WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

Single Radio Interworking between Non-WiMAX® and WiMAX® Access Networks

WMF-T37-011-R016v01

WiMAX Forum® Approved

(2010-11-30)

WiMAX Forum Proprietary

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Document Scope

This document specifies Stage 2 and Stage 3 specifications for Single Radio interworking from Non-WiMAX Access Networks to mobile WiMAX® Access Networks. It covers the various interworking aspects such as authentication and authorization, handover, etc. for the Single Radio MS[1]. The Single Radio handover solution from WiMAX to 3GPP2/Wi-Fi® networks is defined in other specifications.

2 Abbreviations and Definitions

2.1 Abbreviations

FQDN Fully Qualified Domain Name

INE Initial Network Entry

RAT Radio Access Technology

RRQ Registration Request

SFF Signaling Forwarding Function

2.2 Terms & Definitions

Single Radio MS: A multimode MS, depending on packaging configurations, operating with only one active radio may be transmitting and one or more active radios receiving only at a time.

Dual Radio MS: A multimode MS that can have both radios (transmitting and receiving) active at the same time. A DR MS can simultaneously transmit and receive on both radios (for e.g. WiMAX and 3GPP). A DR MS may behave as a SR MS by operating in Single Radio Mode.

Non-WiMAX Access Networks: Refers to other IP based Radio Access Networks which an operator may utilize to provide IP services that do not adhere to the WiMAX® IEEE Std 802.16. Examples include Wi-Fi®, 3GPP2 HRPD, 3GPP LTE, 3GPP HSPA.

Preregistered ASN-GW: An ASN-GW with connectivity to the WiMAX SFF and hosts the Paging Controller and Authenticator for the SR MS.

WiMAX® pre-registration: Pre-registration is the procedure of creating a pre-registered session in a WiMAX SFF and a WiMAX ASN-GW while being active on a non-WiMAX network. Pre-registration happens while being served by non-WiMAX network over an established tunnel between the WiMAX SFF and the SR MS. Pre-registration procedure involves a WiMAX initial network entry through the tunnel and its successful completion when an Initial Service Flow (ISF) is created.

Pre-registered Session: A WiMAX session context, established for a SR MS, while it receives service from a non-WiMAX serving network. The pre-registered session is established by the SR MS and the WiMAX network via the serving non-WiMAX air interface and the Layer 3 network interface between the WiMAX and non-WiMAX networks. A pre-registered WiMAX session facilitates low latency inter-RAT handovers from a non-WiMAX network to the WiMAX network.

[1] MS is also referred as Terminal or Device in this specification.

3 References

This section lists the details of references used in this specification.

[1] WMF-T33-001-R016, WiMAX Forum® Network Architecture – Detailed Protocols and Procedures Base Specification

[2] WiMAX Forum® Mobile System Profile

[3] 3GPP TS 23.401: "3GPP System Architecture Evolution: GPRS Enhancements for E-UTRAN Access".

[4] 3GPP TS 23.402: "3GPP System Architecture Evolution: Architecture Enhancements for non-3GPP accesses".

[5] 3GPP TR 23.882: " 3GPP system architecture evolution (SAE): Report on Technical Options and Conclusions (Release 7)" V 1.12.0 (2007-10)

[6] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions", March 1977

[7] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", July 2003

[8] IETF RFC3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", December 2003

[9] 3GPP2, X.S0058: "WiMAX-HRPD Interworking: Core Network Aspects"

[10] 3GPP2 A.S0023: "Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces and Interworking with World Interoperability for Microwave Access (WiMAX)"

[11] 3GPP2, X.S0013-014: "All-IP Core Network Multimedia Domain: Service Based Bearer Control – Ty Interface Stage 3"

[12] IETF, RFC 3344: "IP Mobility Support for IPv4", August 2002

[13] IETF, RFC 3775: "Mobility Support in IPv6", June 2004

[14] IETF, RFC 2131: "Dynamic Host Configuration Protocol", March 1997

[15] IEEE Std 802.16-2009, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Broadband Wireless Access Systems

[16] WMF-T37-010-R016, WiMAX Forum® Network Architecture – Architecture, detailed Protocols and Procedures – Wi-Fi® – WiMAX® Interworking

[17] 3GPP TS 23.203: "Policy and charging control architecture"

[18] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access network (E-UTRAN); Overall description; Stage 2"

[19] WMF-T37-008-R016, WiMAX Forum® Network Architecture – Interworking Specification WiMAX® – Pre-Release 8 3GPP Interworking

[20] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2"

4 Requirements and Principles

This section defines the assumptions, architectural principles and requirements.

4.1 Need for Single Radio Handovers

There is a need to support Single Radio Handovers between WiMAX® and Non-WiMAX Access Networks in multi-mode devices for the following reasons:

1. Only one radio can operate satisfactorily at any given point of time due to co-existence, interference, platform noise and other such issues for radios operating in close frequency ranges (e.g. for radios in IMT-2000 bands).
2. The battery in a multi-mode device may be able to support only a single radio at a time. Multi-radio operation may lead to higher power requirements at any point of time, leading to need for larger battery sizes in mobile devices.
3. Due to regulatory and other issues, simultaneous multi-radio operation may not be always possible.

4.2 Requirements for Single Radio Handovers

The following are some of the general requirements and principles for single radio handover.

