPP TS 32.422 [27]. This AVP shall have the 'M' bit cleared.	3GPP-EPS	No mapping required.	No

Attribute Name	Reference (29.212 [19] clause)	Description	Access Type	WiMAX Mapping	Need on Gxa for WiMAX access
Trace-Reference	3GPP TS 29.272 [24]	Contains the trace reference parameter, specified in 3GPP TS 32.422 [27]. This AVP shall have the 'M' bit cleared.	3GPP-EPS	No mapping required.	No
Tunnel-Header-Filter	5.3.34	Defines the tunnel (outer) header filter information of a tunnelled IP flow.	All	No mapping required.	No
Tunnel-Header-Length	5.3.35	Indicates the length of the tunnel (outer) header.	All	No mapping required.	No
Tunnel-Information	5.3.36	Defines the tunnel (outer) header information for an IP flow.	All	No mapping required.	No
User-Equipment-Info	IETF RFC 4006 [18]	The identification and capabilities of the terminal (IMEISV, etc.) When the User-Equipment-Info-Type is set to IMEISV(0), the value within the User-Equipment-Info-Value shall be a UTF-8 encoded decimal.	All	The ASN-GW sets this to indicate that the UE provides an IMSI-based ID.	Yes
QoS-Rule-Install	5a.3.1	Used to activate, install or modify QoS rules as instructed from the PCRF to the BBERF.	All	No mapping required.	Yes
QoS-Rule-Remove	5a.3.2	Used to deactivate or remove QoS rules from an Gateway Control session.	All	No mapping required.	Yes
QoS-Rule-Definition	5a.3.3	Defines the QoS rule for a service flow sent by the PCRF to the BBERF.	All	The ASN-GW maps this to the "SF Info" TLV. See the sub-AVPs for detail.	Yes
QoS-Rule-Name	5a.3.4	Defines a name for QoS rule.	All	No mapping required.	Yes
QoS-Rule-Base-Name	5a.3.7	Indicates the name of a pre-defined group of QoS rules	All	No mapping required.	Yes
QoS-Rule-Report	5a.3.5	Used to report the status of QoS rules.	All	No mapping required.	Yes
Session-Linking-Indicator	5a.3.6	Indicates whether the session linking between the Gateway Control Session and the Gx session must be deferred.	All	No mapping required.	Yes

- 1 Note [a]: This parameter could be provided if the ASN-GW is configured with the MCC/MNC by the operator.
- 2 Note [b]: Multiple PDN connection is not supported in this release. Only a single PDN connection ID can be
- 3 assigned to the WiMAX access network currently.
- 4

---

1 **16. MS/UE implications**

2 **16.1 MS/UE Identities**

3 MS/UE identities SHALL be as per section 4.6 of 3GPP TS 23.402 [4].

4 **16.2 CMIP4 security key derivation**

5 MS/UE SHALL derive CMIP4 security keys as per section 9.2.1.2.2 of TS 33.402 [5].

6 Note: This is not an implication on the MS/UE as CMIP4 security key derivation defined in TS 33.402 [5] and  
7 WiMAX specification [1] are same.

---

## 17. AAA implications

### 17.1 3GPP AAA (Informative)

3GPP AAA Server derives CMIP4 security keys as per section 9.2.1.2.2 of TS 33.402 [5].

CMIP4 security key derivation defined in TS 33.402 [5] and WiMAX specification [1] are the same.

### 17.2 WiMAX AAA Proxy Requirements

The WiMAX AAA Proxy SHALL support the STa+ application as defined in section 19 of this document toward the ASN-GW. Optionally the WiMAX AAA Proxy may support the STa application as defined in TS 29.273 [14] toward the ASN gateway. The application to be used on the interface between the WiMAX AAA Proxy and ASN-GW SHALL be negotiated as defined in RFC 3588 [30]. The WiMAX AAA Proxy SHALL support the STa interface to the 3GPP AAA server.

#### 17.2.1 Bi-directional translation between STa and STa+

When the STa+ application is negotiated the WiMAX AAA Proxy SHALL act as a translation agent between the two applications, as defined section 19 in this document, adding and removing information elements as required.

#### 17.2.2 STa Support

When the STa application is negotiated the WiMAX AAA proxy may adapt the information elements as defined in section 19 in this document.

#### 17.2.3 Accounting

The WiMAX AAA Proxy may receive accounting records from the WiMAX ASN-GW. In response to “Accounting Request” the AAA Proxy SHOULD send the ASN-GW an “Accounting Response” using “Acct-Status-Type” with the value set to “8” (i.e. Accounting-off).

