



WiMAX Forum[®] Network Architecture

Interworking Specification

WiMAX[®] – Pre-Release 8 3GPP Interworking

WMF-T37-008-R016v01

WiMAX Forum[®] Approved

(2010-11-30)

WiMAX Forum Proprietary

Copyright © 2010 WiMAX Forum. All Rights Reserved.

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

2
3 Copyright 2010 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, provided that all copies contain all proprietary notices
7 and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or
8 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
57 Forum. All other trademarks are the property of their respective owners.

58

1 **TABLE OF CONTENTS**

2 2.1 Abbreviations2
3 2.2 Terms & Definitions3
4 4.1 Access Credentials Principles.....5
5 4.1.1 Dual Sets of Access Credentials5
6 4.1.2 Single Set of Access Credentials.....5
7 5.1 Non-Roaming Architecture6
8 5.2 Roaming Architecture.....7
9 5.3 Pre-Rel8 Interworking Function7
10 5.4 Reference point mapping8
11 7.1 Initial Attach to 3GPP requesting IPv4 PDP context.....10
12 7.2 Initial Attach to 3GPP requesting IPv6 PDP context.....12
13 7.3 MS requirements.....13
14 7.4 PRIF Requirements.....14
15 7.5 AAA Requirements15
16 7.6 HA/LMA Requirements15
17 8.1 Initial WiMAX® Network Entry for IPv4 Services16
18 8.2 Initial WiMAX® Network Entry for IPv6 services18
19 8.3 AAA Requirements19
20 8.4 MS Requirements19
21 8.5 ASN GW Requirements19
22 9.1 Access Authentication21
23 9.2 Mobility Security.....21
24 9.2.1 PMIP4 considerations.....21
25 9.2.2 PMIP6 considerations.....21
26 9.3 Inter-node Security22
27 10.1 WiMAX® to 3GPP Pre-Rel8 Packet Core Handover for IPv4 service23
28 10.2 WiMAX® to 3GPP Pre-Rel8 Packet Core Handover for IPv6 service24
29 10.3 Requirements for WiMAX® to 3GPP Pre-Rel8 Packet Core Handover25
30 10.3.1 MS Requirements.....25
31 10.3.2 HA/LMA Requirements.....25
32 10.3.3 AAA Requirements.....26
33 10.3.4 PRIF Requirements26
34 10.4 Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX® for IPv4 service26
35 10.5 Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX® in case of IPv6 service28
36 10.6 Requirements for Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX®29
37 10.6.1 MS Requirements.....29
38 10.6.2 HA/LMA Requirements.....29
39 10.6.3 AAA Requirements.....30
40 10.6.4 ASN GW Requirements.....30
41 11.1 Network exit procedure initiated by MS or 3GPP Pre-Rel8 core network31
42 11.2 Network exit procedure initiated by the HA/LMA.....32
43 11.3 Network exit procedure initiated by the FA/MAG32
44 11.4 Network Exit Procedure initiated by the AAA33
45 11.5 PRIF Requirements.....34
46 13.1 Accounting Information Collection37
47 13.2 PRIF Accounting Requirements37
48 14.1 WiMAX® AAA Requirements38
49 15.1 WiMAX-NAS-Type39
50 B.3.1 PCEF re-location during HO from 3GPP to WiMAX®44
51 B.3.2 PCEF re-location during HO from WiMAX® to 3GPP.....46
52
53

1. Introduction and Document Scope

This document defines the core network aspects of interworking between Mobile WiMAX® and 3GPP Pre-Release8 Packet Switched Core Network [4] (referred to as “3GPP Pre-Rel8 Packet Core” in the rest of the document) systems.

The solution described in this document allows seamless data mobility between WiMAX subscribers and large base of existing legacy 3GPP packet data subscribers without impact on deployed 3GPP network elements.

This document describes Interworking solution for Dual Radio MS that is capable of simultaneously transmitting and receiving on both WiMAX and 3GPP Radio. It also assumes that the terminal can communicate simultaneously with both WiMAX and 3GPP Pre-Rel8 Packet Core points of attachment. Interworking solution for Single Radio MS is described in separate specification.

Furthermore, this document considers both non-roaming and roaming scenarios. Note that 3GPP Pre-Rel 8 roaming is fully covered by [7] and [8], and is out of scope of this document.

2. Abbreviations and Definitions

2.1 Abbreviations

Abbreviation	Expansion of Abbreviation
AAA	Authentication Authorization Accounting
APN	Access Point Name
DR	Dual Radio
FA	Foreign Agent
GGSN	Gateway GPRS Support Node
HLR	Home Location Register
HNP	Home Network Prefix
HO	HandOver
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MCC	Mobile Country Code
MNC	Mobile Network Code
MS	Mobile Station
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PLMN	Public Land Mobile Network
PRIF	Pre-Rel8 Interworking Function
RRQ	Registration Request

Abbreviation	Expansion of Abbreviation
RRP	Registration Response
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SPI	Security Parameter Index
USIM	Universal Subscriber Identity Module

1
2

3 2.2 Terms & Definitions

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

6 **Dual Radio Terminal:** Dual radio terminal can have both radios ON and is capable of simultaneous transmitting
7 and receiving on both (WiMAX® and 3GPP) radios.

8
9

3. References

- 1
- 2
- 3 [1] WMF-T33-001-R016, WiMAX Forum® Network Architecture- Detailed Protocols and Procedures Base
4 Specification
- 5 [2] WiMAX Forum® Mobile System Profile
- 6 [3] 3GPP TS 29.061: “Interworking between PLMN supporting packet based service and PDN (Release 7)”
- 7 [4] 3GPP TS 23.060: “GPRS Service description; Stage 2 (Release 7)”
- 8 [5] 3GPP TS 23.234: “3GPP system to WLAN Interworking; System description (Release 7)”
- 9 [6] 3GPP TS 23.003: “3GPP Numbering, addressing and identification (Release 7)”
- 10 [7] 3GPP TS 29.060: “GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 7)”
- 11 [8] 3GPP TS 23.002: “Network architecture (Release 7)”
- 12 [9] WMF-T33-001-R016, WiMAX Forum® Network Architecture- Detailed Protocols and Procedures Base
13 Specification
- 14 [10] 3GPP TS 33.210: “Network Domain Security, IP Network Layer Security (Release 7)”
- 15 [11] RFC 5176, Dynamic Authorization Extension to Remote Authorization Dial In User Service (RADIUS)
- 16 [12] RFC 2866, RADIUS Accounting
- 17 [13] RFC 2869, RADIUS Extensions
- 18 [14] RFC 3588, Diameter Base Protocol
- 19 [15] 3GPP TS 03.20: “Security related network functions (Release 1999)”
- 20 [16] 3GPP TS 33.102: “Security architecture (Release 8)”
- 21

1 **4. General Requirements and Principles**

2 **4.1 Access Credentials Principles**

3 In order to access the serving network, the dual mode MS identifies itself with the subscription credentials.
4 Credential dependency on the deployment models is described in Annex A. The dual radio MS may have either two
5 independent sets of credentials with both 3GPP Pre-Rel8 network and WiMAX® network, or a single active set of
6 credentials with the Home 3GPP Pre-Rel8 network.

7 Due to the limitations of the 3GPP Pre-Rel8 Packet Core legacy network, a single set of credentials at the WiMAX
8 network is not considered.

9 **4.1.1 Dual Sets of Access Credentials**

10 The dual radio MS may maintain two independent sets of credentials: one set with the 3GPP Pre-Rel8 HLR for
11 access to the 3GPP Pre-Rel8 network and another with the WiMAX AAA for access to the WiMAX network. In
12 such case, each accessed network conducts its own access authentication, e.g., SIM/USIM for the 3GPP Pre-Rel8
13 Packet Core access as described in 3GPP TS 03.20 [15] and 3GPP TS 33.102 [16] and EAP-based authentication
14 (e.g.: EAP-AKA, EAP-TTLS) for the WiMAX access as described in WiMAX Forum® Network Architecture stage
15 3 specification [1].

16 When dual set of access credentials are used, independent MS subscriptions are retained at the WiMAX AAA and
17 the 3GPP HLR/HSS, i.e. the WiMAX AAA contains the WiMAX subscription record associated with MS NAI, and
18 the 3GPP HLR/HSS contains the 3GPP Pre-Rel8 network subscription record associated with the IMSI. In this case,
19 the interface between the WiMAX AAA and the 3GPP HLR/HSS is not required.

20 **4.1.2 Single Set of Access Credentials**

21 The dual radio MS may maintain a single set of credentials with the 3GPP Pre-Rel8 HLR/HSS for accessing to both
22 the 3GPP Pre-Rel8 network and the WiMAX network. In this case, the UE on 3GPP Pre-Rel8 access is
23 authenticated by the 3GPP HLR/HSS using SIM/USIM and the MS, for the WiMAX access, is authenticated with
24 the WiMAX AAA, which uses the 3GPP HLR/HSS as the source of authentication parameters for conducting the
25 EAP Access Authentication.

26 When a single set of access credentials is used, the WiMAX AAA may request assistance from the 3GPP HLR/HSS.
27 In such a case, the single MS subscription is retained at the 3GPP HLR/HSS. The WiMAX AAA requests the
28 Authentication Vector (AV) from the HLR/HSS over the Gr'/Wx interface and uses it to conduct the EAP
29 authentication of the MS for the WiMAX access.

5. 3GPP Pre-Rel 8 Interworking Architecture Reference Model

This section defines the Network Reference Model (NRM) for the interworking of the Mobile WiMAX® system with the 3GPP pre-rel8 system defined in the 3GPP TS 23.060 [7] and TS 29.061 [3]. This NRM applies for a dual radio terminal.

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

5.1 Non-Roaming Architecture

This section describes the non-roaming architecture for interworking between WiMAX® and Pre-rel8 3GPP networks.

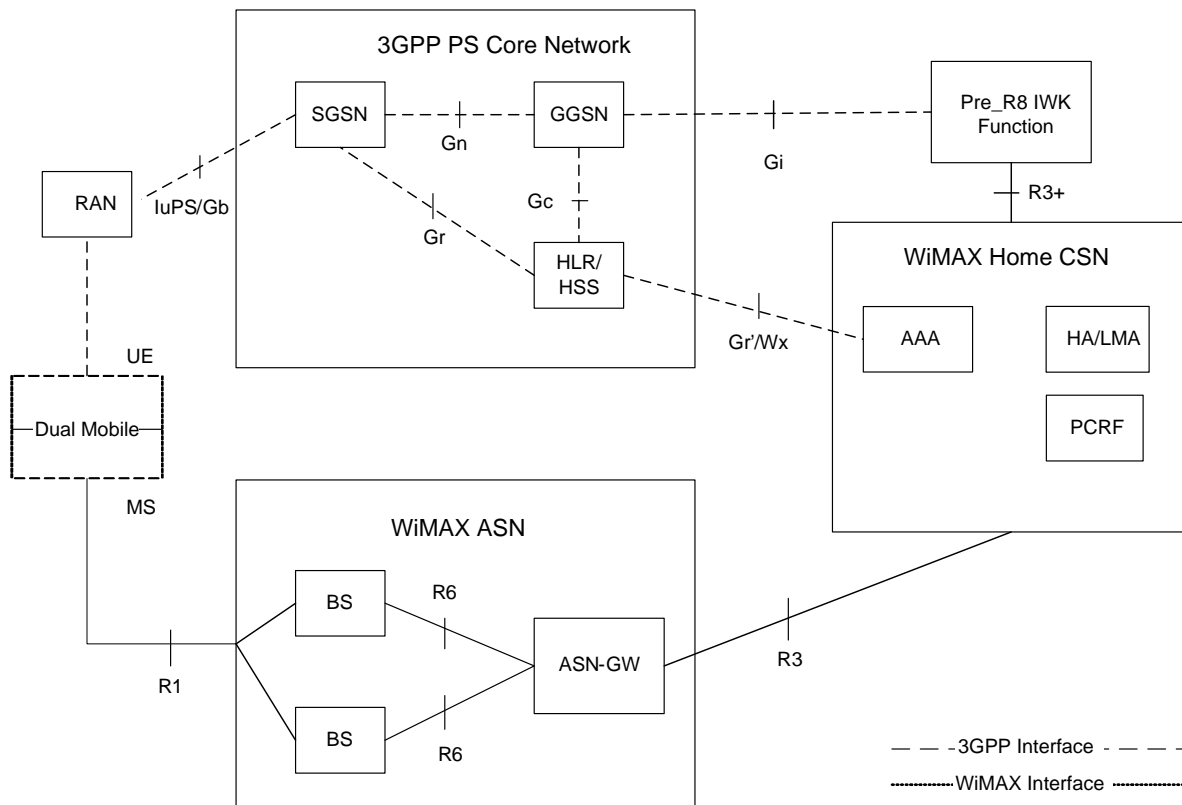


Figure 6-1 - WiMAX® - 3GPP Pre-Rel8 Interworking non-roaming Architecture

Figure 6-1 shows the dual radio 3GPP Pre-Rel 8 Interworking Network Non-roaming Reference Model, in which the Pre-Rel8 Interworking Function (PRIF) is introduced and interfaces with the GGSN through the Gi interface. The functionality of the Gi interface for the interworking is specified in 3GPP TS 29.061 [3].

The HLR location is business deployment dependent, for example it can also be located in the Home CSN.

5.2 Roaming Architecture

This section describes the roaming architecture for interworking between WiMAX® and Pre-rel8 3GPP networks.

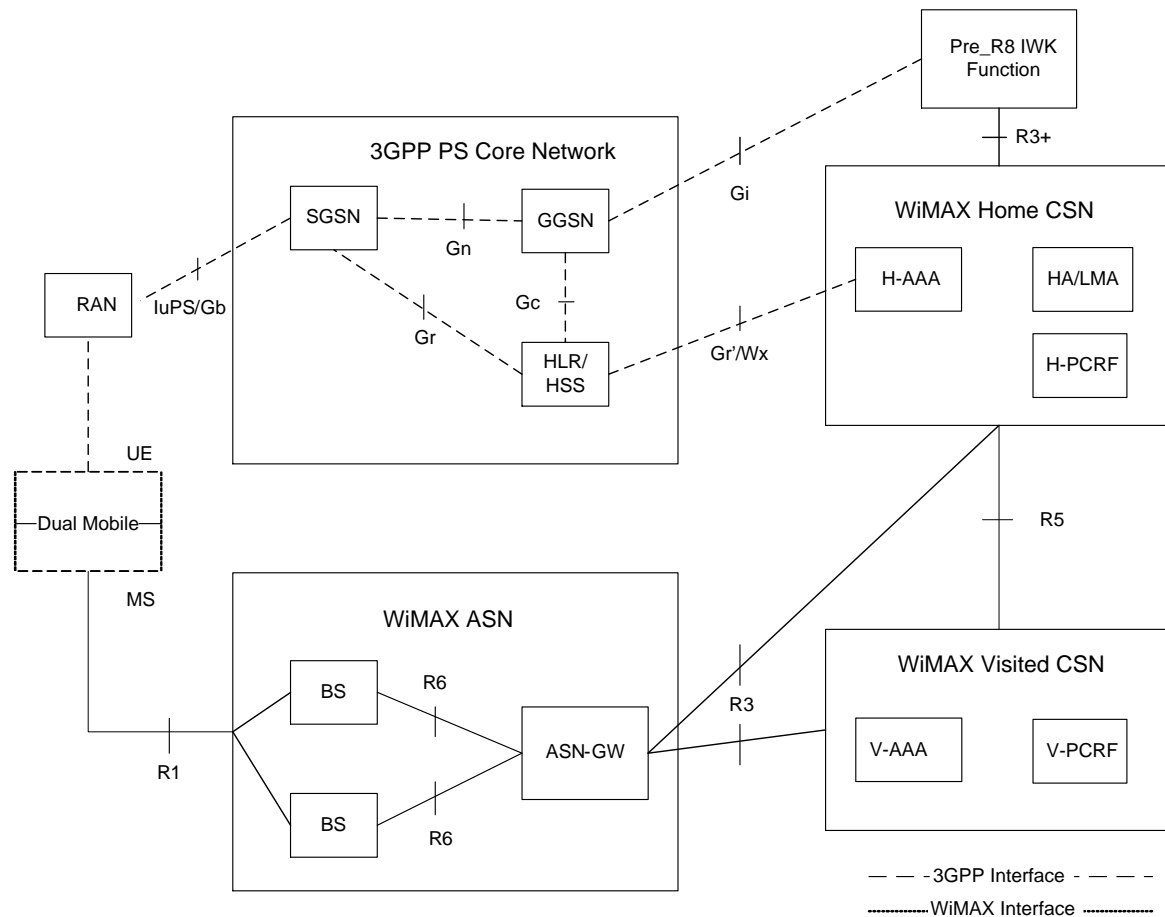


Figure 6-2 - WiMAX® - 3GPP Pre-Rel8 Interworking roaming Architecture

Figure 6-2 shows the dual radio 3GPP Pre-Rel8 Interworking Network Roaming Reference Model, in which the Pre-Rel8 Interworking Function (PRIF) interfaces with the home 3GPP GGSN through the Gi interface described in [3]. The 3GPP roaming cases between visited and home 3GPP networks are covered by the 3GPP standards and the WiMAX roaming cases between V-CSN and H-CSN are described in [1].