1. The single radio handover solution shall enable handovers between WiMAX® and Non-WiMAX Access Networks.
2. The impact on existing core network elements shall be minimized such as for 2G/3G. The impact on Non-WiMAX Access Networks (HRPD, GERAN and UTRAN) shall also be minimized.
3. The mobility management procedures for single radio handover shall include mechanisms to minimize service interruption during handover and shall support bi-directional service continuity wherever possible.

4.3 Overview of Single Radio Handover Modes

Inter-RAT Single Radio handover reduces service interruptions experienced by the user of a SR MS during inter-RAT handovers between non-WiMAX® and WiMAX access networks. Single radio non-WiMAX to WiMAX inter-RAT handover includes network and SR MS support for three additional modes of service in addition to the existing WiMAX Active and Idle modes of service:

1. **NULL Mode:** A SR MS receiving service from a non-WiMAX network and with no pre-registered WiMAX session and WiMAX SFF context is considered to be in WiMAX NULL mode from the network and SR MS perspective.
2. **Pseudo-Active Mode:** WiMAX Pseudo-Active mode is similar to WiMAX Active mode (i.e. R6 connection, transport security association, PMIP resources are allocated) except the SR MS maintains two sessions, a pre-registered inactive session in the WiMAX network and an active on-going session in the non-WiMAX network where it continues to receive service from.
3. **Pseudo-Idle Mode**: WiMAX Pseudo-Idle mode is similar to WiMAX Idle mode except the SR MS maintains two sessions, its pre-registered inactive session in the WiMAX network and an active on-going session in the non-WiMAX network where it continues to receive service from. Principles for support of Single Radio Handover to WiMAX network

4.4 Principles for support of Single Radio Handover to WiMAX® network

The following principles SHALL apply to the WiMAX® network and SR MS for non-WiMAX to WiMAX inter-RAT handover support:

1. The SR MS initiates WiMAX pre-registration for inter-RAT handover based on operator policy and/or user preferences.

2. After the SR MS completes the inter-RAT handover pre-registration and transitions to Pseudo-Active mode, the SR MS may initiate Pseudo-Idle mode entry or remain in Pseudo-Active mode based on operator policy.
3. The WiMAX network may reject the SR MS initiated WiMAX pre-registration. The rejection may be based on operator policy, overload, or maintenance conditions. If for any reason the WiMAX network rejects or cancels the SR MS inter-RAT handover pre-registration the WiMAX network SHALL include a cause code indicating to the SR MS the reason for the rejection or cancelation, e.g. resources not available, operator's policy, etc.
4. The WiMAX network Pseudo-Active mode timer shall be in the order of seconds and shorter in duration than the Pseudo-Idle mode timer.
5. In order to avoid ping-pong effect during WiMAX to non-WiMAX Single Radio inter-RAT handover, the SR MS context (if already exists) may be retained at a WiMAX SFF based on operator policy such as RAT type etc. In this case the WiMAX SFF maintains the SR MS context up to a “Retain-Time” configurable value. During the “Retain-Time” period, the WiMAX network may transition the SR MS to a WiMAX Pseudo-Active mode and from there possibly to a WiMAX Pseudo-Idle mode.

   Note: Operator policy may be based on SLA, RAT type, Type of services supported by the SR MS e.g., the SR MS may initiate WiMAX pre-registration or Pseudo-Idle mode entry only if the real time services are at the time are being supported by the SR MS on the non-WiMAX network, or the Network may reject WiMAX pre-registration if no real time services are at the time being supported by the SR MS (determined during session pre-registration).

5 Single Radio Interworking Architecture Reference Model

5.1 Network Architecture

This section defines the Network Reference Model for the Single Radio Interworking of the Mobile WiMAX® system with Non-WiMAX Access Networks.

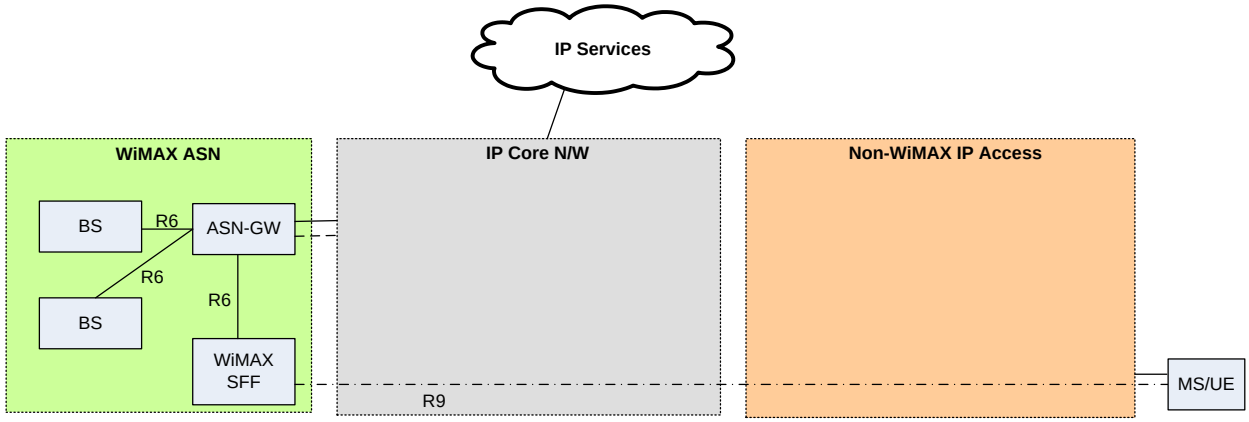


Figure 6-1 – WiMAX® Single Radio Interworking Architecture (Non-WiMAX Access Network to WiMAX Handover)

5.2 Functional Elements

5.2.1 WiMAX® SFF

WiMAX® Signal Forwarding Function (SFF) is a new functional element that is required to support Single Radio handovers from Non-WiMAX IP Access Network to WiMAX. The WiMAX SFF provides layer 3 tunneling. The UE/MS communicates with the WiMAX SFF over the Non-WiMAX Access Network in order to pre-register and execute the handover from the non-WiMAX Access Network to the WiMAX Network.