The WiMAX AAA proxy SHOULD discard the accounting information.

---

## 18. Accounting implications

### 18.1 Charging requirements - no PCC framework

In a WiMAX® 3GPP EPC interworking scenario, the subscriber is assumed to have a 3GPP network subscription only. In 3GPP, typically the PDN-GW generates the accounting records & User Data Records (UDR) for any access technology. Accounting records for a non-PCC session using WiMAX access are generated by the 3GPP EPC & thus, no accounting records are needed from the WiMAX access.

Since the ASN-GW generates the accounting records as a mandatory default behavior, however the WiMAX accounting records are not needed for EPC IWK. Therefore, for EPC IWK, when the ASN-GW sends “Accounting Request” to the WiMAX AAA proxy, the WiMAX AAA proxy upon receiving “Accounting Request” SHOULD send an “Accounting Response” using “Acct-Status-Type” with the value set to “8” (i.e. Accounting-off).

Due to lack of accounting support on STa, the WiMAX AAA proxy SHOULD not forward the accounting information to the 3GPP AAA server.

### 18.2 PCC Charging Requirements at the ASN-GW

Off line accounting functionality in support of PCC may be provided by the ASN-GW. Accounting records at the ASN-GW are typically collected for correlation in the case of roaming or separate ownership of the access and core networks. When off-line PCC accounting is provided, the accounting client/the BBERF functions in the ASN-GW shall collect/generate accounting information for each MS/UE including information for data transmitted in the uplink and downlink directions.

A charging ID per PDN connection is assigned by the PDN-GW and then transferred to the BBERF/ASN-GW via Registration Reply or Proxy Binding Acknowledgement message. When PCC off-line accounting is provided, the BBERF shall generate the CDRs with the charging ID for the purpose of charging correlation in 3GPP EPC. The charging correlation between WiMAX access network and 3GPP network is out of the scope of this specification.

When off-line PCC accounting is provided by the ASN-GW/BBERF, the accounting related functionality shall be aligned with the accounting functionality defined for the S-GW in TS 23.401 [3]. The charging functions in the ASN-GW shall be supported as specified in TS 32.240 [25]. The behavior of the charging functions in the WiMAX ASN-GW/BBERF EPC domain, the reporting of the charging events and creation of the CDRs shall be as specified in TS 32.240 [25] and TS 32.251 [26].

---

## 19. WNAADA+ Description

### 19.1 General

The STa+ reference point is defined between the ASN-GW and the WiMAX AAA Proxy/Server or between an ASN-GW in the visited network and the WiMAX AAA Proxy/Server. The definition of the reference point and its functionality is given in section 5.3.

This section describes the WiMAX Network Access Authentication and Authorization Diameter Application Plus (WNAADA+) which is based on the WiMAX Network Access Authentication and Authorization Diameter Application (WNAADA) defined in Stage3 [1]. The WNAADA+ interworks with the 3GPP STa Diameter Application defined in 3GPP TS 29.273 [14], which operates between the WiMAX AAA Proxy/Server and the 3GPP AAA server over the STa reference point defined in 3GPP TS 29.273 [14].

Over the STa+ reference point, WNAADA+ Diameter application is used to authenticate and authorize the MS with the EPC network. This authentication involves the ASN-GW, the WiMAX AAA Proxy and the 3GPP-AAA Server in the HPLMN or in the case of roaming in a visited network that supports EPC, the authentication involves the ASN-GW, the WiMAX 3GPP AAA Proxy/Server, the 3GPP-AAA proxy server in the Visited PLMN and the 3GPP-AAA server in the HPLMN. The WNAADA+ Diameter application includes support for additional WiMAX specific functionality.

The WNAADA+ shall also be used to transport PMIPv6 or MIPv4 FA-CoA mode related mobility parameters depending upon which mode the UE uses to attach to the EPC over the S2a reference point. In particular, in this case the WNAADA+ may be used for conveying the Home Agent IP address, which may be obtained via FQDN DNS look up from the WIMAX Proxy AAA server to the ASN-GW supporting Home Agent discovery based on DHCPv6 (see TS 24.303 [33]).

The WNAADA+ may also be used to transport charging-related information and optionally information about IP Mobility Mode Selection according to 3GPP TS 29.273 [14].

This document does not address how roaming is achieved with roaming partners that do not support EPC IWK.