The link between the ASN-GW and the H-CSN SHALL be consistent with the NWG NRM (i.e. R3 compliant).

5.3 Pre-Rel8 Interworking Function

The Pre-Rel8 IWK Function (PRIF) is new logical function introduced for interworking between WiMAX® and Pre-Rel8 3GPP systems. PRIF is composed of following functionalities:

- AAA proxy

- 1 • Accounting Client located with the FA/MAG for metering and generating UDRs and sending accounting
- 2 messages to the accounting server in the CSN (AAA). The bearer traffic metering function is optional.
- 3 • In case IPv4 support
- 4 o PMIP4 client and a FA
- 5 • In case of IPv6 support
- 6 o MAG
- 7 o Authenticator function (for generation of the MAG-LMA-PMIP6 key)
- 8 It connects with the 3GPP Pre-Rel 8 network using the Gi interface and to the CSN using R3+ interface.

9 **5.4 Reference point mapping**

10

11 This section lists all the reference points that are used for the WiMAX® - Pre-Rel8 3GPP Interworking:

12

13 Gi - Reference point between GPRS and a packet data network. Defined in [4]

14 Gc - Reference point between the GGSN and an HLR. Defined in [8]

15 Gn - Reference point between two GGSNs within the same PLMN. Defined in [7]

16 Gr - Reference point between an SGSN and an HLR. Defined in [8]

17 Gr' - Reference point between a Pre-Rel8 HSS/HLR and a 3GPP AAA Server/Proxy. Defined in [5]

18 R3 - Reference point between ASN and CSN. Defined in [1]

19 R3+ - R3 plus PMIP4/PMIP6

20 R6 - Reference point between BS and ASN-GW within the same ASN. Defined in [1]

21 R1 - Reference point between MS and BS. Defined in [1]

22 R4 - Reference point between ASN-GWs within or across ASN(s). Defined in [1] Wx - Reference point between an

23 HSS and a 3GPP AAA Server. Defined in [5]

24

1 **6. Access Network Discovery and Selection**

2 Dual Radio terminal has an ability to discover available 3GPP and/or WiMAX® access networks independent of
3 each other. The dual radio terminal uses WiMAX specific procedure for WiMAX NAP/NSP discovery [1] and
4 3GPP specific procedures for 3GPP PLMN Discovery [4]. Dual radio terminal is able to arbitrate connectivity to the
5 network of choice based on radio conditions, user preferences - if so permitted, and/or pre-configured operator
6 policy. The specific procedures employed by the dual mode terminal for choosing an access network are outside the
7 scope of this specification.
8

7. Initial Attach to 3GPP

7.1 Initial Attach to 3GPP requesting IPv4 PDP context

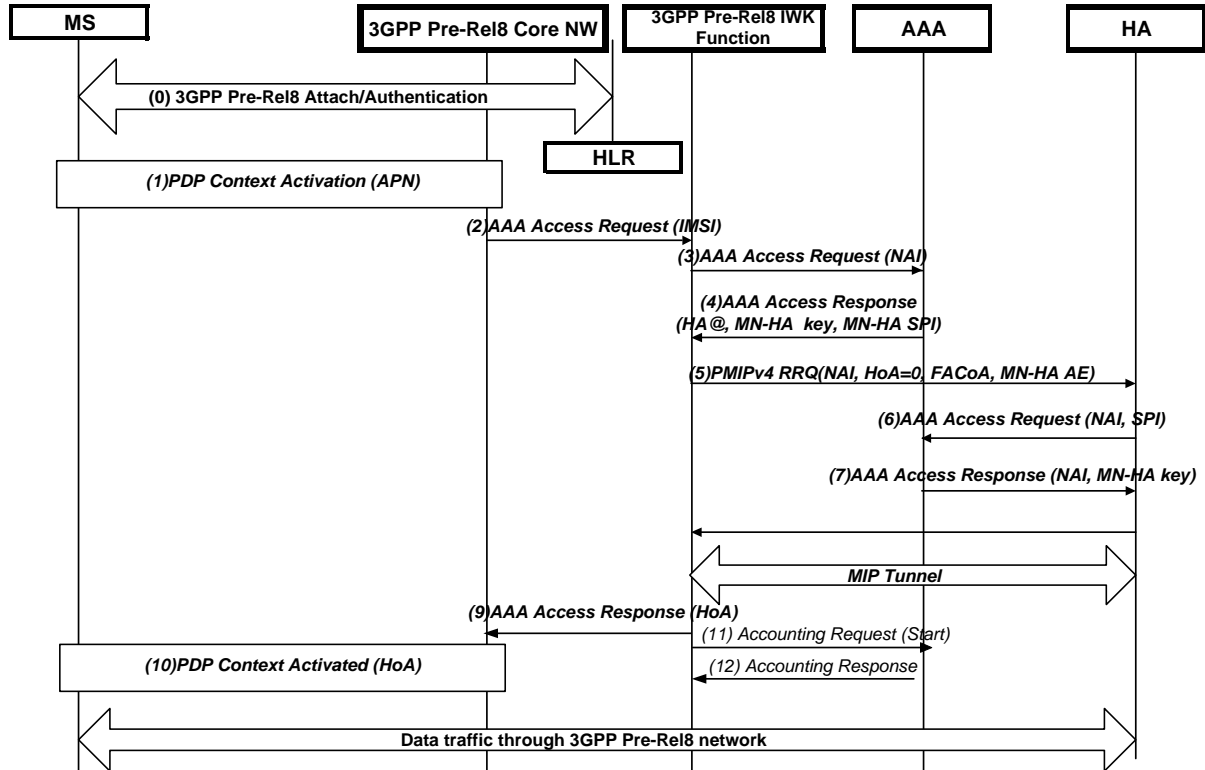


Figure 8-1 - Initial Attach to Pre-Rel8 3GPP system

During initial attachment to Pre-Rel8 3GPP Packet Core, the MS shall indicate the selection of the 3GPP Pre-Rel8 IWK as the target by sending a specific WiMAX® IWK APN to the Pre-Rel8 network when activating the PDP context. The Pre-Rel8 3GPP Packet Core network SHALL associate the WiMAX IWKAPN with the correct 3GPP Pre-Rel8 IWK Function (PRIF) for the WiMAX interworking. The 3GPP Pre-Rel8 network treats the WiMAX network as an ISP identified by the WiMAX IWKAPN. In order to interwork with WiMAX, the 3GPP Pre-Rel8 network uses a non transparent access to the WiMAX CSN, i.e., the MS will be authorized by the WiMAX AAA and obtain the IP address from the home WiMAX network. The TS 29.061 [3] specifies the AAA – based interworking with a Packet Data Network (PDN) that does not belong to the same Public Land Mobile Network (PLMN). As such, the 3GPP Pre-Rel8 network uses the AAA and/or the HA for an IP-address allocation using the 3GPP PRIF as a proxy. During the initial attachment, the AAA server in the WiMAX CSN returns the address of the HA to the 3GPP Pre-Rel8 network.

The following steps happen during initial attachment to Pre-Rel8 3GPP Packet Core:

STEP 0

User initial attachment/access authentication in Pre-Rel8 system happens as per 3GPP TS 23.060 [4].

STEP 1

After the MS is authenticated by the Pre-Rel8 3GPP Packet Core network, it requests establishment of the PDP Context. PDP context establishment request contains the APN, which identifies the PRIF.

STEP 2

1 The 3GPP Pre-Rel8 Packet Core network sends an AAA Access Request message along with the MS's IMSI to the
2 PRIF identified by the APN.

3 **STEP 3**

4 The AAA Proxy function in the PRIF constructs an IMSI based NAI using the same rules as followed when
5 provisioning the IMSI-based NAI for the WiMAX access (See Section 9).

6 Specifically, the NAI is assembled in the following format:

7 IMSI@wimax.mnc<MNC>.mcc<MCC>.wimaxnetwork.org

8 The AAA proxy function in the PRIF sends the AAA Access Request to the home AAA in the WiMAX CSN. It also
9 requests the MN-HA Key (section 4.1), HA-IP and the MN-HA-SPI.

10 It is assumed that that the Pre-Rel8 3GPP Packet Core network issues the AAA *Access Request* with IMSI (step 2)
11 only if the initial Pre-Rel8 3GPP authentication of the MS was successful and MS is allowed to enter the Pre-Rel8
12 3GPP Packet Core network. Optional PAP or CHAP authentication with the AAA server may be performed
13 according to [3]. Note: The entire CHAP/PAP exchange (if executed) is not shown in this document.

14 The Accounting Client in the PRIF requires that a WiMAX-Session-ID and CUI are delivered by the AAA. For that
15 the PRIF includes the CUI attribute in the RADIUS Access-Request packet or the Diameter WDEA message and
16 sets the values to null.

17 **STEP 4**

18 The AAA optionally authenticates the MS and authorizes the MS to use the CSN and sends the HA address, MN-
19 HA key, and MN-HA SPI back to PRIF. The PMIP4 MN-HA key is created by the AAA at random. An associated
20 MN-HA SPI is generated using rules defined in [1]. The MN-HA key is used by the PMIP4 client to calculate the
21 MN-HA authentication extension in the PMIP4 RRQ. In addition, if additional per-node security for the PRIF – HA
22 link is required, the HA-RK key with associated HA-RK SPI is also returned.

23 Per Node security association between the PRIF and the HA is out of scope.

24 If CUI and WiMAX-Session-ID were delivered in the RADIUS Access Accept packet or the Diameter WDEA
25 message, the Accounting Client in the PRIF stores the values received and sends them in each AAA Accounting-
26 Request message. The WiMAX-Session-ID is carried in the accounting records as the Acct-Multi-Session-Id.

27 **STEP 5**

28 PRIF sends a PMIP4 RRQ to the HA with HoA set to all zero ([1]Section 4.8.2.1.5). The PMIP4 RRQ also contains
29 the MS NAI, FA CoA, and MN-HA AE that is calculated with the MN-HA key.

30 **STEP 6-7**

31 If the MN-HA key identified by the MN-HA SPI is not available at the HA, the HA requests the MN-HA key from
32 the AAA.

33 **STEP 8**

34 Once the MN-HA AE is validated, the Home IP address (HoA) is assigned to the MS. The HA creates a binding
35 cache for the MS and sends PMIP4 RRP back to the PRIF, along with the HoA for the MS.

36 **STEP 9**

37 The MN-HA AE in the RRP is validated by the PMIP4 Client in the PRIF. The HoA for the MS is then back to the
38 3GPP Pre-Rel8 Packet Core network in the AAA Access Accept message.

39 **STEP 10**

40 The 3GPP Pre-Rel8 Packet Core network sends the HoA to the MS. At this stage, the MS is ready to communicate
41 using the Pre-Rel8 3GPP Packet Core network and PMIP4 tunnel created between the PRIF and the HA.

42 **STEP 11**

43 The Accounting Client in the PRIF sends Accounting Request (START) message to the AAA.

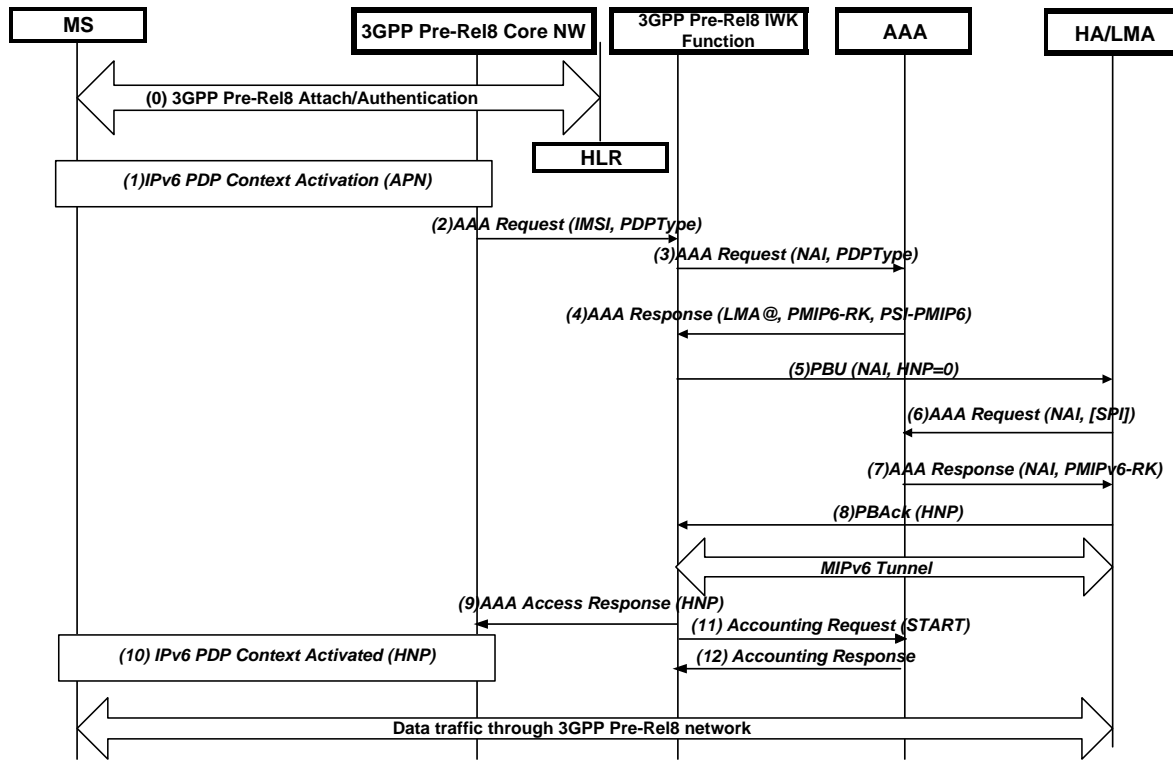
1 Note: During the initial attachment, the 3GPP Pre-Rel 8 network may send Accounting Request (START) to the
2 PRIF. However, the incoming Accounting Request message is not relayed to the AAA.

3 **STEP 12**

4 The AAA server returns Accounting Response message to the PRIF.

5 Note: steps 11 and 12 can be executed after step 9.

6 **7.2 Initial Attach to 3GPP requesting IPv6 PDP context**



7

8 **Figure 8-2 - Initial Attach to Pre-Rel8 3GPP system for IPv6 PDP Context establishment**

9 When the MS attaching to a 3GPP network requests an IPv6 PDP context, and the 3GPP Pre-Rel8 Core network is
10 configured to support it, the 3GPP Pre-Rel8 Core network provides the MS with an IPv6 prefix via the router
11 advertisements. The MS configures an IPv6 address as described in [3]. The 3GPP Pre-Rel8 Core network indicates
12 to the Pre-Rel. 8 IWK function the type of the session being established (IPv6 in this case) by inclusion of the
13 3GPP-PDP Type attribute as defined in [3].