The WiMAX SFF facilitates pre-registration and authentication while the UE/MS is connected via the non-WiMAX Access Network prior to active handover to the WiMAX Network. WiMAX SFF and the SR MS exchange IEEE 802.16-2009 MAC messages over the R9 interface.

The WiMAX SFF is deployed within an operator's network and may use a private IP address. These procedures allow an UE/MS to securely communicate with the WiMAX SFF in an operator's private network.

5.3 Reference Points

R9: R9 is a new reference point between the UE/MS and the WiMAX SFF. It is used to tunnel IEEE 802.16 MAC layer signaling and WiMAX messages to/from the UE/MS over the non-WiMAX Access Network.

R6: R6 is interface between the WiMAX SFF and an ASN-GW. The R6 is the same as the interface between the WiMAX BS and ASN-GW defined in [1].

6 Single Radio Inter-RAT Handover Procedures

6.1 WiMAX® SFF Discovery

Prior to performing active handover from the Non-WiMAX® Access Network to a WiMAX network, the UE/MS discovers the IP address of the WiMAX SFF while active in the non-WiMAX Access Network. WiMAX SFF discovery consists of two steps. The first step is domain name discovery, which is necessary in order to construct a Fully Qualified Domain Name (FQDN) for the WiMAX SFF.

The next step is a WiMAX SFF IP address discovery (Section 7.1.1). The UE/MS performs a Domain Name System (DNS) query with the FQDN constructed with the qualified domain name and a WiMAX network specific identifier (WiMAX Base Station Identification (BS ID)). The DNS returns the IP address of the WiMAX SFF serving the WiMAX Network in location identified in the query.

Communication between the UE/MS and the WiMAX SFF SHOULD be secured. IPsec may be used to secure the messages exchanged between the UE/MS and the WiMAX SFF.

6.1.1 WiMAX® SFF Discovery procedure

Figure 7-1illustrates an example call flow for the discovery of the WiMAX® SFF.

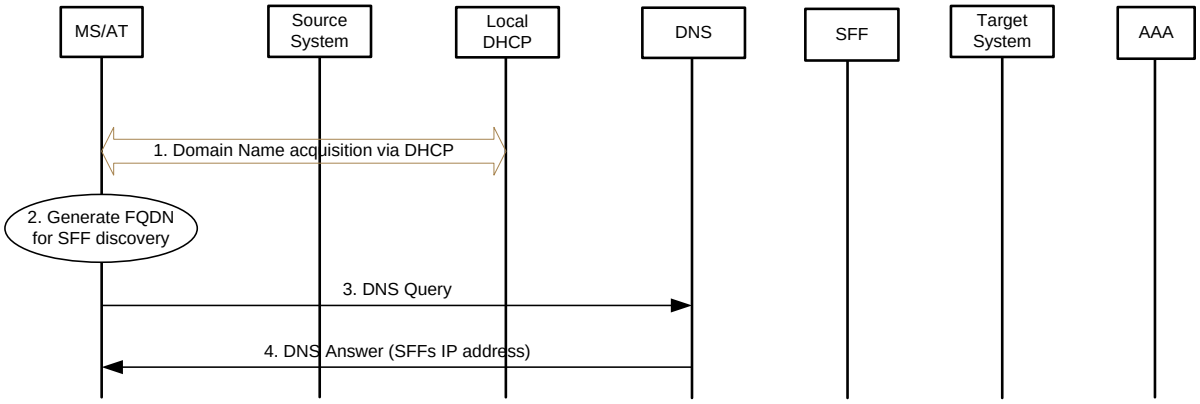


Figure 7-1 – WiMAX® SFF Discovery

1. The UE/MS acquires the domain name via DHCP message exchange. The DHCP procedure is done as in [14]
2. The UE/MS generates the FQDN for the WiMAX SFF with the domain name acquired in step 1. FQDN is generated as below:

   <WiMAX-BSID>.WiMAX.SFF.<domain name>

   Note: WiMAX-BSID is learned by the MS/UE at the WiMAX Network Discovery and Selection stage.
3. The UE/MS sends a DNS query to the DNS Server including the FQDN.
4. The DNS server responds with a DNS answer including the WiMAX SFF's IP address.

6.2 Non-WiMAX® to WiMAX® Handover

This section describes Single Radio inter-RAT handover support from Non-WiMAX network (E.g.: Wi-Fi®, 3GPP or 3GPP2 network) to WiMAX. Single Radio inter-RAT handover procedure is composed of 5 phases. Figure 7-2 provides a high level overview of the non-WiMAX to WiMAX Single Radio Inter-RAT Handover Procedure.