### 19.2 Diameter Capability Negotiation

The STa+ reference point shall support WNAADA+ as defined by this specification. The ASN-GW shall advertise support for WNAADA+ during Diameter Capability Exchange Procedure as described by RFC 3588 [30].

The CER message from the ASN-GW may indicate support for the STa Diameter Application by including the Vendor-Specific-Application-Id VSA with the Vendor-Id attribute of the Vendor-Specific-Application-Id set to the SMI Network Management Private Enterprise Codes assigned to 3GPP (10415) and the Auth-Application-Id set to the STa Diameter Application ID of 16777250 as assigned by IANA. If the ASN-GW supports the STa interface the procedures as defined in TS 29.273 [14] and TS 23.402 [4] are used and will not be addressed in this document.

The CER message from the WiMAX-AAA Proxy Server shall indicate support for WNAADA+ by including the Vendor Specific-Application-Id VSA. The CER message from the ASN-GW may indicate support for the WNAADA+ by including the Vender-Specific-Application-Id VSA. The Vendor-Id attribute of the Vendor-Specific-Application-Id shall be set to the SMI Network Management Private Enterprise Codes assigned to WiMAX (24757) and the Auth-Application-Id set to the WNAADA+ of TBD as assigned by IANA.

### 19.3 WNAADA+ Access Authentication and Authorization

#### 19.3.1 General

This section describes the procedures for Access (Re-)Authentication and Authorization between the ASN-GW in the access network and the WiMAX 3GPP AAA Proxy/Server when WNAADA+ is selected by the ASN-GW and the WiMAX 3GPP AAA Proxy Server.

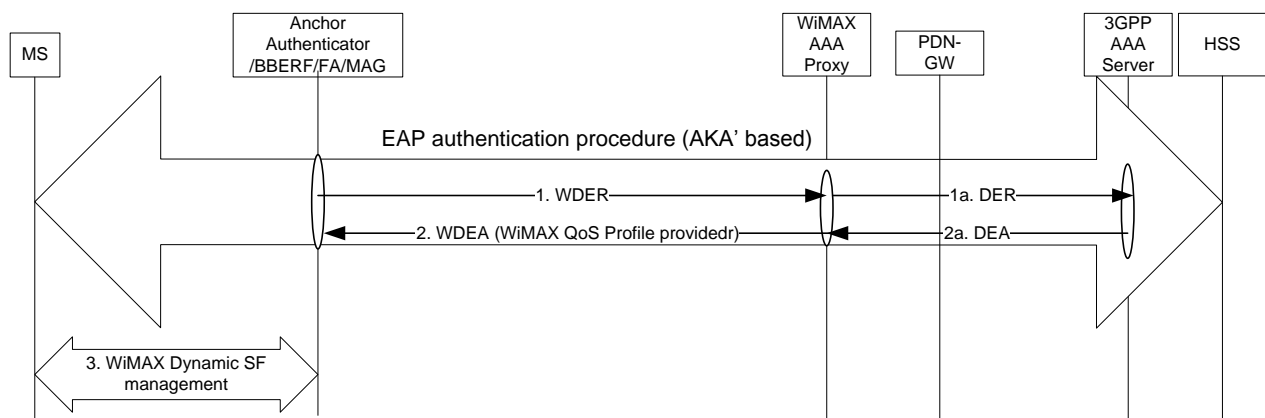
- 1 The WNAADA+ shall be used for authenticating and authorizing the UE for both PMIPv6 and MIPv4 FA-CoA  
2 mode.
- 3 The MS shall be authenticated using EAP-AKA' as defined by RFC 5448 [16]. The Authentication is terminated in  
4 the 3GPP-AAA server following the procedures in TS29.273 [14]. The MS identity shall conform to TS 23.402 [3]  
5 and TS 23.003 [10].
- 6 The role of the WiMAX 3GPP AAA proxy server is as follows:
- 7 Upon receiving a command (request or response) from the ASN-GW, the WiMAX AAA proxy server shall  
8 process the message and send the STa equivalent of the message over the STa interface to the 3GPP-  
9 AAA server, acting as a translation agent removing any WiMAX specific attributes that are not expected by  
10 the 3GPP-AAA. The WiMAX AAA proxy server may modify some of the attributes before forwarding the  
11 message to the 3GPP-AAA server.
- 12 Upon receiving a message over the STa interface (response or request) from the 3GPP-AAA server, the  
13 WiMAX AAA proxy processes the message, acting as a translation agent adding WiMAX specific  
14 attributes and/or modifying the 3GPP-AAA attributes as needed before sending the WNAADA+ version  
15 of the message to the ASN-GW.