14 The following explains the steps for the initial attachment to the Pre-Rel8 3GPP Packet Core in case of IPv6 PDP
15 context establishment by the MS:

16 **STEP 0**

17 Same as step 0 in Section 8.1 (Figure 8-1).

18 **STEP 1**

19 After the MS is authenticated by the Pre-Rel8 3GPP Packet Core network, it requests establishment of the IPv6 PDP
20 Context. PDP context establishment request contains the APN, which identifies the PRIF.

21 **STEP 2-3**

22 Same as steps 2 and 3 in Section 8.1 (Figure 8-1). Note that as part of the AAA request in the step 2 the PRIF
23 receives the indication of the requested PDP type in the 3GPP-PDP Type attribute [3].

1 **STEP 4**

2 The AAA optionally authenticates the MS and authorizes the MS to use the CSN and sends the LMA address,
3 PMIP6-RK key and SPI-PMIP6 back to 3GPP Pre-Rel8 IWK node. The PMIP6-RK key is created by the AAA at
4 random. An associated PMIP6 SPI is generated using rules defined in [9]. The authenticator in the PRIF derives the
5 MAG-LMA-PMIP6 key using the PMIP6-RK as described in [9]. The MAG-LMA-PMIP6 key is used by the MAG
6 to calculate the MN-HA Authentication Option in the PMIP6 PBU [9]. Usage of MAG-LMA-PMIP6 key and SPI-
7 PMIP6 is not required if lower-layers security model (IPsec tunnel) is used between MAG and LMA.

8 If CUI attribute was requested in the RADIUS Access Request packet or the Diameter WEDR message and
9 delivered in the Access Accept/WEDA, the Accounting Client in the PRIF stores the value received and send it and
10 the WiMAX-Session-Id in each AAA Accounting-Request message.

11 **STEP 5**

12 Triggered by the indication of the IPv6 PDP type received in step 2, the PRIF sends a Proxy Binding Update (PBU)
13 to the LMA with Home Network Prefix (HNP) set to all zero and HI set to "Handoff state unknown" ([9]). The PBU
14 message also contains the MS NAI and depending on the selected security mode, may be protected by the MN-HA
15 authentication option ([9]).

16 **STEP 6-7**

17 After receiving the PBU message, LMA initiates Authorization of MAG that has sent the Proxy Binding Update by
18 sending the Access-Request message to the AAA. When in-band security is enabled, the LMA indicates the SPI
19 received in the PBU message to the AAA to retrieve the associated PMIP6-RK from the AAA. LMA derives the
20 MAG-LMA-PMIP6 key from the PMIP6-RK as per [9].

21 **STEP 8**

22 The LMA assigns the Home Network Prefix to the MS, creates a binding cache for the MS and sends the Proxy
23 Binding Acknowledgement (PBA) back to the PRIF, along with the HNP for the MS.

24 **STEP 9**

25 In case of in-band security mode the MN-HA AO in the PBA message is validated by the MAG in the PRIF. The
26 Home Network Prefix for the MS is sent back to the 3GPP Pre-Rel8 GGSN via the AAA Access Accept message.

27 **STEP 10**

28 The address configuration process takes place as described in [3]. After the address is successfully configured, the
29 MS is ready to communicate using the Pre-Rel8 3GPP Packet Core network and PMIP6 tunnel created between the
30 PRIF and the LMA.

31 **STEP 11**

32 The Accounting Client in the PRIF sends Accounting Request (START) message to the AAA.

33 Note: During the initial attachment, the 3GPP Pre-Rel 8 network may send Accounting Request (START) to the
34 PRIF. However, the incoming Accounting Request message to the PRIF is not relayed to the AAA.

35 **STEP 12**

36 The AAA server returns Accounting Response message to the PRIF.

37 Note: steps 11 and 12 can be executed after step 9.

38 **7.3 MS requirements**

39 The MS SHALL follow the requirements and procedures specified in 3GPP TS 29.061 [3] for connecting to the
40 Packet Domain Bearer services when accessing the 3GPP Pre-Rel8 packet network. The MS shall indicate selection
41 of the PRIF as the target PDN by sending the pre-configured WiMAX® IWK APN to assist the Pre-Rel8 3GPP
42 Packet Core network in associating the APN with the correct PRIF for the WiMAX interworking.

43 The MS SHALL indicate the preference for the non-transparent access to the PLMN and request the dynamic IP
44 address allocation. The MS has the ability to request either an IPv4 or IPv6 PDP context.

1 After the MS receives the assigned IP address from the 3GPP Pre-Rel8 Packet Core network, the MS SHALL
2 configure the interface and protocol with this address to communicate using the Pre-Rel8 3GPP Packet Core
3 network and the tunnel created between the PRIF and the HA/LMA.

4 **7.4 PRIF Requirements**

5 Upon receiving the AAA request from the 3GPP Pre-Rel8 Core network to setup the connection from MS to the
6 WiMAX® CSN, the AAA Proxy function in the PRIF SHALL extract the MS IMSI received in the 3GPP-IMSI
7 attribute of the RADIUS Access Request message.

8 The PRIF SHALL construct an IMSI based NAI from the extracted IMSI in the following format:

9 IMSI@wimax.mnc<MNC>.mcc<MCC>.wimaxnetwork.org

10 The NAS function at the PRIF SHALL construct the AAA request to the WiMAX AAA with a WiMAX-NAS-Type
11 VSA value of 3 (refers to section 16.1) to request the HA-IP, MN-HA key, and associated MN-HA SPI. The PRIF
12 SHALL populate the User-Name attribute of the AAA request with the IMSI-based NAI.

13 Upon receiving the AAA response from the WiMAX AAA containing the HA IP Address and if the type of the
14 session as indicated by the 3GPP-PDP Type attribute [9] is IPv4,, the PRIF SHALL generate the PMIP4 RRQ to the
15 HA.

- 16 • The PRIF SHALL set the NAI in the RRQ to the IMSI-based NAI assembled from the IMSI received
17 from the 3GPP Pre-Rel8 network, as shown above in this section.
- 18 • The PRIF SHALL set the HA-IP in the RRQ to the HA address received from the WiMAX AAA.
- 19 • The PRIF SHALL generate the MN-HA AE using the MN-HA key received from the WiMAX AAA.
20 The 3GPP Pre-Rel8 IWK SHALL include the SPI set to the value of MN-HA-SPI received from the
21 WiMAX AAA.

22 When the PRIF receives the PMIP4 RRP from the HA along with the HoA for the MS, the PRIF SHALL construct
23 the AAA Access Response message to the 3GPP Pre-Rel8 Core network. The AAA Proxy in PRIF SHALL populate
24 the Framed-IP-Address attribute with the assigned MS HoA.

25 Upon receiving the AAA response from the WiMAX AAA containing the LMA address and if the type of the
26 session as indicated by the 3GPP-PDP Type attribute [9] is IPv6, the 3GPP Pre-Rel8 IWK SHALL generate the
27 PMIP6 PBU to the LMA:

- 28 • The PRIF SHALL set the NAI in the PBU to the IMSI-based NAI assembled from the IMSI received
29 from the 3GPP Pre-Rel8 network, as shown above in this section.
- 30 • The PRIF SHALL send the PBU message to the LMA address received from the WiMAX AAA.
- 31 • Depending on the operator policies and network configuration, the PRIF MAY generate the MN-HA
32 AO using the MAG-LMA key derived from the PMIP6-RK received from the WiMAX AAA. The
33 PRIF SHALL include the SPI set to the value of SPI-PMIP6 received from the WiMAX AAA.
- 34 • The PRIF SHALL trigger Proxy MIP6 function when it receives a request to assign an IPv6 prefix.
35 This request is generated when the 3GPP-PDP Type attribute for IPv6 is received from the 3GPP Pre-
36 Rel8 Core network.
- 37 • The rest of the fields in the PMIP6 PBU SHALL be set as per [9]

38 When the PRIF receives the PMIP6 PBA from the LMA along with the HNP for the MS, the PRIF SHALL
39 construct the AAA Access Response message to the 3GPP Pre-rel8 Core network. The AAA proxy in PRIF SHALL
40 populate the Framed-IPv6 Prefix attribute with the assigned MS's HNP.

41 During 3GPP Network attachment, the PRIF SHALL include the WiMAX capability attribute in the RADIUS
42 Access-Request or the Diameter WEDR message indicating its capabilities to the HAAA. The PRIF SHALL also
43 indicate support for IP session based accounting. If the PRIF receives an Access-Accept/WEDA in which the
44 HAAA did not select IP session accounting mode, the PRIF SHALL not generate nor provide any Accounting
45 information to the AAA.

1 **7.5 AAA Requirements**

2 When the HAAA receives the AAA Access Request message along with the IMSI based NAI in User-Name
3 attribute and the WiMAX-ASN-Type VSA value of 3 (refers to section 16.1) indicating the request of the MN-HA
4 key or PMIP6 key and associated SPI from the 3GPP Pre-Rel8 Packet Core network, the HAAA SHALL perform
5 the following:

- 6 • The HAAA SHALL allocate the HA IP address and include it in the hHA-IP-MIP4 attribute of the
7 AAA Access Accept.
- 8 • In the case of AAA assigning the IP address, the HAAA SHALL allocate the MS IP address and
9 include it in the Framed-IP-Address attribute of the AAA Access Accept.
- 10 • The HAAA SHALL generate the random MN-HA key and include it in the MN-hHA-MIP4-KEY
11 attribute of the AAA Access Accept.
- 12 • The HAAA SHALL select the MN-HA-SPI associated with the generated MN-HA key. While
13 selecting the MN-HA-SPI, the HAAA SHALL avoid collisions with any other active MN-HA-SPI
14 associated with the same MS. The HAAA SHALL populate the MN-hHA-MIP4-SPI attribute of the
15 AAA Access Accept with the selected value.
- 16 • The HAAA SHALL sent the AAA response to the PRIF.

17 The AAA MAY optionally support PAP/CHAP authentication as specified in [3].

18 Based on IPv6 PDP Type Value in the AAA Access Request, the HAAA SHALL select the PMIP6 mode for the MS,
19 in which case the HAAA returns the LMA address as part of the final Access Accept message. If in-band PMIP6
20 security is in place, the HAAA SHALL generate the random PMIP6-RK and include it in the PMIP6-RK attribute of
21 the AAA Access Accept. The HAAA SHALL also generate the SPI associated with the PMIP6-RK as per [9].

22 If the PRIF includes the WiMAX capability attribute in the RADIUS Access-Request packet or in the Diameter
23 WDER message and a request for CUI, the AAA SHALL provide a WiMAX Session ID, compute a value for the
24 CUI and returns these attributes in the Access Accept/WDER message.

25 **7.6 HA/LMA Requirements**

26 No additional requirements

27

28

8. Initial WiMAX® Network Entry

8.1 Initial WiMAX® Network Entry for IPv4 Services

The WiMAX® initial network entry for the dual radio device shall follow the procedures specified in section 4.8.2.1.7.1 of [1].

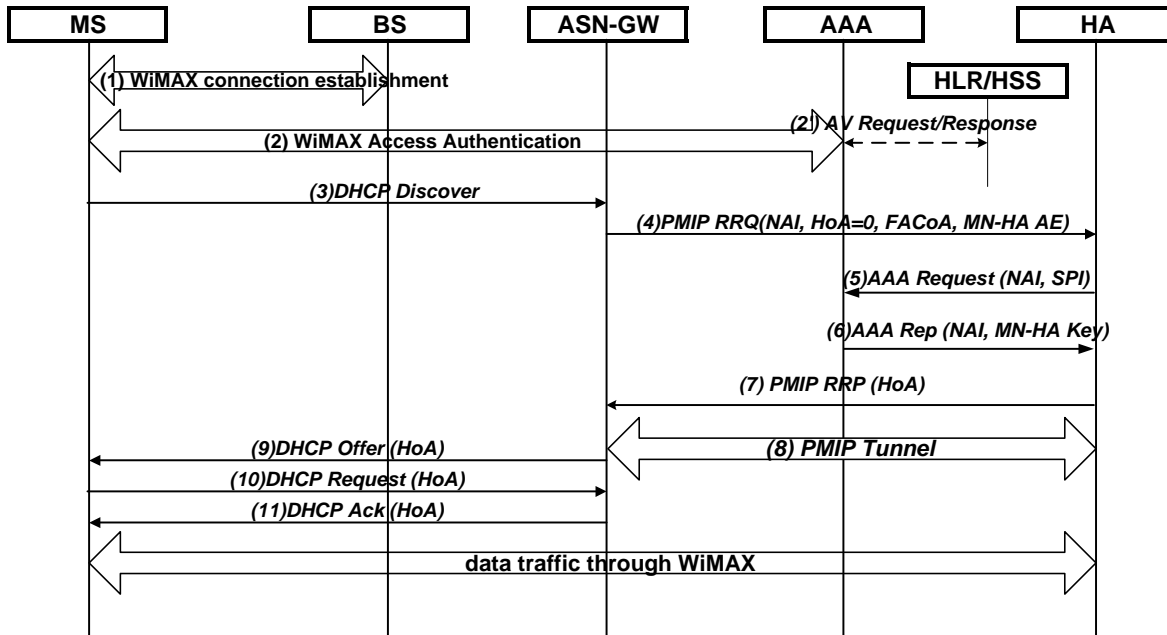


Figure 9-1 - WiMAX® Initial Network entry for IPv4 Services

In all cases, to allow for the session continuity while interworking between the 3GPP Pre-Rel8 network and WiMAX systems, the 3GPP Pre-Rel8 network Identity of the mobile, IMSI, and the WiMAX identity, the NAI, must be aligned.

For the WiMAX entry, a dual radio MS identifies itself with the NAI during access authentication.

If a home operator chooses to protect subscriber identity when it is reported to the accessed network, the dual radio MS is configured to follow requirements of [1] Section 4.4.1.3.2 without any restrictions, i.e. a pseudo-NAI can be used as an outer NAI. In such case, the IMSI-based NAI has to be provisioned in the H-AAA subscription record. This IMSI-based NAI shall be returned by the H-AAA to the ASN-GW containing the PMIP Client during the EAP authentication stage. This IMSI-based NAI shall be used by the PMIP4 Client when assembling the PMIP4 RRQ.

If a home operator chooses not to protect subscriber identity when it is reported to the accessed network, the dual mode mobile shall be preconfigured with the NAI based on IMSI, e.g. following the procedures specified in 3GPP TS 23.003. This NAI (IMSI@realm) shall be used as an outer NAI during the EAP authentication stage. The format of the realm shall be consistent with the rules specified below in this section of the document for construction of the “realm” by the PRIF from IMSI reported by the MS during the 3GPP Pre-Rel8 access.

Specifically, the NAI provisioned in the dual-mode mobile and used for the WiMAX access shall be in the following format:

IMSI@wimax.mnc<MNC>.mcc<MCC>.wimaxnetwork.org,

1 The ASN-GW receives the HA address and PMIP4 security context from the HAAA at the time of successful
2 Device/User Access Authentication. The ASN-GW may also receive the HoA address if it is assigned by the H-
3 AAA. Subsequently, the following steps take place:

4 **STEP 1**

5 WiMAX Connection established.

6 **STEP 2**

7 WiMAX access authentication happens as described in NWG stage 3 specification [1]. See section 5.1 for more
8 detail.

9 **STEP 3**

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

11 **STEP 4**

12 Upon receiving the DHCPDISCOVER message, the DHCP Proxy triggers the PMIP4 client to initiate the Mobile
13 IPv4 Registration procedure. The NAI (IMSI@realm) used in the registration message is the same one used during
14 EAP authentication described above. If the HoA (H-AAA assigns HoA) was received during access authentication,
15 then the PMIP4 client uses the HoA information and constructs a PMIP4 RRQ message. If the HoA was not
16 received, then the HoA field is set to 0.0.0.0. In either case, the CoA field is set to the FA-CoA address that is
17 configured locally. The PMIP4 client sends the RRQ to the FA address including the MN-HA authentication
18 extension. The FA forwards the registration request to the HA. The source address for the RRQ is the FA-CoA and
19 the destination address is the HA address. The HoA in the RRQ to the home agent will be set to all zero or the IP
20 address that the MS is currently using (refer to NWG spec Section 4.8.2.1.4[1]). The PMIP4 RRQ message also
21 contains the MS NAI, FA CoA and MN-HA AE that is calculated with the MN-HA key.