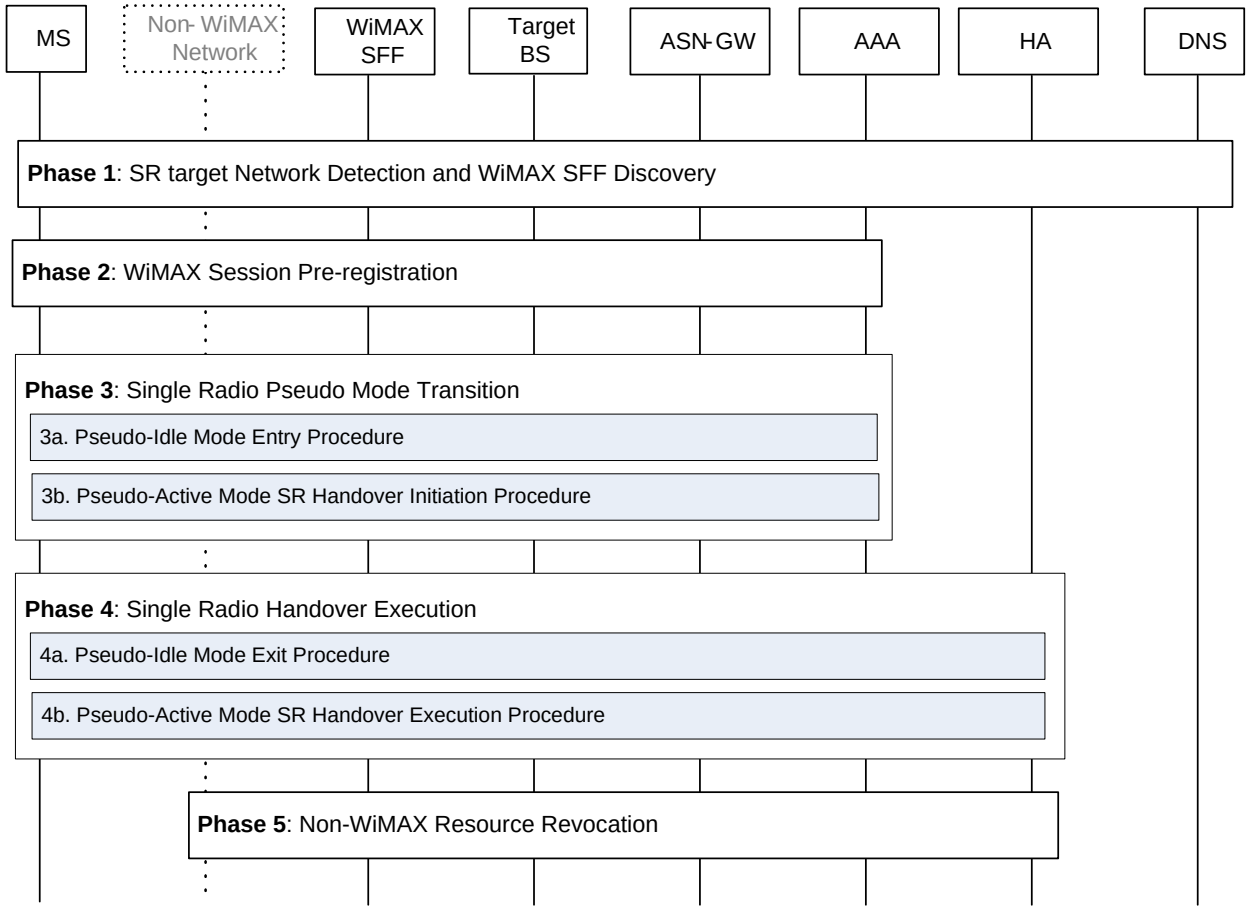


Figure 7-2 – Single Radio Handover Procedure from non-WiMAX® to WiMAX® Network

Phase 1 is the Target Network Detection and WiMAX SFF Discovery Phase involving a single radio MS, detecting the presence of a WIMAX network signal and discovering the address of the WiMAX SFF. The WiMAX SFF simulates a WiMAX BS in the WiMAX network. Once the SR MS discovers the address of the WiMAX SFF the first phase of the handover procedure is completed.

Phase 2 of the SR inter-RAT handover procedure is the WiMAX Session Pre-Registration Phase. In this phase, the SR MS, WiMAX SFF, ASN-GW and the AAA complete the existing WiMAX initial network entry procedure. Prior to completing this procedure, the SR MS may initiate the establishment of a secure (IPSec) tunnel between it and the WiMAX SFF in the WiMAX network. If the optional secure tunnel is established, initial network entry procedures between the SR MS and WiMAX SFF are completed through the secure tunnel. Upon completion of WiMAX session pre-registration (i.e. ISF established), the SR MS enters Pseudo-Active mode.

Phase 3 of the SR inter-RAT handover procedure is the Single Radio Pseudo Mode Transition Phase. Phase 3 occurs over the WiMAX SFF tunnel. As part of Phase 3 either Phase 3a or 3b happens. Selection procedure for

Phase 3a or Phase 3b is defined in section 5.4. In case of phase 3a, SR MS transitions from Pseudo-Active mode to Pseudo-Idle mode by performing Pseudo-Idle mode entry procedure. Alternatively in case of phase 3b, SR MS initiates Pseudo-Active mode SR handover initiation procedure as described in section 7.2.3.2 Since the WiMAX SFF emulates a WiMAX BS, the WiMAX SFF emulates the source BS while the target WiMAX BS performs the WiMAX target BS role.