### 16 19.3.2 Handling WiMAX Subscriber QoS Profile Information

17 The following stage 2 figure shows the retrieval of the WiMAX QoS information using WNAADA+ during the user  
18 authentication procedure.

19 The MS performs authentication with the 3GPP AAA using EAP-AKA's via the WiMAX AAA Proxy/Server and  
20 the Anchor Authenticator as described in sections 11.1 of this spec and 4.4.1.2.2 of stage 3 [1]. During  
21 authentication, the WiMAX subscriber QoS profile information SHALL be provided by the WiMAX AAA  
22 Proxy/Server upon successful authentication to the Anchor Authenticator.

23



24  
25

26 **Figure 19-1 – WiMAX QoS profile retrieval from the WiMAX AAA Proxy Server**

27 Step1: The Anchor Authenticator sends the WiMAX Diameter EAP authentication Request to the WiMAX AAA  
28 Proxy, which in turns forwards it to the 3GPP AAA using the DER message.

29 Step 2: Upon successful authentication and processing of the WDER and DEA messages, the WiMAX AAA  
30 Proxy/Server responds to the Anchor Authenticator with Diameter Success reply and, as done with any WiMAX  
31 initial entry, returns the subscriber WiMAX QoS information by translating the STa response from the 3GPP AAA  
32 to a WNAADA+ response.

33 Step 3: The QoS rules and event triggers received by the target Anchor Authenticator are passed to the BBERF,  
34 which initiates dynamic service flow management process as shown in Figure 15-1 steps 3-12.

1 **19.3.3 WNAADA+ WiMAX® Diameter-EAP-Request/Answer Commands**

2 **19.3.3.1 WiMAX® Diameter-EAP-Request (WDER) Command**

3 The WiMAX Diameter EAP-Request Command is derived from the DER Command as specified for the Diameter  
4 EAP Application in RFC 4072 [31] and is used to carry out EAP authentication between the ASN and the CSN.

5 The WiMAX® Network Access and Authorization Diameter Application extends the DER command by adding  
6 WiMAX specific AVPs:

7

8 <WiMAX Diameter-EAP-Request> ::= < Diameter Header: 8388609, REQ, PXY >  
                   \* \* \* \* \* \* \* \* \* \*           Attributes defined in RFC4072 [31].  
                   { Session-Id }  
                   { Auth-Application-Id }  
                   { Origin-Host }               The identity of the ASN-GW.  
                   { Origin-Realm }             The identity of the ASN-GW realm.  
                   { Destination-Realm }       The realm of the home network (3GPP-AAA).  
                   { Auth-Request-Type }  
                   { EAP-Payload }  
                   [ User-Name ]                The identity of the MS. NAI formatted as per TS  
   23.003 [10].  
                   [ Calling-Station-Id ]       MAC address of the device (see Section  
   5.4.3.1 in Stage 3 [1]).  
                   [ WiMAX-Capability ]         Not transferable to the 3GPP-AAA.  
                   [ WiMAX-Session-Id ]        Not transferable to the 3GPP-AAA.  
                   [ GMT-Time-Zone-Offset ]    Not transferable to the 3GPP-AAA.  
                   [ BS-ID ]                    Not transferable to the 3GPP-AAA.  
                   [ NAP-ID ]                   Not transferable to the 3GPP-AAA.  
                   [ NSP-ID ]                   Not transferable to the 3GPP-AAA.  
                   [ Operator-Name ]           The WiMAX WRI-Code of the VN-SP.  
                   \* [ AVP ]

9 **19.3.3.2 WiMAX® Diameter-EAP-Answer (WDEA) Command**

10 The WiMAX® Diameter EAP-Answer Command is derived from the DEA Command as specified for the Diameter  
11 EAP Application in RFC 4072 [31] and is used to carry out EAP authentication between the ASN and the CSN.

12 The WiMAX Diameter EAP-Answer Command is used to carry out EAP authentication between the ASN and the  
13 CSN. Upon successful authentication, the WiMAX Diameter EAP Answer Command as used in the context of the  
14 WiMAX Network Access and Authorization Diameter Application carries authorization attributes which include:

- 15     • The resulting keys from the EAP procedures;
- 16     • Authorization attributes such as IP address assignments, and flow description;
- 17     • Attributes used to bootstrap mobility service;
- 18     • Attributes used to bootstrap DHCP service.