22 When the HA receives the PMIP4 RRQ, it validates the MN-HA AE.

23 **STEP 5**

24 If the MN-HA key identified by the SPI is not available, the HA requests the MN-HA key from the AAA.

25 **STEP 6**

26 The MN-HA key associated with the MN-HA SPI is returned to the HA for MN-HA AE validation.

27 Once the MN-HA AE is validated, the HA assigns an IP address to MS. If the assigned HoA value in the MIP RRQ
28 is 0.0.0.0, the HA assigns the HoA. Otherwise, the HoA in the PMIP4 RRQ is used. If this is the initial entry for the
29 MS, the HA creates a binding cache for the MS.

30 **STEP 7**

31 The HA responds with the PMIP4 Registration Response (RRP) message. The source address for the PMIP4 RRP
32 message is HA and the destination address is FA-CoA. The FA forwards the message to the PMIP4 client. The
33 PMIP4 client passes the HoA information to the DHCP proxy.

34 **STEP 8**

35 PMIP4 tunnel is established between ASN-GW and HA.

36 **STEP 9**

37 The DHCP proxy sends the DHCP OFFER message with the HoA to the MS.

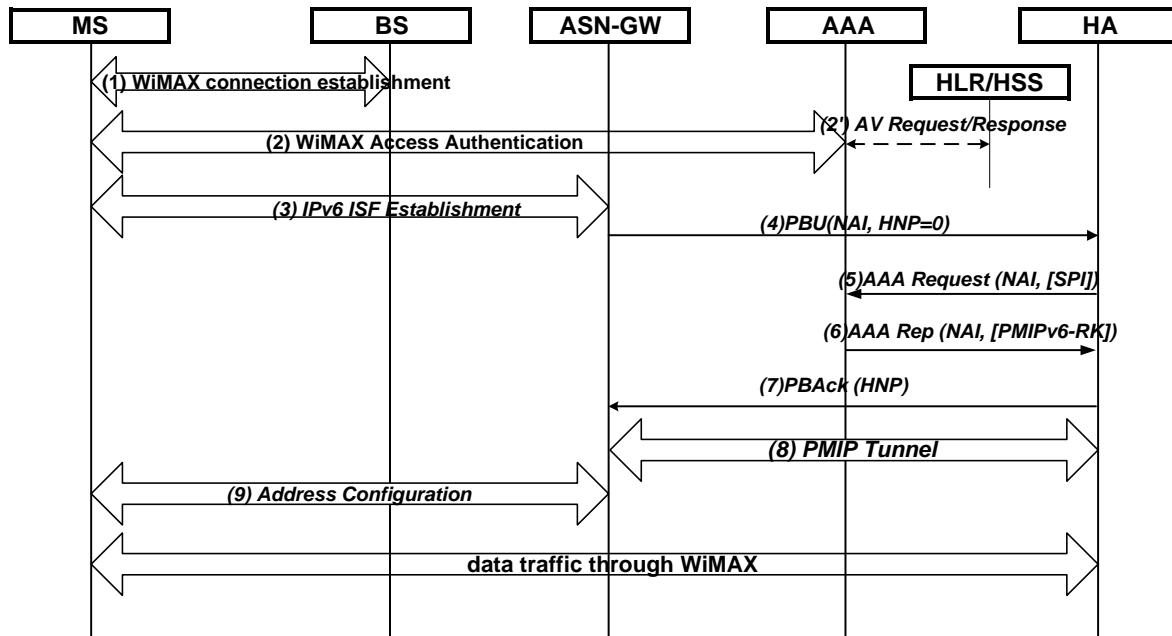
1 **STEP 10**

2 MS responds to the first DHCP OFFER message received with a DHCP REQUEST to the DHCP Proxy with the
3 HoA information received in the DHCP OFFER.

4 **STEP 11**

5 The DHCP Proxy acknowledges the use of this IP address and other configuration parameters as defined in RFC
6 2131 by sending the DHCP ACK message.

7 **8.2 Initial WiMAX® Network Entry for IPv6 services**



8
9 **Figure 9-2 - WiMAX® Initial Network entry for IPv6 services**

10 **STEP 1**

11 WiMAX® connection established.

12 **STEP 2**

13 Same as step 2 in Section 9.1 (Figure 9-1).

14 **STEP 3**

15 IPv6 ISF is established between MS and the ASN-GW.

16 **STEP 4**

17 Upon establishment of the IPv6 ISF, the MAG in the ASN-GW is triggered to initiate the PMIP6 registration
18 procedure. The NAI (IMSI@realm) used in the Proxy Binding Update message is the same one used during EAP
19 authentication described above. The rest of the fields in the PBU message are initialized as per [9].

20 **STEP 5-6**

21 Those steps are the same as the steps 6 and 7 in the Section 8.2 (Figure 8-2).

1 **STEP 7**

2 The LMA responds with the PMIP6 PBA message as per [9].

3 **STEP 8**

4 PMIP6 tunnel is established between ASN-GW (MAG) and LMA.

5 **STEP 9**

6 The MS configures the IPv6 address as per [9].

7 **8.3 AAA Requirements**

8 For general requirement, the WiMAX AAA should be compliant with section 13.1 - AAA Requirements.

9 In the case of shared credential with 3GPP Pre-Rel8 network, when the AAA performs the access authentication for
10 the MS:

- 11 • The AAA SHALL construct the authentication vector request message based on 3GPP WLAN
12 interworking spec TS 23.234 [5] and send the request to HLR/HSS over Gr'/Wx interface.
- 13 • The AAA SHALL use the Authentication Vector parameters received from HLR/HSS to conduct the EAP
14 authentication of the MS for WiMAX access.

15 When the AAA receives the AAA Access Request from the HA/LMA with MN NAI and SPI:

- 16 • In case of IPv4 service, the AAA SHALL return the MN-HA key associated with the SPI along with MN
17 NAI back to HA.
- 18 • In case of IPv6 service, the AAA SHALL return the PMIP6-Root Key (PMIP6-RK) and the associated SPI
19 along with the MN NAI back to the LMA as per [9].

20 After successful authentication, the H-AAA SHALL return the IMSI-based NAI to the ASN-GW which contains the
21 PMIP Client during the EAP authentication stage in the PMIP-Authenticated-NAI TLV.

22 **8.4 MS Requirements**

23 If a home operator chooses to protect subscriber identity that is reported to the accessed network, the dual radio MS
24 SHALL follow NAI requirements as per section 4.4.1.3.2 – NAS Requirements of WiMAX Forum® Network
25 Architecture Stage 3 specification [1].

26 If a home operator chooses not to protect subscriber identity that is reported to the accessed network, the dual radio
27 MS SHALL be preconfigured with the IMSI based on NAI, e.g., following the procedures specified in 3GPP TS
28 23.003 [6]. This NAI (IMSI@realm) SHALL be used as an outer NAI during the EAP authentication stage. The
29 format of the realm SHALL be consistent with the rules specified in the Section 9 of NWG stage 3 specification
30 [1] for construction of the “realm” by the 3GPP Pre-Rel8-IWK from IMSI reported by the MS during the 3GPP Pre-
31 Rel8 access.

32 Specifically, the NAI provisioned in the dual-mode mobile and used for the WiMAX access SHALL be in the
33 following format:

34 IMSI@wimax.mnc<MNC>.mcc<MCC>.wimaxnetwork.org,

35 **8.5 ASN GW Requirements**

36 Upon receiving the DHCPDISCOVER message, the DHCP Proxy triggers the PMIP4 client to initiate the Mobile
37 IPv4 Registration procedure.

- 38 • The ASN GW SHALL use the IMSI based NAI (IMSI@realm) that it received from the HAAA during
39 access authentication in the PMIP-Authenticated-NAI TLV for the PMIP4 RRQ construction.

- 1 • When the ASN GW receives the PMIP4 RRP from the HA along with the HoA that is assigned to the MS,
2 the ASN GW SHALL send the HoA to MS in the DHCP Offer message.

3 Upon establishment of an IPv6 ISF and if the AAA Access Accept message provides the LMA address, the MAG
4 SHALL initiate the PMIP6 registration procedure as per [9]. In addition, the ASN GW SHALL use the IMSI based
5 NAI (IMSI@realm) that it received from the HAAA during access authentication in the PMIP-Authenticated-NAI
6 TLV for the PMIP6 PBU construction.

7

1 9. Authentication and Security

2 9.1 Access Authentication

3 The access authentication in WiMAX system shall follow the procedure defined by the WiMAX Forum® Network
4 Architecture specification [1].

5 When the dual radio MS maintains two independent sets of credentials (as per section 5.1.1), authentication of the
6 WiMAX® access is performed by the WiMAX H-AAA as described in [1] using the WiMAX security credentials
7 and authentication for the 3GPP Pre-Rel8 Packet Core is performed by the 3GPP HLR/HSS, as described in 3GPP
8 standards, by using the 3GPP security credentials.

9 When the dual mode MS maintains a single set of credentials (as per section 5.1.2), these credentials shall be
10 provisioned at the 3GPP Pre-Rel8 HLR/HSS. To conduct the WiMAX access authentication, the WiMAX H-AAA
11 SHALL request the authentication vector from the 3GPP HLR/HSS via the Gr'/Wx interface defined by TS 23.234
12 [5]. The WiMAX H-AAA SHALL be able to obtain the IMSI associated with the subscription of the dual radio MS,
13 and using this IMSI, SHALL discover the 3GPP HLR/HSS containing the credentials.

14 9.2 Mobility Security

15 After a successful access authentication in the WiMAX® system, keys used for mobility security SHALL be sent to
16 the authenticator per [1]. In addition, during the EAP authentication stage, the H-AAA SHALL return the IMSI-
17 based NAI to the ASN-GW which contains the Anchor Authenticator and PMIP4 Client and the MAG for the IPv6
18 case. This IMSI-based NAI SHALL be used by the PMIP4 Client and the MAG when assembling the PMIP4 RRQ
19 messages or the PMIP6 PBU messages.

20 The access authentication of the user in the 3GPP Pre-Rel8 system SHALL follow the procedure defined by the
21 3GPP standards and briefly described in Section 8 of this specification.

22 9.2.1 PMIP4 considerations

23 After successful access authentication in the 3GPP Pre-Rel8 system (as described in Section 8), the H-AAA SHALL
24 generate the MN-HA key and associated MN-HA SPI and send them along with HA IP address to the PRIF in a
25 AAA response message. The MN-HA key is created by the AAA at random and the associated MN-HA SPI is
26 generated using rules defined in [1]. The MN-HA key SHALL be used by the PMIP4 client located in the PRIF to
27 calculate the MN-HA Authentication Extension in the PMIP4 RRQ.

28 If additional per-node security for the IWK – HA link is required, the HA-RK key with its associated HA-RK SPI is
29 also generated by the H-AAA and returned in the AAA response.

30 The PMIP4 client in the PRIF SHALL send a PMIP4 RRQ message to the HA with MN-HA AE calculated with the
31 MN-HA key. If the MN-HA key identified by the MN-HA SPI is not available at the HA, the HA SHALL request
32 the required MN-HA key from the AAA. If per node security for the PRIF – HA is required, the HA SHALL request
33 HA-RK from the AAA.

34 Once the MN-HA AE is validated, the HA SHALL send PMIP4 RRP back to the PRIF, along with the MN-HA AE
35 indicating successful binding of the session.

36 9.2.2 PMIP6 considerations

37 After successful access authentication in the 3GPP Pre-Rel8 system and the AAA authorization described in Section
38 8, the H-AAA SHALL generate the PMIPv6 Root Key (PMIP6-RK) and associated SPI (SPI-PMIP6), and send
39 them along with LMA IP address to the authenticator function in the PRIF in an AAA response message. The
40 PMIP6-RK key is created by the AAA at random and the associated SPI-PMIP6 SPI is generated using rules defined
41 in [9]. The authenticator at the PRIF SHALL use the PMIP6-RK to derive the MAG-LMA-PMIP6 key as defined in
42 [9]. The MAG-LMA-PMIP6 key SHALL be used by the MAG located in the PRIF to calculate the MN-HA
43 Authentication Option in the PMIP6 Proxy Binding Update.

1 The MAG in the PRIF SHALL send a PMIP6 Proxy Binding Update message to the LMA with MN-HA AO
2 calculated with the MAG-LMA-PMIP6 key. If the MAG-LMA-PMIP6 key identified by the MN-HA SPI is not
3 available at the LMA, the LMA SHALL request the required PMIP6-RK key from the AAA and derive the MAG-
4 LMA-PMIP6 key as per [9].

5 Once the MN-HA AO is validated, the LMA SHALL send PMIP6 Proxy Binding Ack back with the Home Network
6 Prefix to the PRIF, along with the MN-HA AO indicating successful binding of the session. Usage of MAG-LMA-
7 PMIP6 key and SPI-PMIP6 is not required if lower-layers security model is used between MAG and LMA. In such
8 a case, an IPsec tunnel is established between MAG and LMA and MN-HA AO is not used.

9 **9.3 Inter-node Security**

10 Transport link security between 3GPP Pre-Rel8 Packet Core network and the PRIF should follow the requirements
11 of the 3GPP TS 33.210 [10] for Network Domain Security.

12 Transport link security between WiMAX® CSN and the IWK node should be based on the policy of the operator –
13 owner of the PRIF.

14 Security of the Gr'/Wx interface between the WiMAX AAA and the 3GPP HLR/HSS should be based on the inter-
15 operators agreements and respective operating policies.

16

17

10. Handover

10.1 WiMAX® to 3GPP Pre-Rel8 Packet Core Handover for IPv4 service

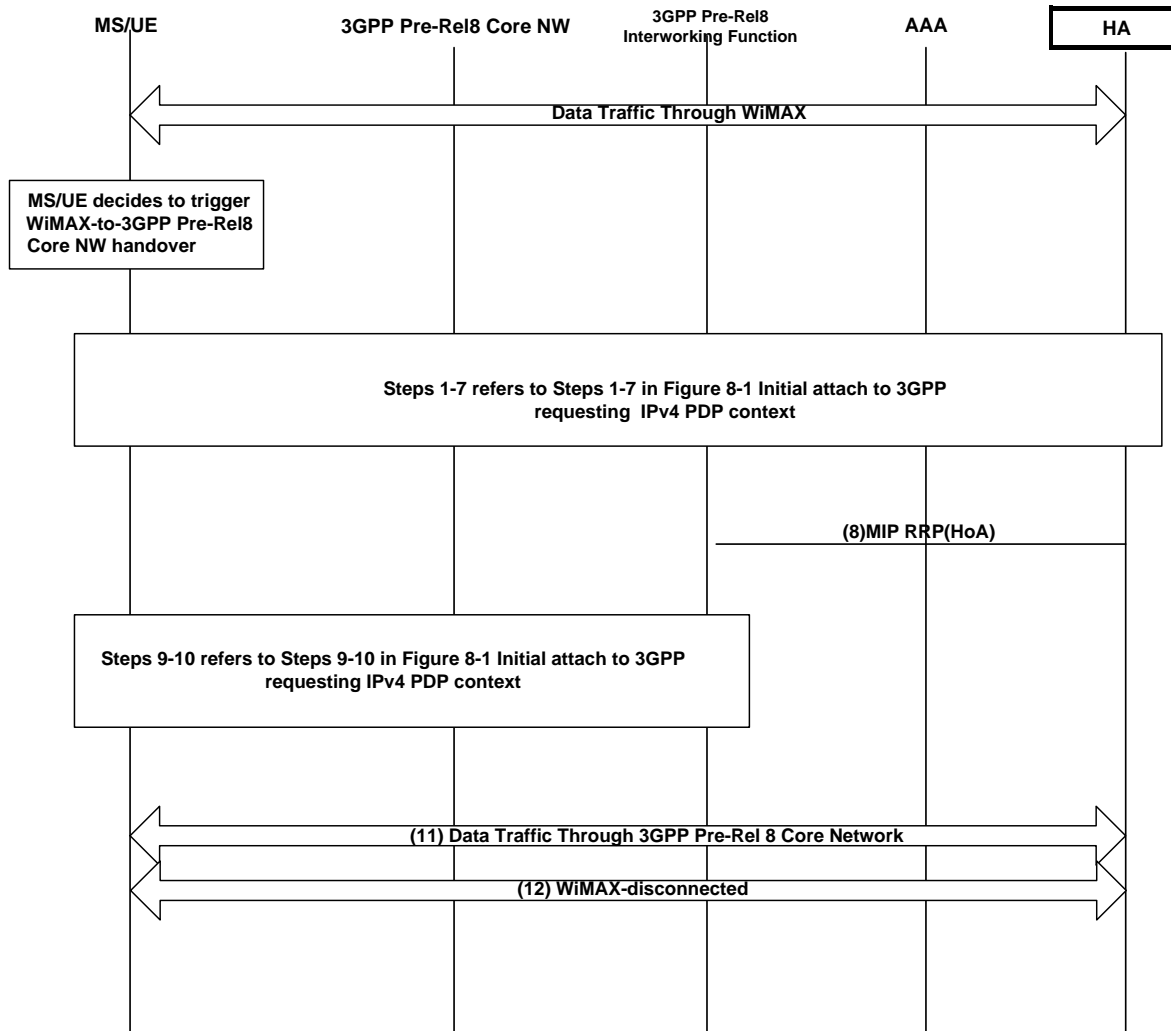


Figure 11-1 - WiMAX® to 3GPP Pre-Rel8 Packet Core Handover for IPv4 service

At the beginning of this handover scenario, the MS is connected to the WiMAX network. Once the MS/UE decides to handover from the WiMAX network to the 3GPP network, the UE performs an attachment to the 3GPP Pre-Rel8 Packet Core network as described in Section 8.1 of this document. Consequently the following steps are performed:

STEP 1-7

Refer to steps 1-7 of Initial attach to 3GPP requesting IPv4 PDP context in Section 8.1.