Phase 4 of the SR inter-RAT handover procedure is Single Radio Handover Execution phase. Phase 4 occurs over the WiMAX Radio Interface. As part of phase 4 either phase 4a or 4b happens. Phase 3a is followed by phase 4a and phase 3b is followed by phase 4b. In case of 4a, SR MS transitions from Pseudo-Idle mode to WiMAX Active mode by performing Pseudo-Idle mode exit procedure. Alternatively in case of phase 4b, SR MS initiates Pseudo-Active mode SR handover execution procedure as described in section 7.2.4. As part of SR Handover Execution phase, the SR MS, ASN-GW and the HA/LMA perform existing IP allocation procedures to obtain the same IP address for the MS from the HA/LMA Since the HA/LMA is the session anchoring element, for seamless session continuity it assigns the same IP address (HoA) that is being used for the same session by the SR MS in the non-WiMAX source network.

Finally in **Phase 5**, once the SR MS obtains the same IP address from the HA/LMA as used in the source non-WiMAX network and completes the SR Handover Execution Phase, the source non-WiMAX network releases the network resources previously allocated to the MS. This is known as the SR Handover Resource Revocation Procedure

Detailed procedures for the different phases are described in the sections below:

6.2.1 Phase 1: SR Target Network Detection and WiMAX® SFF Discovery

The SR MS connected to the non-WiMAX network, may acquire the WiMAX network details from the Information Server such as ANDSF. The Information Server contains data management and control functionality necessary to provide network discovery and selection assistance data as per operators' policy. The Information Server is able to initiate data transfer to the UE, based on network triggers, and respond to requests from the UE. For 3GPP non-WiMAX access detailed functionality for ANDSF is defined in section 4.8.2 of TS 23.402 [4]. 3GPP ANDSF discovery shall be done as per section 4.8.4 of TS 23.402 [4]. For Wi-Fi® – WiMAX Single Radio handover detailed functionality of ANDSF is defined in [16].

After learning the WiMAX network parameters, the SR MS acquires the BSID of a target WiMAX BS in the WiMAX Radio Access Network, via its periodic scanning and measurement in the WiMAX mode.

The SR MS discovers WiMAX SFF as per procedure defined in section 7.1.

6.2.2 Phase 2: WiMAX® Session Pre-Registration

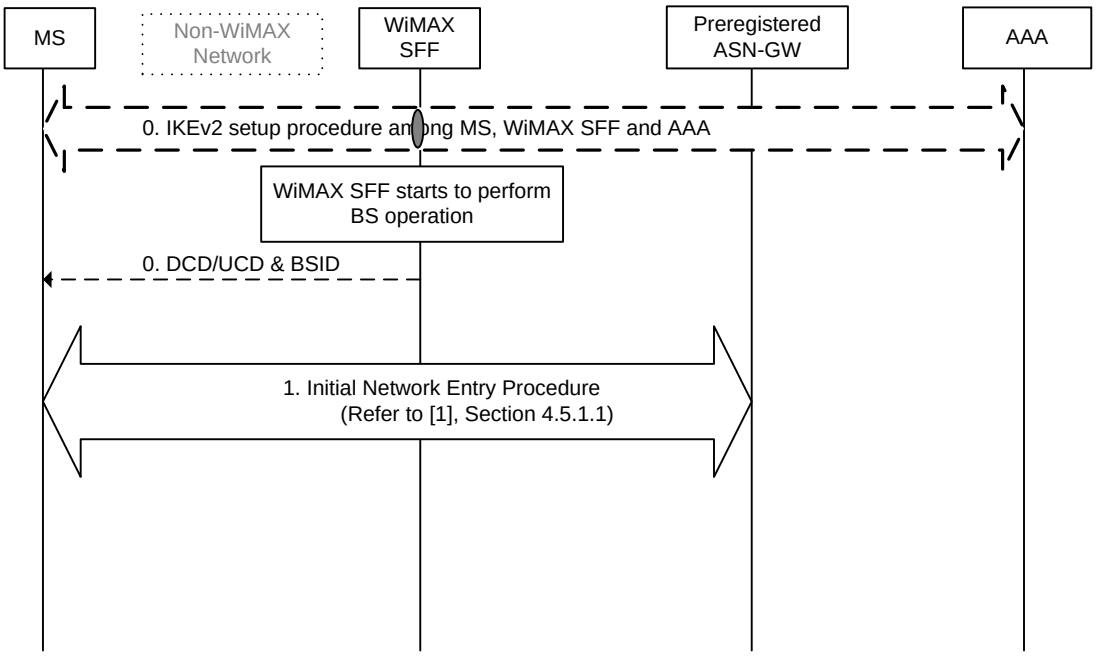


Figure 7-3 – Phase 2: WiMAX® Pre-Registration Procedure

STEP 0

The SR MS MAY initiate IKEv2 procedure with WiMAX SFF to setup a secure tunnel. The SR MS, WiMAX SFF and AAA perform EAP over IKEv2.