- 1       • Attributes required to set up additional service flows.  
2 The WiMAX® Network Access and Authorization Diameter Application extends the DEA command by adding the  
3 following WiMAX AVPs:

4 <WiMAX Diameter-EAP-Answer> ::= < Diameter Header: 8388609, PXY >

* * * * *	Attributes defined in RFC4072 [31].
[ WiMAX-Capability ]	WiMAX AAA Proxy provides this value.
[ WiMAX-Session-Id ]	WiMAX AAA Proxy provides this value.
* [ Packet-Flow-Descriptor-V2 ]	WiMAX AAA Proxy could derive this from STa APN-Configuration AVP as defined in section 19.3.4.2.
[ QoS-Descriptor ]	WiMAX AAA Proxy could derive this from STa APN-Configuration AVP as defined in section 19.3.4.2.
* [ DNS ]	WiMAX AAA Proxy provides this value.
[ Operator-Name ]	WiMAX AAA Proxy provides this value. Contains the WRI-Code of the HNSP.
[ MS-Authenticated ]	WiMAX AAA Proxy provides this value.
[ Context-Identifier ]	Contains the default APN of the MS.

Proxy and Client MIP Support

[ PMIP-Authenticated-Network-Identity ]	Inserted by the Proxy and contains the true IMSI as it appears in the Mobile-Node-Identifier AVP received over STa.
[ hHA-IP-MIP4 ]	
[ hHA-IP-MIP6 ]	In the case of PMIPv6 this is the IP address of the authorized LMA in the home network.
[ FA-RK-MSA ]	For CMIP. WiMAX AAA Proxy constructs this group AVP from STa MIP-FA-RK and MIP-FA-SPI AVPs as defined in section 19.3.4.2.
[ HA-RK-MSA ]	For CMIP.[a]
[ hDHCPv4-Server ]	WiMAX AAA Proxy provides this value.
[ hDHCPv6-Server ]	WiMAX AAA Proxy provides this value.
[ hDHCP-Server-Parameters ]	WiMAX AAA Proxy provides this value.

Hot-Lining Services

[ Hotline-Profile-ID ]	WiMAX AAA Proxy provides this value.
[ HTTP-Redirection-Rule ]	WiMAX AAA Proxy provides this value.
[ IP-Redirection-Rule ]	WiMAX AAA Proxy provides this value.
[ NAS-Filter-Rule ]	WiMAX AAA Proxy provides this value.
[ Hotline-Session-Timer ]	WiMAX AAA Proxy provides this value.
[ Hotline-Indication ]	WiMAX AAA Proxy provides this value.

\* [ Time-Of-Day-Time ] WiMAX AAA Proxy provides this value.

Feature Information

[ Certified-MS-Feature-List-For-GW ] WiMAX AAA Proxy provides this value.  
]

[ Certified-MS-Feature-List-For-BS ] WiMAX AAA Proxy provides this value.

\* [ AVP ]

1  
2 Note [a]: Need to add in 3GPP a CR so that the 3GPP-AAA generates HA-RK and HA-RK-SPI. Otherwise ASN-  
3 GW will have to change its behaviour when IWK with 3GPP EPC core and not expect this key for MIP session  
4 revocation.

5 **19.3.4 WiMAX AAA Proxy/Server STa to STa+ Translation Requirements**

6 **19.3.4.1 Translation of DER message**

7 The following describes how the WiMAX AAA Proxy/Server generates an STa DER from a WNAADA+ WDER  
8 command. A column indicates if a particular attribute is MANDATORY (M) to include or OPTIONAL  
9 (O)/CONDITIONAL(C) or NOT USED(X).

10 < Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >

< Session-Id >	M	Generated at the WiMAX AAA Proxy/Server.[a]
{ Auth-Application-Id }	M	As per 29.273 [14].
{ Origin-Host }	M	WiMAX-AAA Proxy/Server overwrites this attribute with its host information.[a]
{ Origin-Realm }	M	WiMAX AAA Proxy/Server overwrites this attribute with its host information.[a]
{ Destination-Realm }	M	From WNAADA+ DER.
{ Auth-Request-Type }	M	From WNAADA+ DER.
{ EAP-Payload }	M	From WNAADA+ DER.
[ User-Name ]	M	From WNAADA+ DER.
[ Calling-Station-Id ]	M	The Layer-2 address of the UE which is the MAC address received in the WNAADA+ DER Calling-Station-Id attribute. The Proxy will need to translate this attribute if received in a format not supported by the 3GPP-AAA server.
[ RAT-Type ]	M	Inserted by WiMAX-AAA Proxy/Server as per TS 29.212 [19]. [b]
[ ANID ]	M	Inserted by WiMAX-AAA Proxy/Server. As per TS 24.302 [9] it is set to the string “WIMAX” where the quotes are not part of the string.
[ MIP6-Feature-Vector ]	C	- MIP6_INTEGRATED, always supported - PMIP6_SUPPORTED In DER, this can be mapped from WDER ASN-Network-Service-Capabilities AVP Bit#11; - MIP4_SUPPORTED In DER, this can be mapped from WDER ASN-Network-Service-Capabilities AVP Bit#4; - ASSIGN_LOCAL_IP (not supported) OPTIMIZED_IDLE_MODE_MOBILITY (not supported)
*[ AVP ]		