STEP 8

Based on the NAI, the HA assigns the same IP address that is used by the MS in the WiMAX network. The HA then updates the binding cache for the MS and sends PMIP4 RRP back to the PRIF, along with the HoA for the MS. If

1 the HA doesn't support simultaneous binding, it invokes release procedure as described in section 4.5.2.1.2.5 (HA
2 Initiated MS Network Exit) in [1].

3 **STEP 9-10**

4 Refers to steps 9-10 of Initial attach to 3GPP requesting IPv4 PDP context in Section 8.1.

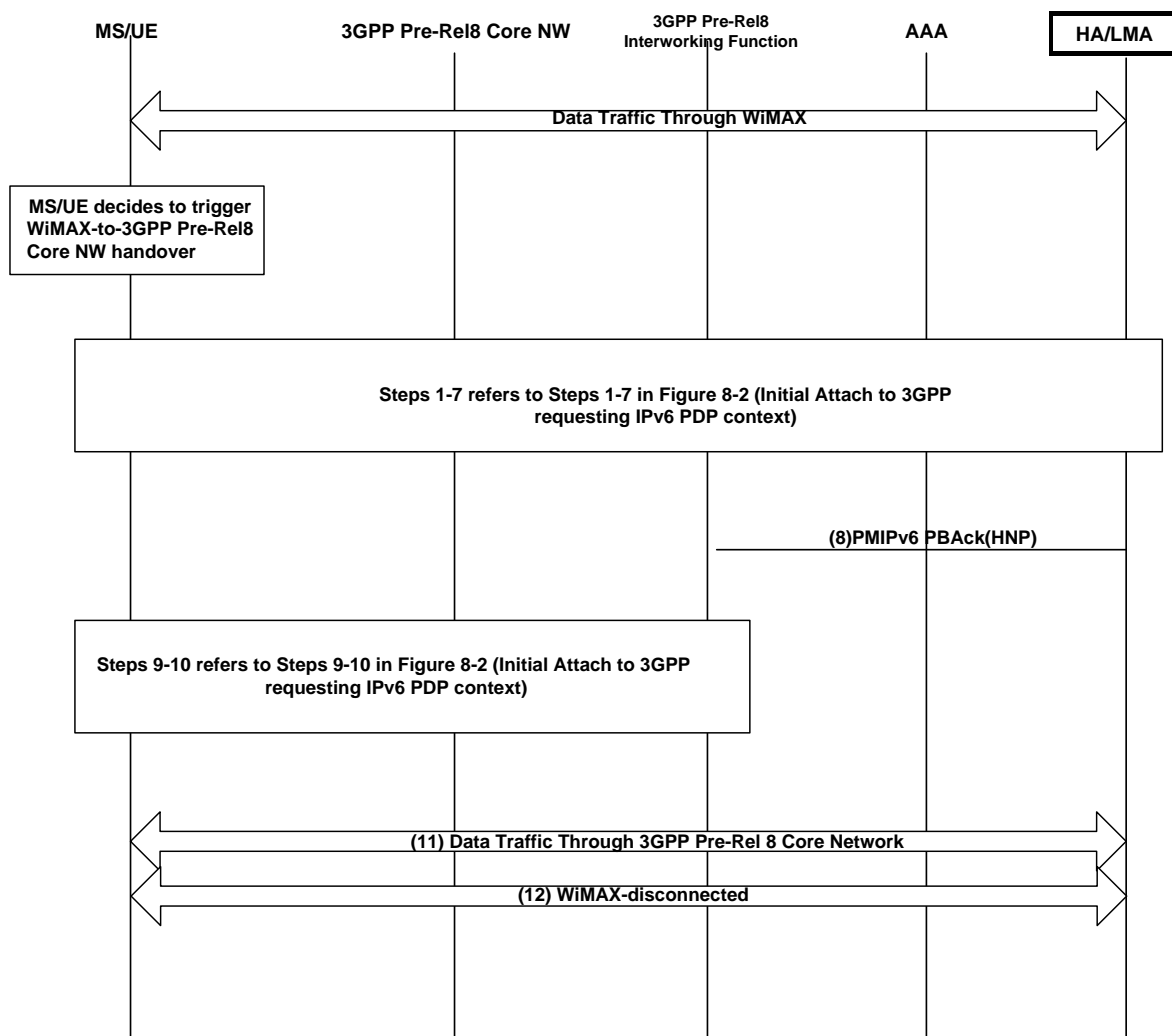
5 **STEP 11**

6 The data traffic for the MS/UE can be switched to the 3GPP Pre-Rel8 Packet Core network. If simultaneous binding
7 is supported and both radios (WiMAX and 3GPP) are "ON", the MS/UE can receive packets from both interfaces
8 during handover.

9 **STEP 12**

10 The MS disconnects from the WiMAX network per the procedure described in section 4.5.2.1.1 in [1].

11 **10.2 WiMAX® to 3GPP Pre-Rel8 Packet Core Handover for IPv6 service**



12 **Figure 11-2 - WiMAX® to 3GPP Pre-Rel8 Packet Core Hand Over for IPv6 service**

13 **STEP 1-7**

14 Refer to steps 1-7 of Section 8.2 (Figure 8-2) for Initial Attach to 3GPP requesting IPv6 PDP context.

1 **STEP 8**

2 Based on the NAI, the LMA assigns the same HNP that is used by the MS in the WiMAX network. The LMA then
3 updates the binding cache for the MS and sends PMIP6 PBA message back to the PRIF, along with the HNP for the
4 MS. The LMA also sends the Binding Revocation message containing the MS NAI to the previous MAG in the
5 WiMAX ASN to terminate the MS session on the WiMAX side. The procedure for revoking the PMIP6 binding by
6 the LMA is described in the [9].

7 **STEP 9-10**

8 Refer to steps 9-10 of Section 8.2 (Figure 8-2) for Initial Attach to 3GPP requesting IPv6 PDP context

9 **STEP 11**

10 The data traffic for the MS/UE is switched to the 3GPP Pre-Rel8 Packet Core network.

11 **STEP 12**

12 The MS disconnects from the WiMAX network per the procedure described in section 4.5.2.1.1 (MS Triggered
13 Network Exit) in [1].

14 **10.3 Requirements for WiMAX® to 3GPP Pre-Rel8 Packet Core Handover**

15 **10.3.1 MS Requirements**

16 Once the MS makes a decision to handover from the WiMAX to the 3GPP Pre-Rel8 core network, the MS SHALL
17 perform the 3GPP Pre-Rel8 initial attach procedures as specified in section 8 of this document.

18 The MS SHALL verify that the IP address assignment received as the result of accessing the 3GPP Pre-Rel8 core
19 network is the same as the IP address that the MS was assigned while communicating through the WiMAX network.
20 If the IP address assigned by the 3GPP Pre-Rel8 network is different from the IP address that the MS was using on
21 the WiMAX network, the MS SHALL terminate the WiMAX session and establish the new 3GPP Pre-Rel8 session.

22 The MS SHALL exit the WiMAX network after the handover procedures are complete.

23 **10.3.2 HA/LMA Requirements**

24 During the handover from WiMAX to 3GPP Pre-Rel8 network, the HA SHALL meet the following requirements:

25 Upon receiving the PMIP4 RRQ from the PRIF, the HA SHALL determine if an active binding already exists for
26 the MS NAI included in the RRQ. If an active binding does not exist, the HA SHALL follow the procedures
27 specified in section 8 of these specifications. Otherwise, if an active binding already exists, the HA SHALL validate
28 the MN-HA AE included in the RRQ as defined in section 4.8.2 of [1]. Once the MN-HA AE is validated, the HA
29 SHALL respond to the PRIF with the PMIP4 RRP message, setting its parameters as specified in section 4.8.2 of [1]
30 with the following exception:

- 31
 - To preserve the IP session continuity, the HA SHALL set the HoA attribute in the RRP to the same IP
32 address that is used for the MS currently active binding.

33 If the HA does not support simultaneous binding, it SHALL reject a simultaneous binding request. If it supports
34 simultaneous binding, the HA SHALL accept a new simultaneous binding request for a HoA/NAI having an already
35 active binding. In addition the HA SHALL provide packet duplication feature if multiple bindings to the same
36 HoA/NAI are active at the same time. If a new valid binding request is received for the same HoA/NAI and
37 simultaneous binding feature is not requested, the HA SHALL replace any existing binding for the HoA/NAI with
38 the new one.

39 Upon receiving the PMIP6 PBU from the PRIF, the LMA SHALL determine if an active binding already exists for
40 the MS NAI included in the PBU. If an active binding does not exist, the LMA SHALL follow the procedures
41 specified in section 8 of these specifications. Otherwise, if an active binding already exists, the LMA SHALL
42 respond to the PRIF with the PMIP6 PBA message, setting its parameters as specified in section 8.2 of this
43 document with the following exception:

- 1 • To preserve the IP session continuity, the LMA SHALL set the HNP attribute in the PBA to the same
2 IPv6 prefix that is used for the MS currently active binding.

3 Upon accepting the PMIP6 PBU from the PRIF, the LMA SHOULD terminate the PMIP6 session on the WiMAX
4 ASN side by sending the Binding Revocation Indication as described in [9].

5 **10.3.3 AAA Requirements**

6 When the HAAA receives the AAA Access Request message, along with the IMSI based NAI in User-Name
7 attribute and the WiMAX-ASN-Type VSA with a value of 3 (refers to section 16.1) indicating the request of the
8 MN-HA key and associated SPI from the 3GPP Pre-Rel8 Packet Core network, the HAAA shall perform the
9 following:

- 10 • The HAAA SHALL determine if an active session exists for this NAI. If the session does not exist, the
11 HAAA SHALL follow requirements defined in section 8.5 of this document. Otherwise, if the session
12 already exists, the HAAA SHALL set the hHA-IP-MIP4 attribute of the AAA Access Accept to the
13 address of the HA that handles the current session, i.e. HA-IP value.
- 14 • The HAAA SHALL set the MN-hHA-MIP4-KEY attribute of the AAA Access Accept to the value of
15 the MN-HA key allocated for the current session.
- 16 • The HAAA SHALL set the MN-hHA-MIP4-SPI attribute of the AAA Access Accept to the value of
17 the MN-HA-SPI associated with the MN-HA key.

18 When the HAAA receives the AAA Access Request message, along with the IMSI based NAI in User-Name
19 attribute and if the HAAA determines that the MS has an active PMIP6 session on the WiMAX side, the HAAA
20 SHALL set the LMA address in the Access Accept message to the address of the LMA that handles the current MS
21 session. If the in-band security mode is in use, the HAAA SHALL include the PMIP6-RK and the associated SPI
22 that are active for the current session, in the AAA Access Accept message.

23 The H-AAA SHALL send the AAA response to the PRIF.

24 **10.3.4 PRIF Requirements**

25 The PRIF SHALL follow the requirements specified in Section 8.4 of this specification.

26 **10.4 Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX® for IPv4 service**

27 The MS is initially connected to the 3GPP Pre-Rel8 network and the MS is assigned an IP address from its home
28 WiMAX® CSN as described in Section 8 of this document.

29 When a WiMAX access network is available and the Dual Radio MS decides to perform a HO to the WiMAX
30 access network, the MS performs the WiMAX entry procedure. After the WiMAX access authentication, all the
31 required keys for WiMAX access and mobility security are bootstrapped.

32 For consistency with the Pre-Rel8 Packet Core access, the MS can either use IMSI based NAI or regular WiMAX
33 NAI as specified in the section 9 of this document.

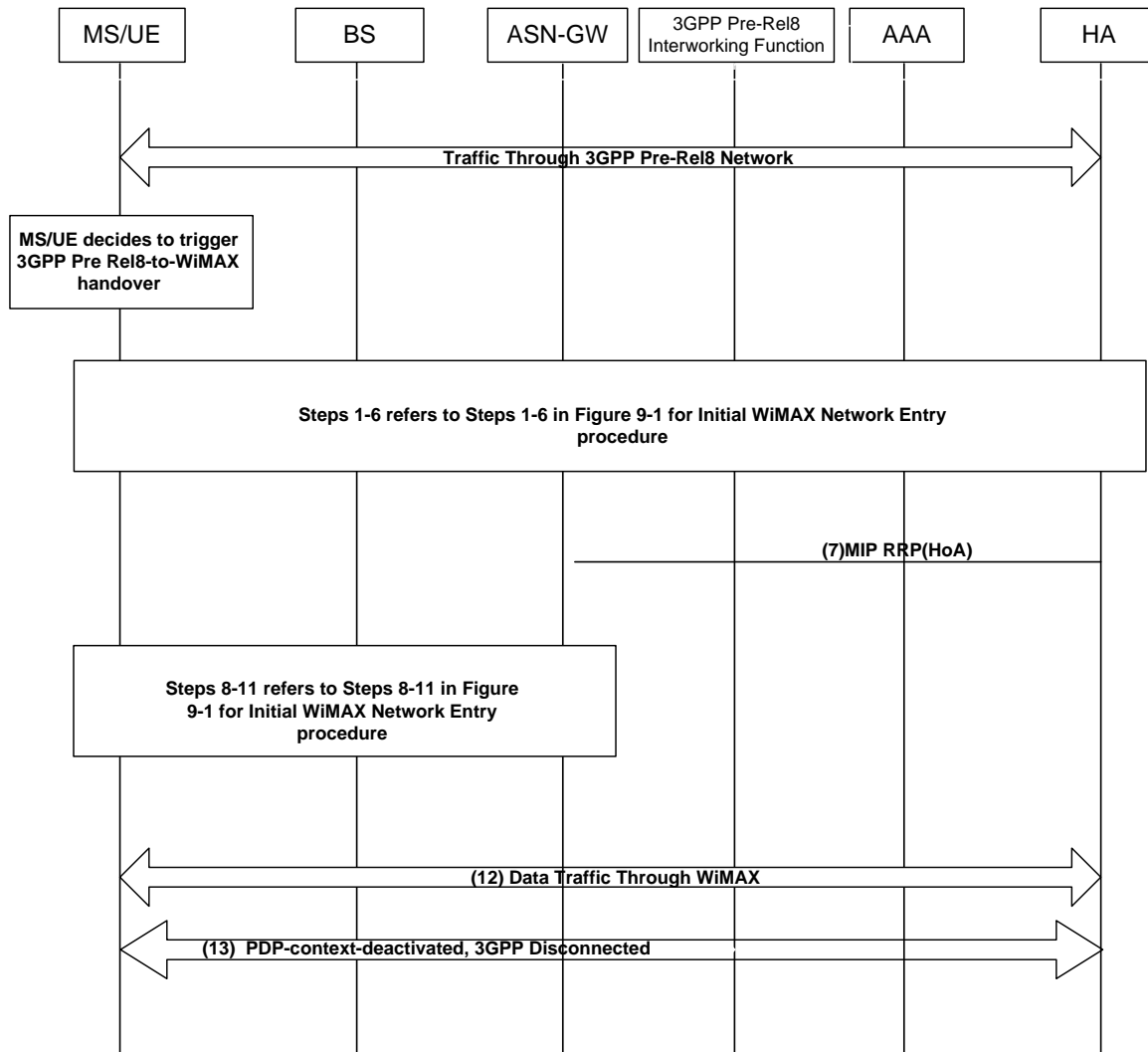
34

35 For the WiMAX access, a Dual Radio MS SHALL identify itself with the NAI during access authentication.

36 If a home operator chooses to protect subscriber identity when it is reported to the accessed network, the dual mode
37 mobile shall be configured to follow requirements of [1] Section 4.4.1.3.1 without any restrictions, i.e. a pseudo-
38 NAI can be used as an outer NAI. In such case, the IMSI-based NAI has to be provisioned in the H-AAA
39 subscription record. This IMSI-based NAI shall be returned by the H-AAA to the ASN-GW as the PMIP4-
40 Authenticated-Network-Identity received in AAA Access Accept. This IMSI-based NAI shall be used by the PMIP4
41 Client when assembling the PMIP4 RRQ.