STEP 1

The SR MS completes Initial Network Entry (INE) procedures with the WiMAX® network via the WiMAX SFF while continuing to receive active service from the Non-WiMAX network. These procedures may optionally occur over the secure tunnel between the WiMAX SFF and MS if previously established in step 0. Details of INE procedure is defined in section 4.5.1.1 of [1].

Upon completion of WiMAX session pre-registration (i.e. ISF established), the SR MS enters Pseudo-Active mode. SR MS may remain in Pseudo-Active mode until the expiry of Pseudo-Active mode timer. The SR MS shall not start DHCP procedure to get the IP address. Also during initial network entry, the ASN-GW shall be made aware that it is connecting to WiMAX SFF so that it does not release the connection because the typical DHCP procedure is not invoked by the SR MS.

6.2.3 Phase 3: Single Radio Pseudo Mode Transition Phase

6.2.3.1 Phase 3a: Session Pre-registration using Pseudo-Idle mode entry procedure

The call flow shown in Figure 7-4 describes Psuedo Idle mode entry procedure initiated by SR MS and is part of Phase 3a.

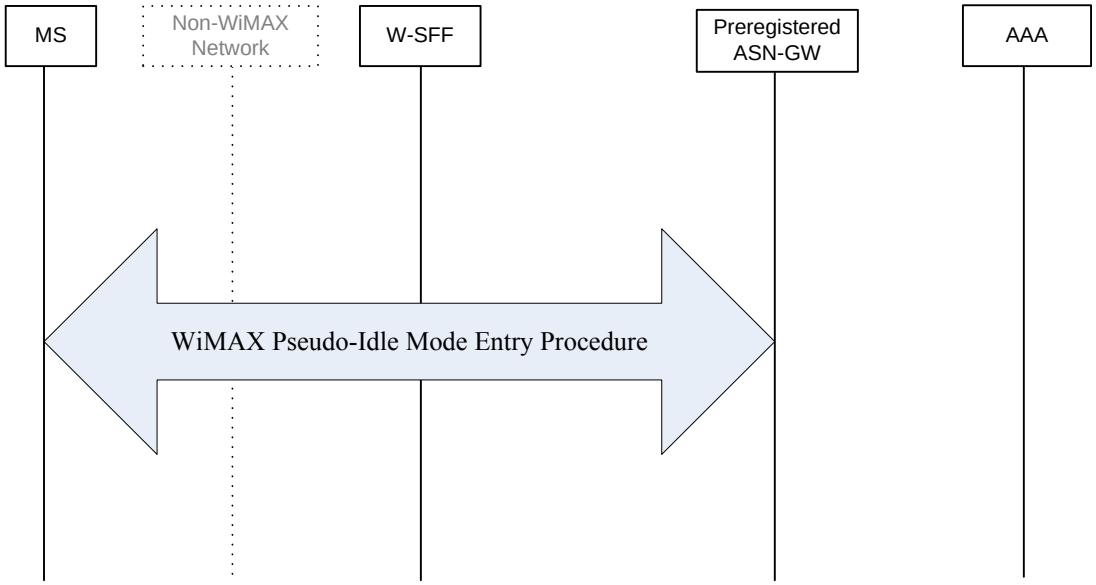


Figure 7-4 – Phase 3a: Pseudo-Idle mode entry procedure

Details of this procedure resemble the ones described in section 4.10.5.1 of [1].

6.2.3.2 Phase 3b: Pseudo-Active Mode Handover Initiation Procedure

The call flow shown in Figure 7-5 describes Pseudo-Active mode handover initiation procedure.