- 1  
2 Note [a]: The WiMAX AAA Proxy/Server asserts its host and realm identity to the 3GPP AAA. The 3GPP AAA  
3 only sees one ASN-GW. The WiMAX AAA Proxy/Server hides all ASN-GW handovers.  
4 Note [b]: The support of this AVP depends on a future 3GPP change of the RAT-Type AVP (i.e. WiMAX addition  
5 is required).

6 **19.3.4.2 Translation of DEA message**

7  
8 The following describes how the WiMAX AAA Proxy/Server process the attributes of STa DEA command received  
9 from the 3GPP-AAA over STa in formulating the WNAAADA+ WDEA command. A column indicates if a  
10 particular attribute is MANDATORY (M) to include or OPTIONAL (O)/CONDITIONAL(C) or NOT USED(X).

11

12 < Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >

< Session-Id >	M	Not forwarded by the WiMAX AAA Proxy.
{ Auth-Application-Id }	M	Not forwarded by the WiMAX AAA Proxy.
{ Result-Code }	M	Forwarded to the ASN-GW.
[ Experimental-Result ]	O	Not forwarded by the WiMAX AAA Proxy.
{ Origin-Host }	M	Forwarded to the ASN-GW.
{ Origin-Realm }	M	Forwarded to the ASN-GW.
{ Auth-Request-Type }	M	Forwarded to the ASN-GW.
{ EAP-Payload }	M	Forwarded to the ASN-GW.
[ User-Name ]	M	Forwarded to the ASN-GW.
[ Session-Timeout ]	O	Forwarded to the ASN-GW.
[ Accounting-Interim-Interval ]	O	Forwarded to the ASN-GW.
[ EAP-Master-Session-Key ]	O	Forwarded to the ASN-GW.
[ Context-Identifier ]	C	The default APN of the user and is included only when PMIPv6 is indicated.
[ APN-OI-Replacement ]	C	Used to construct the Domain Name of the PDN GW for PMIPv6. It has lower priority then the APN-OI-Replacement received in the APN-Configuration. The WiMAX AAA Proxy Server uses this attribute per 3GPP 23.003 [10] to replace the domain part of the FQDN of the PDN-GW for PMIPv6 and determine the IP address to use in WNAAADA+ hHA-IP-MIP6 AVP.
[ APN-Configuration ]	C	APN-Configuration may include: (PMIPv6) - APN (shall be the default APN) - Authorized 3GPP QoS profile (map to Packet-Flow-Descriptorv2 and QoS-Descriptor. For the mapping relationship of the sub-AVPs, refer to Table 15-2)[a] - Statically allocated User IP Address (IPv4 and/or IPv6)(map to Framed-IP-Address/ Framed-IPv6-Prefix)[b] - Allowed PDN types (IPv4, IPv6, IPv4v6)(This value is not forwarded by the WiMAX AAA Proxy) - PDN GW identity (maps to hHA-IP-MIP4/ hHA-IP-MIP6). WiMAX AAA Proxy may perform DNS lookup to translate the FQDN to the PDN-GW IP address. - PDN GW allocation type(this value is not forwarded by the WiMAX AAA proxy) - VPLMN Dynamic Address Allowed(this value is not forwarded by the WiMAX AAA proxy)
[ MIP6-Feature-Vector ]	C	This information element shall only be sent if the