42 If a home operator chooses not to protect subscriber identity when it is reported to the accessed network, the dual
43 mode mobile shall be preconfigured with the NAI based on IMSI, e.g. following the procedures specified in 3GPP
44 TS 23.003. The detail of NAI construction is specified in the section 9 of this specification.

1



2

Figure 11-3 - Handover from 3GPP Pre-Rel8 Packet Core to WiMAX® in case of IPv4 service

3

STEP 1-6

4

Same as steps 1-6 in Section 9.1.

5

STEP 7

6

Once the MN-HA AE is validated, based on the NAI, the HA assigns (if the HoA is set to all zero in the MIP RRQ) the same IP address that has been assigned when accessing the Pre-Rel8 Packet Core network by the WiMAX HA. The HA then updates the binding cache for the MS and sends PMIP4 RRP back to the ASN-GW, along with the HoA for the MS. If the HA doesn't support simultaneous binding, it will invoke release procedure as described in section 4.5.2.1.2.5 in [1].

7

8

9

10

11

STEP 8-11

12

Same as steps 8-11 in Section 9.1.

13

STEP 12

14

The data traffic for the MS can now be switched to the WiMAX network. Please note that if simultaneous binding is supported and as both radios (WiMAX and 3GPP) are "ON" the MS/UE can receive packets from both interfaces.

15

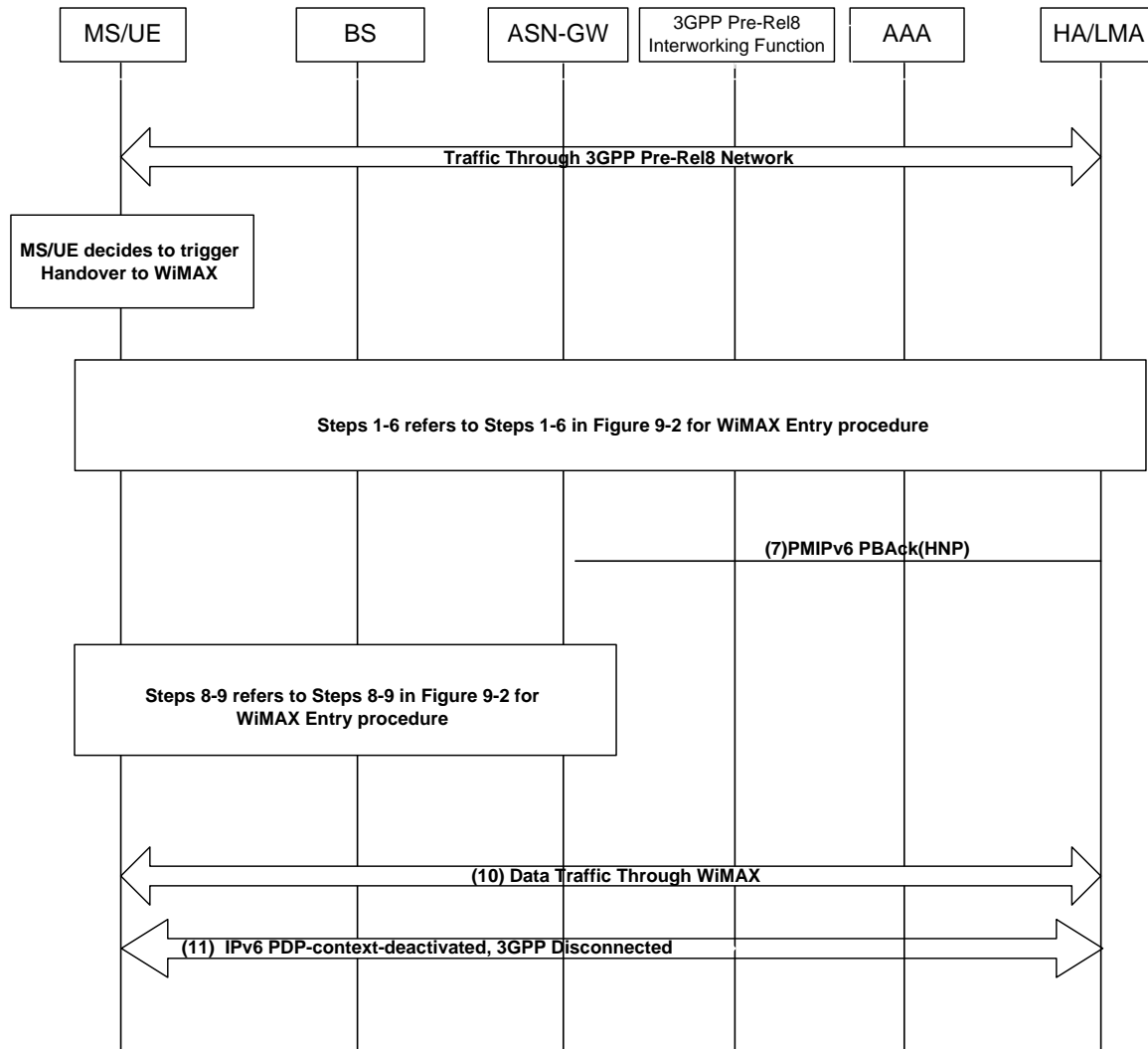
16

STEP 13

17

- 1 The MS deactivates the PDP Context and disconnects from the Pre-Rel8 Packet Core network and the HO is
- 2 complete. The MS is connected to the WiMAX network and traffic to and from the MS is provided through the
- 3 WiMAX network. The MS can perform the network exit procedure specified in this document.

4 **10.5 Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX® in case of IPv6**
5 **service**



6
7 **Figure 11-4 - Handover from 3GPP Pre-Rel8 Packet Core to WiMAX® in case of IPv6 service**

8
9 **STEP 1-6**

10 Same as steps 1-6 in Section 9.2.

11 **STEP 7**

12 Based on the NAI received in the PBU message, the LMA selects the same prefix for the MS that has been already
13 assigned to the MS on the Pre-Rel8 Packet Core side. The LMA then updates the binding cache entry for the MS
14 and sends PMIPv6 PBA back to the MAG in the ASN-GW, along with the HNP for the MS. The LMA also sends the
15 Binding Revocation message containing the MS NAI to the previous MAG in the PRIF to terminate the MS session
16 on the 3GPP side. The procedure for revoking PMIPv6 binding by the LMA is described in the [9].

1 **STEP 8-9**

2 Same as steps 8-9 in section 9.2.

3 **STEP 10**

4 The data traffic for the MS is switched to the WiMAX network.

5 **STEP 11**

6 The MS deactivates the IPv6 PDP Context and disconnects from the Pre-Rel8 Packet Core network and the
7 handover is completed. The MS is connected to the WiMAX network and traffic to and from the MS is provided
8 through the WiMAX network. The MS can perform the network exit procedure specified in this document.

9 **10.6 Requirements for Handover from 3GPP Pre-Rel. 8 Packet Core to WiMAX®**

10 **10.6.1 MS Requirements**

11 Once the MS makes a decision to handover from the 3GPP Pre-Rel8 core network to the WiMAX, the MS SHALL
12 perform the WiMAX Initial WiMAX network entry procedures as specified in section 9.1 of this document.

13 The MS SHALL verify that the IP address assignment received as the result of accessing the WiMAX core network
14 is the same as the IP address that the MS was assigned while communicating through the 3GPP Pre-Rel8 core
15 network. If the IP address assigned by the WiMAX network is different from the IP address that the MS was using
16 on the 3GPP Pre-Rel8 core network, the MS SHALL terminate the 3GPP Pre-Rel8 session and establish a new
17 WiMAX session.

18 The MS SHALL disconnect from the 3GPP Pre-Rel8 core network after the handover procedures are complete.

19 **10.6.2 HA/LMA Requirements**

20 During the handover from the 3GPP Pre-Rel8 network to WiMAX, the HA SHALL meet the following
21 requirements.

22 Upon receiving the PMIP4 RRQ from the WiMAX, the HA SHALL determine if an active binding already exists for
23 the MS NAI included in the RRQ. If an active binding does not exist, the HA SHALL follow the procedures
24 specified in section 9.1 of this specification. Otherwise, if an active binding already exists, the HA SHALL validate
25 the MN-HA AE included in the RRQ as defined in section 4.8.2 of [1]. Once the MN-HA AE is validated, the HA
26 SHALL respond to the WiMAX ASN GW with the PMIP4 RRP message setting its parameters as specified in
27 section 4.8.2 [1] with the following exception:

- 28
 - To preserve the IP session continuity, the HA SHALL set the HoA attribute in the RRP message to the
29 same IP address that is used for the MS currently active binding.

30 If the HA does not support simultaneous binding, it SHALL reject a simultaneous binding request. If it supports
31 simultaneous binding, the HA SHALL accept a new simultaneous binding request for a HoA/NAI having an already
32 active binding. In addition the HA SHALL provide packet duplication feature if multiple bindings to the same
33 HoA/NAI are active at the same time. If a new valid binding request is received for the same HoA/NAI and
34 simultaneous binding feature is not requested, the HA SHALL replace any existing active binding for a HoA/NAI
35 with the new one.

36 Upon receiving the PMIP6 PBU from the MAG in WiMAX ASN-GW, the LMA SHALL determine if an active
37 binding already exists for the MS NAI included in the PBU. If an active binding does not exist, the LMA SHALL
38 follow the procedures specified in section 9.2 of this specification. Otherwise, if an active binding already exists, the
39 LMA SHALL respond to the WiMAX ASN GW with the PMIP6 PBA message, setting its parameters as specified
40 in [9] with the following exception:

- 41
 - To preserve the IP session continuity, the LMA SHALL set the HNP attribute in the PBA to the same
42 IPv6 prefix that is used for the MS currently active binding.

1 Upon accepting the PMIP6 PBU from the PRIF, the LMA SHOULD terminate the PMIP6 session on the WiMAX
2 ASN side by sending the Binding Revocation Indication as described in [9].The security requirements for PMIP6
3 signaling and the processing of PMIP6 messages is as described in [9].

4 **10.6.3 AAA Requirements**

5 For general requirements, the WiMAX AAA SHALL be compliant with section 13.1 – AAA Requirements. For the
6 WiMAX access authentication during the MS handover from the 3GPP Pre-Rel8 network to WiMAX network, the
7 HAAA SHALL determine if an active session exists for this NAI in the 3GPP Pre-Rel8 core network. If the session
8 does not exist, the HAAA SHALL follow requirements defined in section 9.3 of this document. Otherwise, if the
9 session already exists, the AAA SHALL follow the AAA requirements defined in the section 11.3.3 for MS
10 handover from the WiMAX network to 3GPP pre-rel8 network.

11 The HAAA SHALL send the AAA response to the WiMAX ASN GW.

12 **10.6.4 ASN GW Requirements**

13 The ASN GW SHALL follow the requirements specified in Section 9.5 of this specification.

14

11. Network Exit Procedures

11.1 Network exit procedure initiated by MS or 3GPP Pre-Rel8 core network

Figure 12.1-1 represents MS or 3GPP Pre-Rel8 core network initiated network exit procedure.

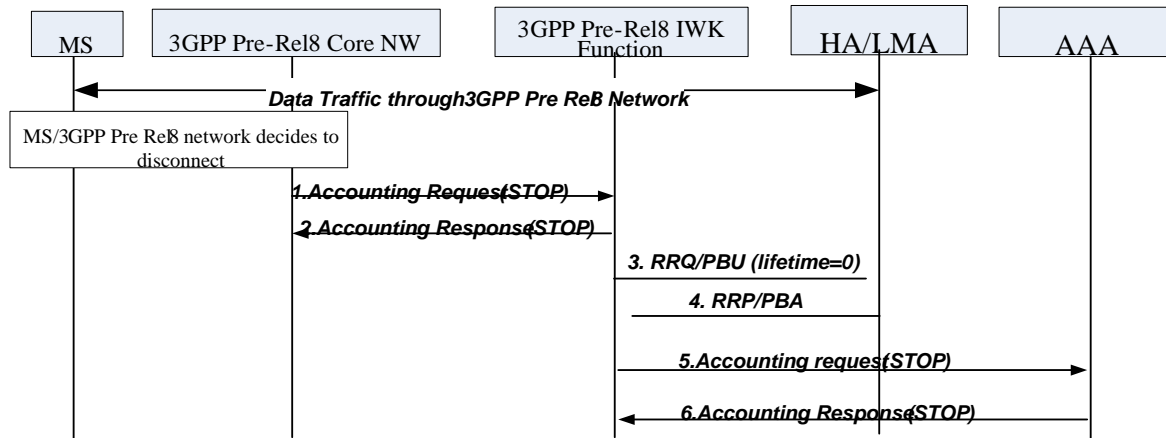


Figure 12.1-1 - MS or 3GPP Pre-Rel8 core network initiated network exit procedure

STEP 1

The MS/3GPP Pre-Rel8 network may decide to disconnect. In this case the 3GPP Pre-Rel8 Core network may send Accounting Request (STOP) message with the 3GPP Session Stop VSA to the PRIF. If this optional message is not received or supported by the PRIF, the PMIP session will time-out based on the PRIF and HA configuration.

STEP 2

PRIF on receiving the Accounting Request (STOP) with a Session Stop VSA, returns the Accounting Response (STOP) to the 3GPP system.

STEP 3

PRIF initiates MIP session release with HA/LMA by sending RRQ with lifetime=0 in case of PMIP4 or PBU with lifetime=0 message in case of PMIP6.

STEP 4

The HA/LMA sends RRP/PBA message back to the PRIF indicating release of the session.

STEP 5

The Accounting Client in the PRIF stops collecting traffic information and generates an Accounting Request (STOP) message with a 3GPP Session Stop VSA.

Note: 3GPP Session Stop VSA in the Accounting Request (STOP) may be used by the AAA as an indication of the 3GPP Pre-Rel8 accounting session being discontinued.

STEP 6

The AAA server returns Accounting Response (STOP) message to the PRIF.

Note: Step 2, step 3, and step 5 are triggered by the Accounting Request (STOP) in step 1, and can be executed in any sequence independent of each other.

11.2 Network exit procedure initiated by the HA/LMA

Figure 12.2-1 represents HA/LMA initiated network exit procedure.