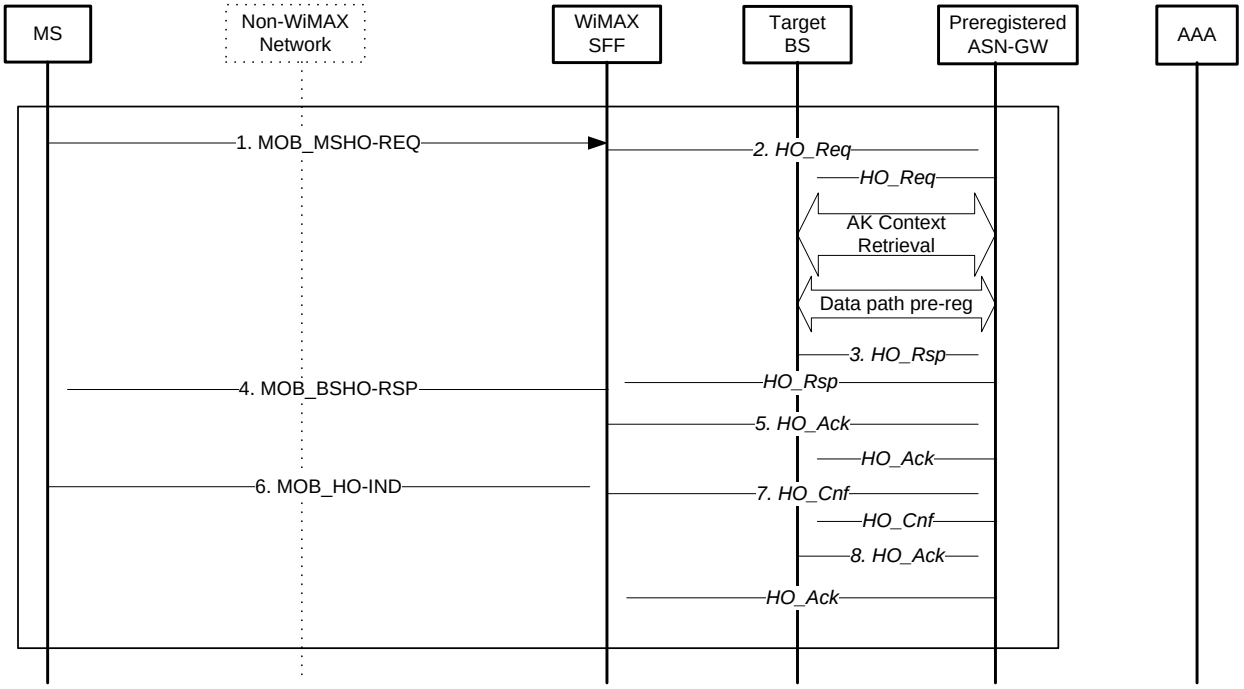


Figure 7-5 – Phase 3b: Pseudo-Active mode handover initiation procedure

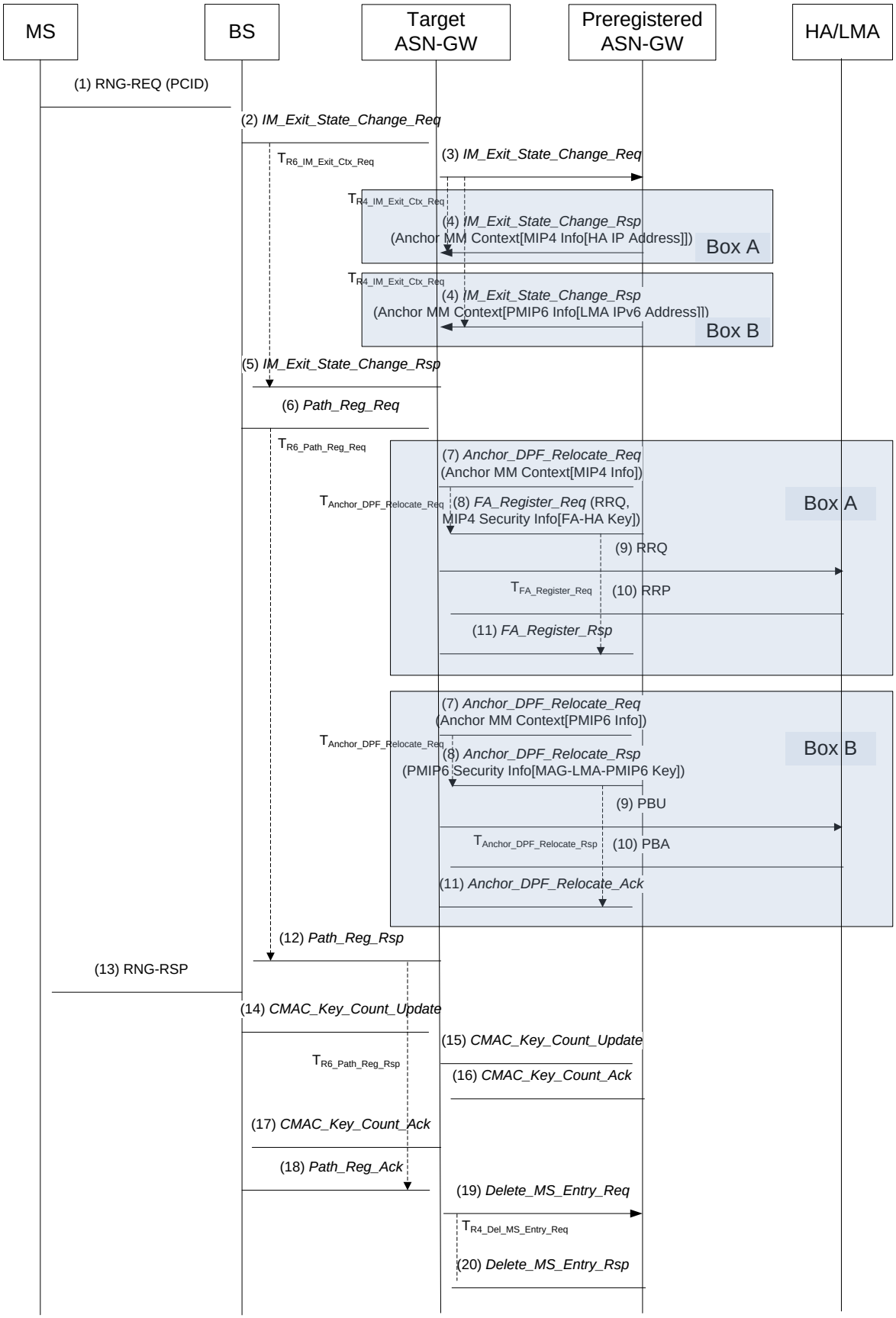
Details of steps 1 - 5 are described in section 4.7.2.1.2 of [1].

Details of steps 6 - 8 are described in section 4.7.2.2.2 of [1].