		<p>Result-Code AVP is set to DIAMETER_SUCCESS.</p> <ul style="list-style-type: none"> <li>- MIP6_INTEGRATED, always supported</li> <li>- PMIP6_SUPPORTED</li> </ul> <p>In DEA, this is mapped to WDEA Authorized-Network-Services AVP Bit#4 in the WiMAX capability AVP;</p> <ul style="list-style-type: none"> <li>- MIP4_SUPPORTED</li> </ul> <p>In DEA, this is mapped to Authorized-Network-Services AVP Bit#0 in the WiMAX capability AVP;</p> <ul style="list-style-type: none"> <li>- ASSIGN_LOCAL_IP (not supported)</li> <li>- OPTIMIZED_IDLE_MODE_MOBILITY (not supported)</li> </ul>
[ Mobile-Node-Identifier ]	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. Used as the PMIP-Authenticated-Network-Identity
*[ Redirect-Host ]	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. Not forwarded to the ASN-GW
[ AN-Trusted ]	C	This AVP shall be included only in the first authentication and authorization response. Not forwarded by WiMAX AAA Proxy. If the AN-Trusted is not set to “TRUSTED” then the WiMAX-AAA Proxy Server shall reject the session.
[ MIP-FA-RK ]	C	This AVP shall be present if MIPv4 is used, MN-FA authentication extension is supported and the Result-Code AVP is set to DIAMETER_SUCCESS. WiMAX AAA Proxy uses this to construct FA-RK-MSA.
[ MIP-FA-RK-SPI ]	C	This AVP shall be present if MIP-FA-RK is present. WiMAX AAA Proxy uses this to construct FA-RK-MSA.
*[ Supported-Features ]	O	Not forwarded by WiMAX AAA Proxy.
...		
*[ AVP ]	O	Forwarded to the WiMAX AAA Proxy.

1

2 Note [a]: AMBR is not supported by WiMAX network in this release. To set the equivalent bitrate of a WiMAX  
3 service flows, the PCC architecture may be used, or it may be based on the user profile provided by the WiMAX  
4 AAA Proxy or based on a translation of the AMBR AVP provided by the 3GPP AAA to the Maximum-Sustained-  
5 Traffic-Rate AVP or alternatively based on a default user profile set by the operator and sent to the Anchor  
6 SFA/ASN-GW.

7 Note [b]: This is depended on a future CR to Rel1.6 stage3.

### 8 19.3.4.3 Result-Code and Experimental-Result Handling by WiMAX-AAA Proxy/Server

9 The following table lists the values that may be received by the WiMAX-AAA Proxy/Server from the 3GPP-AAA  
10 server in the Experimental-Result AVP over STa.

11 WiMAX does not have an equivalent attribute thus the WiMAX-AAA Proxy/Server does not forward this attribute.  
12 The Experimental-Result-Codes are for informational only. The WiMAX-AAA Proxy/Server forwards the Result-  
13 Code AVP to the WNAADA+.

STa Experimental-Result-Code	Code	Description	WiMAX AAA Proxy/Server action over STa+
DIAMETER_ERROR_USE	5001	Indicates that the user	Use RESULT-CODE

R_UNKNOWN		identified by the IMSI is unknown.	received from STa.
DIAMETER_ERROR_ROAMING_NOT_ALLOWED	5004	Indicate that the subscriber is not allowed to roam in a certain non-3GPP V-PLMN.	Use RESULT-CODE received from STa.
DIAMETER_ERROR_USE_R_NO_NON_3GPP_SUBSCRIPTION	5450	Indicate that no non-3GPP subscription is associated with the IMSI.	Use RESULT-CODE received from STa.
DIAMETER_ERROR_USE_R_NO_APN_SUBSCRIPTION	5451	Indicate that the requested APN is not included in the user's profile, and therefore is not authorized for that user.	Use RESULT-CODE received from STa.
DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED	5452	Indicates the RAT type the UE is using is not allowed for the IMSI.	Use RESULT-CODE received from STa.

## 1 19.4 Commands for WNAANA+ HSS/AAA Initiated Detach

### 2 19.4.1 Abort-Session-Request (ASR) Command

3 The Abort-Session-Request (ASR) command, indicated by the Command-Code field set to 274 and the "R" bit set in  
4 the Command Flags field, is sent from a WiMAX AAA proxy to the WiMAX ASN-GW. ABNF for the ASR  
5 commands is as follows:

```
6         < Abort-Session-Request > ::= < Diameter Header: 274, REQ, PXY, 16777250 >
7         < Session-Id >
8         { Origin-Host }
9         { Origin-Realm }
10        { Destination-Realm }
11        { Destination-Host }
12        { Auth-Application-Id }
13        [ User-Name ]
14        [ Auth-Session-State ]
15        ...
16        *[ AVP ]
17
```