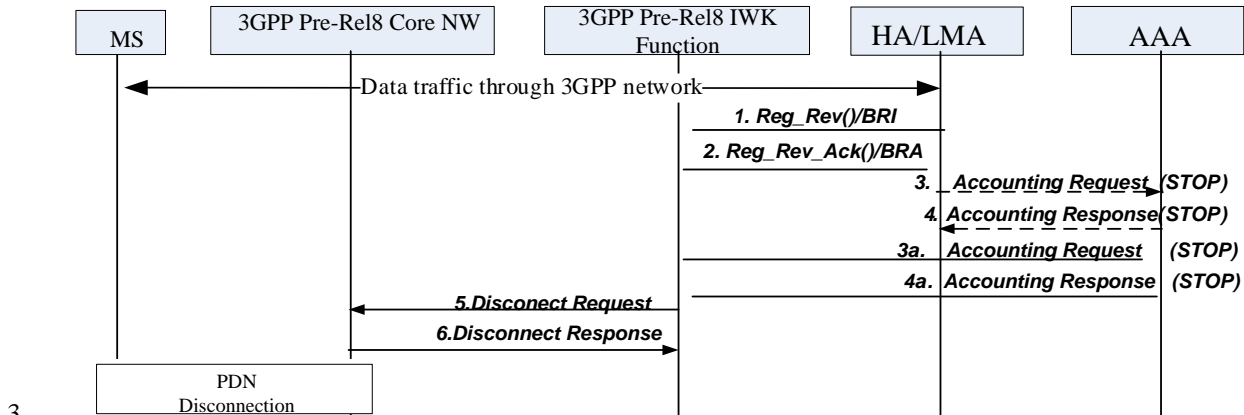


Figure 12.2-1- HA/LMA Initiated network exit

STEP 1

HA/LMA initiates network exit procedure by sending Registration_Revocation message to the IWK in case of PMIP4 or Binding Revocation Indication (BRI) message in case of PMIP6, performing MIP session release procedure as specified in [1].

STEP 2

The 3GPP Pre-Rel8 IWK responds with a Registration_Revocation_Ack message in case of PMIP4 or BRA message in case of PMIP6.

STEP 3a

The PRIF sends Accounting Request (STOP) message to the AAA server. This message can be sent without waiting for step 2.

STEP 3

Optionally the HA/LMA may contain the Accounting Client and in this case it sends the Accounting Request (STOP) message to the AAA server. This message can be sent by the HA/LMA without waiting for step 2.

STEP 4

The AAA server acknowledges the HA/LMA's accounting client by sending Accounting Response (STOP) message.

STEP 4a

The AAA server acknowledges the PRIF's accounting client by sending Accounting Response (STOP) message..

STEP 5

After the completion of the MIP Session Release procedure, the 3GPP Pre-Rel8 IWK function sends a Disconnect Request message to the 3GPP Pre-Rel8 network to indicate network exit.

STEP 6

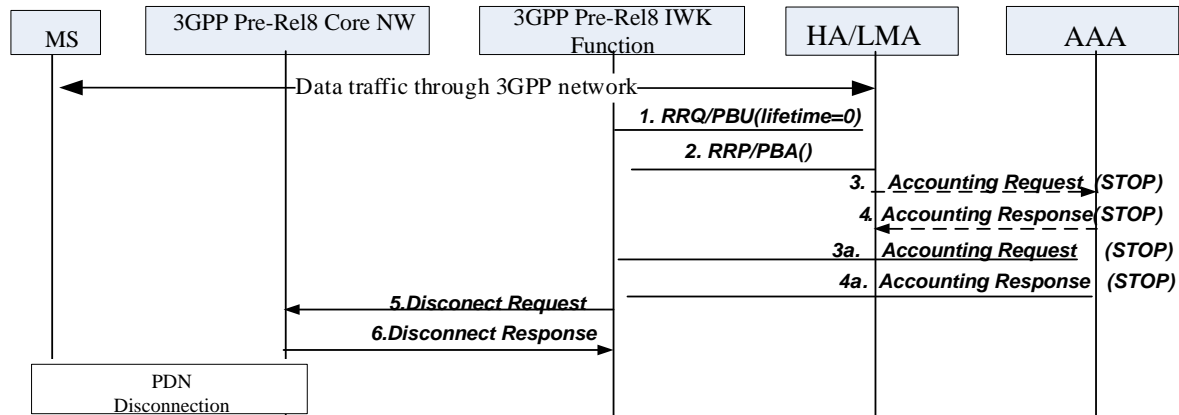
Upon receiving the Disconnect Request message, the 3GPP Pre-Rel8 Core returns a Disconnect Response message to the 3GPP Pre-Rel8 IWK function and performs session disconnect operation.

11.3 Network exit procedure initiated by the FA/MAG

This procedure can only take place during graceful shut down of the IWK Network Element for maintenance. No handover procedures SHALL be serviced during the shut down.

1 Figure 12.3-1 represents FA/MAG initiated network exit procedure.

2



3

4

Figure 12.3-1 - FA/MAG Initiated network exit

5 **STEP 1**

6 FA/MAG initiates network exit procedure by sending RRQ (lifetime=0) message to the HA/LMA in case of PMIP4
7 or PBU (lifetime=0) message in case of PMIP6, performing MIP session release procedure as specified in [1].

8 **STEP 2**

9 HA/LMA responds with a RRP message in case of PMIP4 or PBA message in case of PMIP6.

10 **STEP 3a**

11 The PRIF sends Accounting Request (STOP) message to the AAA server. This message can be sent without waiting
12 for step 2.

13 **STEP 3**

14 Optionally the HA/LMA may contain the Accounting Client and in this case it sends the Accounting Request (STOP)
15 message to the AAA server. This message can be sent by the HA/LMA without waiting for step 2.

16 **STEP 4**

17 The AAA server acknowledges the HA/LMA's accounting client by sending Accounting Response (STOP) message.

18 **STEP 4a**

19 The AAA server acknowledges the PRIF' accounting client by sending Accounting Response (STOP) message..

20 **STEP 5**

21 After the completion of the MIP Session Release procedure, the 3GPP Pre-Rel8 IWK function sends a Disconnect
22 Request message to the 3GPP Pre-Rel8 network to indicate network exit.

23 **STEP 6**

24 Upon receiving the Disconnect Request message, the 3GPP Pre-Rel8 Core returns a Disconnect Response message
25 to the 3GPP Pre-Rel8 IWK function and performs session disconnect operation.

26 **11.4 Network Exit Procedure initiated by the AAA**

27 Figure 12.4-1 represents AAA server initiated network exit procedure.

28

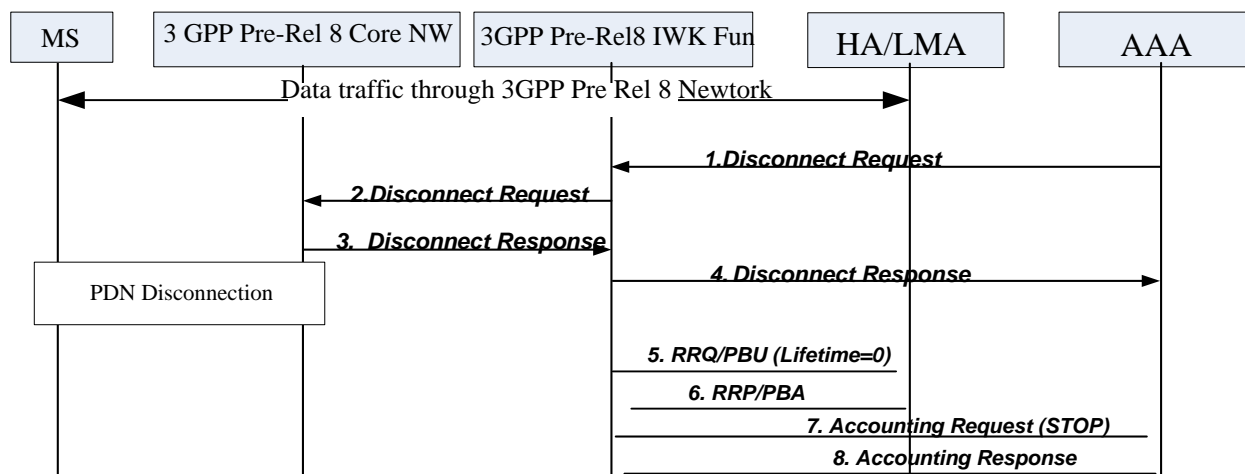


Figure 12.4-1 - AAA Initiated network exit

STEP 1

The AAA server sends Disconnect Request message to the PRIF to indicate a request to disconnect the 3GPP Pre-Rel8 session.

Note: This step is not expected to be triggered by the Accounting Request (STOP) message received from the PRIF containing the session Stop VSA

STEP 2

PRIF forwards the Disconnect Request message to the 3GPP Pre-Rel8 core network.

STEP 3

Upon receiving the Disconnect Request message indicating network exit, the 3GPP Pre-Rel8 core network returns a Disconnect Response message to the PRIF and performs the PDN Disconnection procedures.

STEP 4

PRIF forwards a Disconnect Response message to the AAA server.

STEP 5

PRIF initiates MIP Session Release with the HA/LMA by sending RRQ with lifetime=0 in case of PMIP4 or PBU with lifetime=0 message in case of PMIP6.

STEP 6

The HA/LMA responds to PRIF with a RRP/PBA message.

Note: Step 2 and step 5 are independent and can be executed by the PRIF independently.

STEP 7

The PRIF's Accounting client sends an Accounting Request (STOP) message to the AAA

STEP 8

The AAA server returns Accounting Response message to the PRIF.

11.5 PRIF Requirements

The PRIF SHALL be able to perform following operations:

- 1 • As the Proxy Mobile IP Client, e.g. PMIP4 MN or PMIP6 MAG, executes MIP session management
2 procedures.
3 • Notify a network exit event to the 3GPP Pre-Rel8 core network by sending the AAA Disconnect
4 Request message [3].
5 • Use the Accounting Request (STOP) from 3GPP Pre-Rel8 core network as the trigger for the PMIP
6 release.

7 The PRIF SHOULD be able to perform following operation:

- 8 • The PRIF re-generates the Accounting Request messages received from the 3GPP Pre-Rel8 core
9 network and sends them to the Accounting Server located in the WiMAX CSN.
10 • If the Accounting Client in the PRIF doesn't count user data information, it uses the accounting data it
11 may receive from the 3GPP Pre-Rel8 core network and relays it in the Accounting Request messages
12 to the WiMAX CSN.

13

1

2 **12. Policy and Charging Control**

3 For Policy and Charging Control, please refer to the informative description in Annex B.

4

5

13. Accounting

Accounting records for a session that involves WiMAX® and Pre-Rel8 3GPP networks SHALL be independently generated by the WiMAX NAS and CSN [1] and by the 3GPP Pre-Rel8 Core Network [3]. As described in Appendix A, since a subscriber can access both networks with different subscriptions simultaneously, subscriber or subscription based accounting can only be done after accounting records are consolidated and correlated at the back office. Hence the specification of subscriber or subscription based accounting is out of scope of this document.

For better correlation of the accounting records generated for the same session at each of the access networks, the PRIF also generate Accounting Records and may include User Data Records (UDRs) information that comply with the WiMAX format and send the UDRs to the HAAA. If accounting information is not collected, the counter values SHALL be set to zero. The correlation of the potential numerous sets of accounting records for the same session (i.e. 3GPP, PRIF, WiMAX, HA) by the billing mediation system is out of scope of this document. Nevertheless, if the WiMAX-Session-ID and the Chargeable User Identity (CUI) attributes are supplied by the AAA and the PRIF provides valid Accounting Records for the traversing 3GPP traffic, it SHALL include the WiMAX-Session-ID (carried in the Acct-Multi-Session-Id) and CUI in all the accounting messages and the generated UDRs. The WiMAX-Session-ID, the CUI and accounting records time stamps can be used to correlate the accounting records generated by the WiMAX system and the similar accounting records generated by the PRIF for the interworking session.

13.1 Accounting Information Collection

The accounting client in the PRIF MAY report counts of all data packets and octet counts sent and received through the FA/MAG to or from the mobile. Report of control and signaling data is optional. UDRs (User Data accounting Records) may be collected by the AAA client at the PRIF and sent to the HAAA. The UDR records SHALL conform to the RADIUS packet structure as defined in [1], [12] and [13] as well as in [14] for the case of Diameter. Also note that per the WiMAX accounting architecture described in [1], the HA/LMA in the CSN may also generate all or a subset of the accounting records that are generated at the PRIF.

13.2 PRIF Accounting Requirements

The PRIF SHALL generate IP-session based accounting records complying with the WiMAX accounting format specified in [1] and SHALL also support [11]. If the PRIF supports on-line accounting capabilities then it SHALL include the PPAC attribute in the RADIUS Access-Request packets.

The PRIF SHALL include the WiMAX Capability attribute in the RADIUS Access-Request packet or WiMAX-Capability AVP in the Diameter WEDR message during the 3GPP network attachment in order to indicate its capabilities to the HAAA. The PRIF SHALL also indicate support for IP session based accounting. If the PRIF receives an Access-Accept/WEDA in which the HAAA did not select IP session accounting mode, the PRIF SHALL not generate UDRs, nor provide any Accounting information to the AAA.

When full Accounting Information is generated by the PRIF, any incoming accounting message from the 3GPP Pre-Rel 8 network SHALL NOT be forwarded to the AAA.

14. AAA implications

14.1 WiMAX® AAA Requirements

The AAA SHALL conform to the WiMAX specifications [1]. For supporting single set of credentials the WiMAX AAA SHALL support the Wx and MAY also support Gr' interface (a deployment choice) to the HLR [3]. During an initial WiMAX network access, the H-AAA SHALL extract the IMSI information from the IMSI based NAI either reported directly from EAP Identify Response, or provisioned in the H-AAA. In the case where a home operator chooses to protect subscriber identity then it SHALL maintain a non-IMSI based NAI associated with IMSI. In such case, the WiMAX H-AAA SHALL be provisioned with user's IMSI based NAI and the H-AAA SHALL map the non-IMSI based and send the non-IMSI based NAI to the ASN-GW as PMIP-Authenticated-Network-Identity in AAA Access Accept. The IMSI information SHALL be used by the AAA to send to the correct HLR/HSS a request for the authentication vector if the authentication credentials are shared between the 3GPP Pre-Rel8 and the WiMAX systems.

After a successful WiMAX access authentication, the H-AAA SHALL return IMSI-based NAI to the ASN-GW which contains the Anchor Authenticator (AA), the PMIP4 Client, and MAG in the case of IPv6. This IMSI-based NAI SHALL be used by the PMIP4 Client when assembling the MIP RRQ messages or it SHALL be used by the MAG when assembling the PMIP6 PBU message.

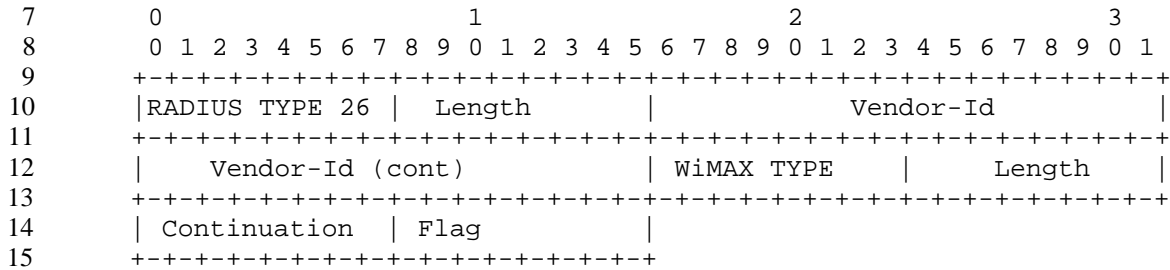
AAA SHALL also support the AAA requirements specified in section 8.5, 9.3, 11.3.3, 11.6.3.

The WiMAX H-AAA SHALL support the 3GPP defined vendor specific attributes specified in [3].

15. WiMAX® RADIUS VSA for Interworking with 3GPP Pre-Rel8 Network

WiMAX® RADIUS VSAs are transported in a RADIUS Vendor Specific Attribute. The general format of WiMAX VSAs is defined in the section 5.4.2 of WiMAX Forum® Network Architecture stage 3 specification[1].

15.1 WiMAX-NAS-Type



WType-ID	234 for WiMAX-NAS-Type
Description	This attribute Shall appears in the AAA Access Request and Accounting packets to indicate the WiMAX® NAS Type When this attribute is absent (in the case of previous WiMAX specifications) then the AAA server determines the NAS type by the presence or absence of the NAS-Port-Type attribute . The presences of this attribute MUST NOT preclude the presence of the NAS-Port-Type attribute which may be required by other standards.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. An enumerated value defined as follows: 0: Reserved 1: ASN Gateway 2: Home Agent 3: Pre-Release 8 Interworking Function (PRIF) 4: Wi-Fi Interworking Function (WIF) All other values reserved.

17
18
19

1 **Annex A, Deployment Scenarios (Informative)**

2 This Informative Annex provides some examples of deployment scenarios that can be addressed by the interworking
3 solutions described in this document. This document does not claim to cover all possible deployment scenarios. The
4 following deployment models are considered by this Document for WiMAX/Pre-Rel 8 3GPP Interworking.

- 5 • The WiMAX® network may be directly owned by a 3GPP operator.
 - 6 ○ In this case, the Operator may continue utilizing the 3GPP HLR/HSS as the main repository of
7 authentication credentials. To accommodate the WiMAX access, the Operator will deploy the
8 WiMAX AAA, which will obtain the authentication parameters from the 3GPP HLR/HSS using
9 Wx/Gr' [5] in order to conduct the WiMAX EAP Authentication as per RFC 4187 or RFC4186
10 (optionally)
 - 11 ○ Alternatively, the Operator may provision all dual mode subscriber terminals with a second
12 subscription specific to the WiMAX access and retain this second subscription at the WiMAX
13 AAA. In this case upon network entry, independent authentication takes place in the respective
14 access network.
- 15 • The WiMAX network may belong to a WiMAX operator who has a partnership/agreement with a 3GPP
16 operator.
 - 17 ○ Each operator may conduct an independent authentication of the dual mode mobiles by their
18 respective systems. In such case, the dual mode terminals will have to be provisioned with an
19 independent dual set of access credentials.
 - 20 ○ The WiMAX Operator may use the 3GPP HLR/HSS as the main repository of authentication
21 credentials for his subscribers. When a dual mode mobile attempts to access the WiMAX network,
22 the WiMAX Operator's AAA will query the authentication parameters from the 3GPP HLR/HSS
23 in order to conduct the WiMAX EAP Authentication [5].

24 It is assumed that roaming agreements between different 3GPP operators, as well as between different WiMAX
25 operators, will accommodate the interworking involving different home and serving networks. Such roaming
26 scenarios are outside of scope of this document.

27

1 **Annex B: Architectural options for integrating 3GPP Release-**
2 **7 PCRF (Informative)**

1 **B.1 PCC Architecture Overview**

2 For PCC functionality, the PCEF entities are located in the GGSN and in the ASN-GW. 3GPP pre-R8 PCC assumes
3 a single, fixed PCEF for the lifetime of an IP session, i.e., the traffic plane for each IP session passes through a
4 single PCEF and there is no support for relocation of a PCEF during a session. In an interworking architecture
5 however, the PCEF associated with the user session changes during a HO and thus PCC relocation can't be
6 supported after inter-RAT handover. Therefore, a new PCC session and policies are separately installed in each
7 access technology even when the MS maintains the same ID and IP address after an inter-RAT handover.

8 The following sections describe options for integrating PCC in WiMAX – 3GPP Pre-Rel-8 IWK;

B.3 Shared 3GPP Rel-7 PCRF with WiMAX® extensions

An operator can choose to upgrade its 3GPP Release 7 PCRF and integrate the WiMAX PDF with it so that it can serve both access networks and support PCC session association. The PCEF entity associated with a user session changes from one network to the other during a HO. When the PCRF serves both access networks, it is able to correlate the Gx Diameter session with the GGSN to the PCC-R3-P Diameter session with the ASN-GW and after handoff installs the same policy and charging rules when applicable. It can also ensure termination of the old session in scenarios where the MS does not disconnect from the network it is leaving during the HO.

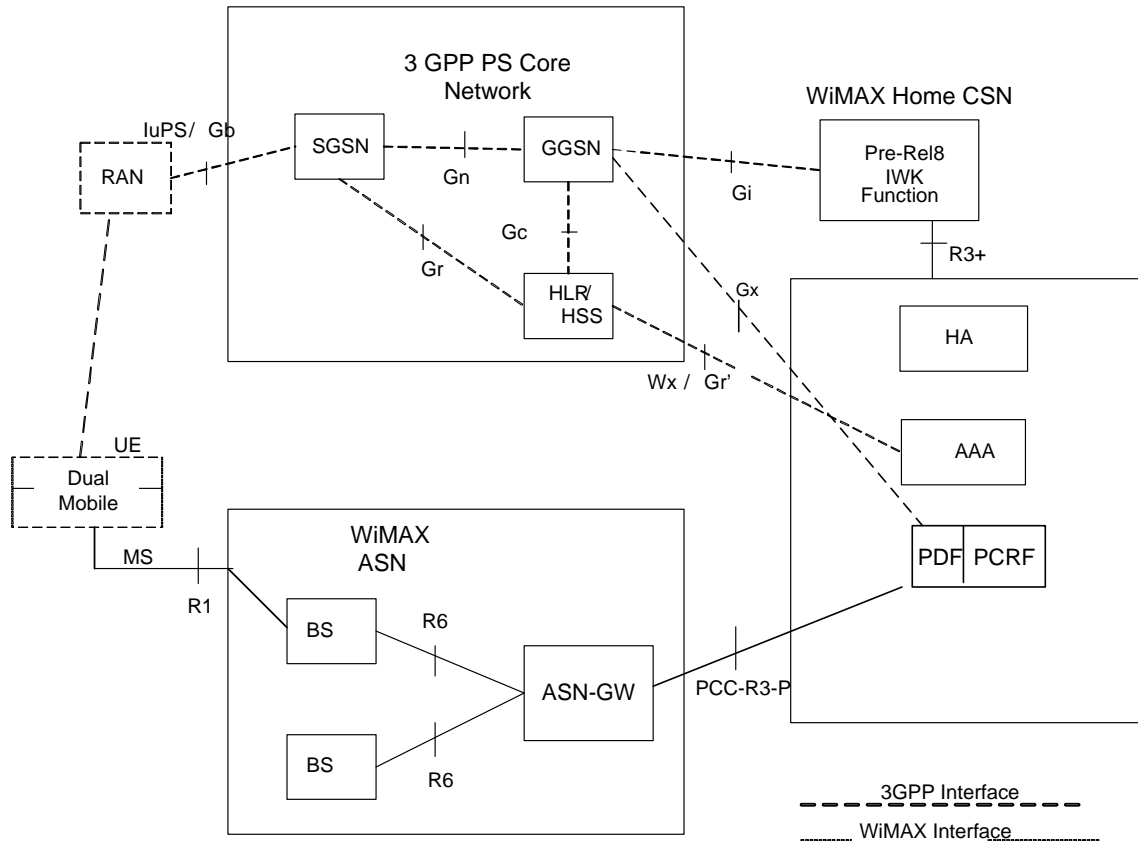


Figure B-2 - Shared PCRF for both networks

B.3.1 PCEF re-location during HO from 3GPP to WiMAX®

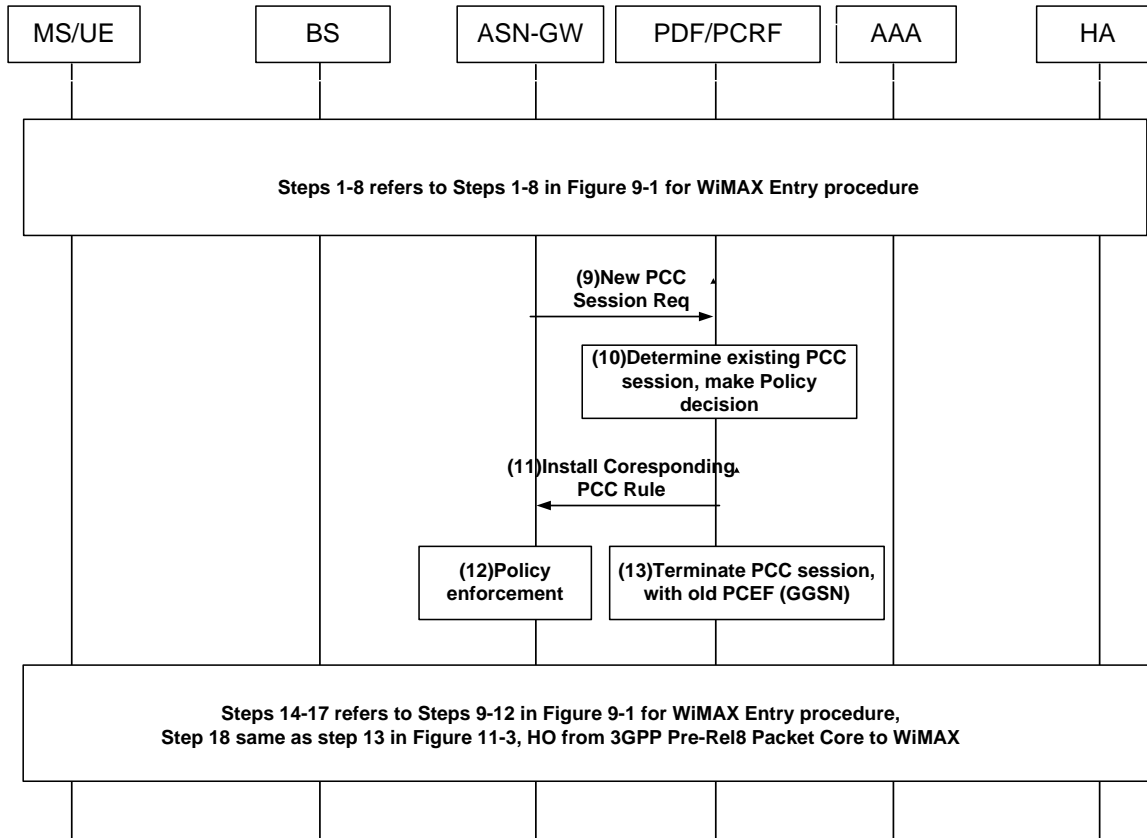


Figure B-3 - HO from 3GPP to WiMAX® with a Shared PCRF

STEP 1-8

Same as steps 1-8 in Figure 9-1, WiMAX Initial Network Entry.

STEP 9

The PCEF in the ASN-GW sends request for PCC rules for the new IP CAN session establishment to the PDF/PCRF.

STEP 10

PCRF checks for existing PCC session contexts associated with the new request. It uses either the Subscription ID or IP Address information in the request to perform the association. If there is an existing session, the PCRF makes the authorization and policy decision to send either the existing or updated PCC rules to the new PCEF.

STEP 11

PCRF provides the old or updated PCC rules to the PCEF.

STEP 12

PCEF installs the PCC rules received from the PCRF.

STEP 13

PCRF initiates PCC session termination with the old-PCEF in the GGSN.

STEP 14-17

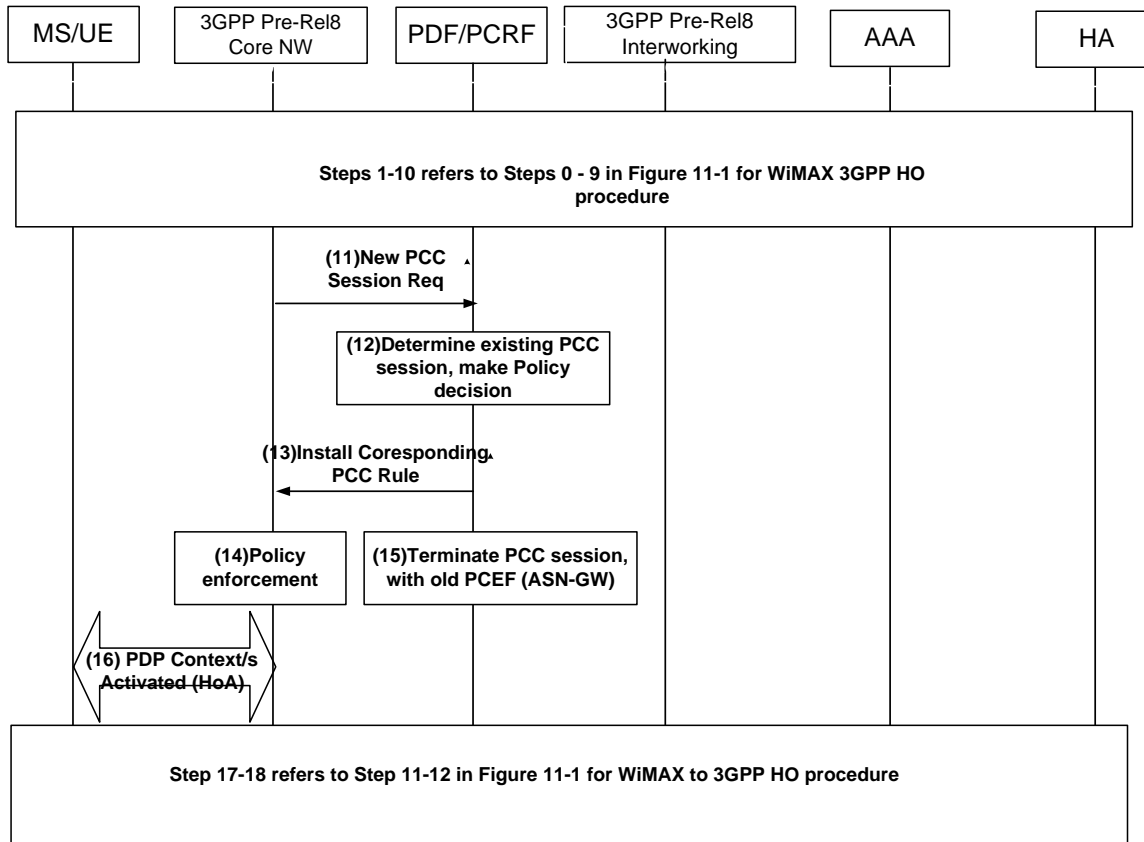
Same as steps 9-12 in Figure 9-1, WiMAX Initial Network Entry.

STEP 18

Same as step 13 in Figure 11-3, HO from 3GPP Pre-Rel8 Packet Core to WiMAX

1
2
3
4
5

B.3.2 PCEF re-location during HO from WiMAX® to 3GPP



6
7
8

Figure B-4 - HO from WiMAX® to 3GPP with a shared PCRF

9 STEP 1-10

10 Same as steps 0-9 in Figure 11-1, in Section 11.1, WiMAX to 3GPP Pre-Rel8 Packet CoreHO.

11 STEP 11

12 The PCEF in the GGSN (which is part of the Release 7 3GPP core) sends request for PCC rules for the new PDP
13 context establishment to the PCRF.

14 STEP 12

15 PCRF checks for existing PCC session contexts associated with the new request. It uses either the Subscription ID or
16 IP Address information in the request to perform the association. If there is an existing session, the PCRF makes the
17 authorization and policy decision to send either the existing or updated PCC rules to the new PCEF.

18 STEP 13

19 PCRF provides the old or updated PCC rules to the PCEF

1 **STEP 14**

2 PCEF installs the PCC rules received from the PDF.

3 **STEP 15**

4 PCRF initiates PCC session termination with the old-PCEF in the ASN-GW.

5 **STEP 16**

6 In step 16, the GGSN initiates secondary PDP context(s) in addition to the primary one, for the handover of multiple
7 service flows with different QoS characteristics, depending on the PCC rules received from the PCRF. It is expected
8 that these secondary PDP contexts for the HO services flows will be initiated by the GGSN and not by the MS to
9 avoid any race conditions.

10 **STEP 17-18**

11 Same as steps 11-12 in of Figure 11-1, WiMAX to 3GPP Pre-Rel8 Packet Core HO.

12