### 18 19.4.2 Abort-Session-Answer (ASA) Command

19 The Abort-Session-Answer (ASA) command, indicated by the Command-Code field set to 274 and the "R" bit  
20 cleared in the Command Flags field, is sent from a WiMAX ASN-GW to a WiMAX AAA Proxy. ABNF for the  
21 ASA commands is as follows:

```
22
23        < Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777250 >
24        < Session-Id >
25        { Result-Code }
26        { Origin-Host }
27        { Origin-Realm }
28        ...
29        *[ AVP ]
```

1 **19.4.3 Session-Termination-Request (STR) Command**

2 The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R"  
 3 bit set in the Command Flags field, is sent from the WiMAX ASN-GW to a WiMAX AAA Proxy. The Command  
 4 Code value and ABNF are re-used from the IETF RFC 3588 [30] Session-Termination-Request command.

```
5 <Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777250 >
6 < Session-Id >
7 { Origin-Host }
8 { Origin-Realm }
9 { Destination-Realm }
10 { Auth-Application-Id }
11 { Termination-Cause }
12 [ User-Name ]
13 ...
14 *[ AVP ]
```

15 **19.4.4 Session-Termination-Answer (STA) Command**

16 The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit  
 17 cleared in the Command Flags field, is sent from a WiMAX AAA Proxy to the WiMAX ASN-GW. The Command  
 18 Code value and ABNF are re-used from the IETF RFC 3588 [30] Session-Termination-Answer command.

```
19 <Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777250 >
20 < Session-Id >
21 { Result-Code }
22 { Origin-Host }
23 { Origin-Realm }
24 *[ AVP ]
```

25 **19.5 Commands for Re-Authentication and Re-Authorization Procedure**

26 **19.5.1 Re-Auth-Request (RAR) Command**

27 The Diameter Re-Auth-Request (RAR) command, indicated by the Command-Code field set to 258 and the "R" bit  
 28 set in the Command Flags field, is sent from a WiMAX AAA Proxy to a WiMAX ASN-GW. ABNF for the RAR  
 29 command is as follows:

```
30
31 < Re-Auth-Request > ::= < Diameter Header: 258, REQ, PXY, 16777250 >
32 < Session-Id >
33 { Origin-Host }
34 { Origin-Realm }
35 { Destination-Realm }
36 { Destination-Host }
37 { Auth-Application-Id }
38 { Re-Auth-Request-Type }
39 [ User-Name ]
40 ...
41 *[ AVP ]
```

42 **19.5.2 Re-Auth-Answer (RAA) Command**

43 The Diameter Re-Auth-Answer (ASA) command, indicated by the Command-Code field set to 258 and the "R" bit  
 44 cleared in the Command Flags field, is sent from a WiMAX ASN-GW to a WiMAX AAA proxy. ABNF for the  
 45 RAA commands is as follows:  
 46

```

1      < Re-Auth-Answer > ::=
2
3      < Diameter Header: 258, PXY, 16777250 >
4      < Session-Id >
5      { Result-Code }
6      { Origin-Host }
7      { Origin-Realm }
8      ...
9      *[ AVP ]

```

### 8 19.5.3 AA-Request (AAR) Command

9 The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the  
10 Command Flags field, is sent from a WiMAX GW to a WiMAX AAA Proxy. The ABNF is re-used from the IETF  
11 RFC 5779 [32].

```

12
13      < AA-Request > ::=
14
15      < Diameter Header: 265, REQ, PXY, 16777250 >
16      < Session-Id >
17      { Auth-Application-Id }
18      { Origin-Host }
19      { Origin-Realm }
20      { Destination-Realm }
21      { Auth-Request-Type }
22      [ Destination-Host ]
23      [ User-Name ]
24      [ MIP6-Feature-Vector ]
25      ...
26      *[ AVP ]

```

### 26 19.5.4 AA-Answer (AAA) Command

27 The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the  
28 Command Flags field, is sent from a WiMAX AAA Proxy to a WiMAX ASN-GW. The ABNF is re-used from the  
29 IETF RFC 5779 [32].

```

30      < AA-Answer > ::=
31
32      < Diameter Header: 268, PXY, 16777250 >
33      < Session-Id >
34      { Auth-Application-Id }
35      { Auth-Request-Type }
36      { Result-Code }
37      [ Experimental-Result ]
38      { Origin-Host }
39      { Origin-Realm }
40      [ Session-Timeout ]
41      [ Context-Identifier ]
42      [ APN-OI-Replacement ]
43      [ APN-Configuration ]
44      ...
45      *[ AVP ]

```