6.2.4 Phase 4: SR Handover Execution Phase

6.2.4.1 Phase 4a: Pseudo-Idle Mode Exit Procedure

This procedure is similar to that of Idle mode exit procedure since the WiMAX SFF stores the contexts of the Preregistered ASN-GW which hosts Paging Controller. Since the ASN-GW has the contexts of the SR MS, the SR MS performs Pseudo-Idle mode exit procedure as if it has performed the Idle mode entry procedure in the WiMAX network. When it attaches to the target BS, it sends the PCID which was received during the Pseudo-Idle mode entry procedure over the R9 tunnel. The PCID assigned during the Pseudo-Idle entry stage is located in the Preregistered ASN-GW.


MS
BS
Target ASN-GW
Preregistered ASN-GW
HA/LMA
(1) RNG-REQ (PCID)
(2) IM_Exit_State_Change_Req
T R6_IM_Exit_Ctx_Req
(3) IM_Exit_State_Change_Req
T R4_IM_Exit_Ctx_Req
(4) IM_Exit_State_Change_Rsp
(Anchor MM Context[MIP4 Info[HA IP Address]])
Box A
T R4_IM_Exit_Ctx_Req
(4) IM_Exit_State_Change_Rsp
(Anchor MM Context[PMIP6 Info[LMA IPv6 Address]])
Box B
(5) IM_Exit_State_Change_Rsp
(6) Path_Reg_Req
T R6_Path_Reg_Req
(7) Anchor_DPF_Relocate_Req
(Anchor MM Context[MIP4 Info])
T Anchor_DPF_Relocate_Req
(8) FA_Register_Req (RRQ,
MIP4 Security Info[FA-HA Key])
Box A
(9) RRQ
T FA_Register_Req
(10) RRP
(11) FA_Register_Rsp
(7) Anchor_DPF_Relocate_Req
(Anchor MM Context[PMIP6 Info])
T Anchor_DPF_Relocate_Req
(8) Anchor_DPF_Relocate_Rsp
(PMIP6 Security Info[MAG-LMA-PMIP6 Key])
Box B
(9) PBU
T Anchor_DPF_Relocate_Rsp
(10) PBA
(11) Anchor_DPF_Relocate_Ack
(12) Path_Reg_Rsp
(13) RNG-RSP
(14) CMAC_Key_Count_Update
(15) CMAC_Key_Count_Update
T R6_Path_Reg_Rsp
(16) CMAC_Key_Count_Ack
(17) CMAC_Key_Count_Ack
(18) Path_Reg_Ack
(19) Delete_MS_Entry_Req
T R4_Del_MS_Entry_Req
(20) Delete_MS_Entry_Rsp

1

Figure 7-6 – Phase 4a: Pseudo-Idle Mode Exit Procedure

Note: **Box A** and **Box B** procedures in Figure 7-6 refer to PMIP4 and PMIP6 cases respectively.

STEP 1

MS initiates exit procedure from Idle mode and sends RNG-REQ message as described in IEEE Std 802.16-2009 [15]. The Ranging Purpose Indication TLV Bit #0 is set to network reentry from Idle mode and PC ID TLV is included, thus indicating that the MS intends to Re-Entry from Idle mode.

STEP 2

On receiving the RNG-REQ message from MS indicating Idle mode exit, the BS sends R6 *IM_Exit_State_Change_Req* message to the Preregistered ASN-GW which hosts Paging Controller (PC). If the BS cannot reach the Anchor PC directly, the BS sends *IM_Exit_State_Change_Req* message to the Target ASN-GW. Timer $T_{R6\_IM\_Exit\_Ctx\_Req}$ is started.

STEP 3

The Target ASN-GW receives the R6 *IM_Exit_State_Change_Req* message from the BS indicating Idle mode exit and forwards R4 *IM_Exit_State_Change_Req* message to the Anchor PC, indicating that the MS wants to become active.

STEP 4

Anchor PC responds with R4 *IM_Exit_State_Change_Rsp* message to the Target ASN-GW. R4 *IM_Exit_State_Change_Rsp* message contains the stored information for the MS at the Anchor PC.

For PMIP4 and PMIP6, HA IP address and LMA IPv6 Address TLV are included, respectively.

STEP 5

The Target ASN-GW retrieves the MS context from the Anchor PC and forwards *IM_Exit_State_Change_Rsp* message over the R6 interface. Once the BS receives this message, Timer $T_{R6\_IM\_Exit\_Ctx\_Req}$ is stopped. The AK is fetched from the authenticator and is used to verify the RNG-REQ message.

STEP 6

After successful verification, the BS starts data path establishment. It sends R6 *Path_Req_Req* message to the DPF in the Target ASN-GW. Timer $T_{R6\_Path\_Reg\_Req}$ is started at this point by the BS.

STEP 7

The Target ASN-GW may send an *Anchor_DPF_Relocate_Req* message to the pre-registered ASN-GW hosting the Anchor Authenticator requesting a DPF relocation.

For PMIP4, the Target ASN-GW starts a timer $T_{Anchor\_DPF\_Relocate\_Req}$ for *FA_Register_Req* message. This message relays information about Target ASN-GW that is necessary in order to construct and send the MIP RRQ message in step 8. The message contains a CoA for the target FA and the target FA address if it is different from the CoA.

For PMIP6, the Target ASN-GW starts a timer $T_{Anchor\_DPF\_Relocate\_Req}$ for *Anchor_DPF_Relocate_Rsp* message. If in-band protocol security is enabled, the Target ASN-GW requests the necessary PMIP6 key information from the Authenticator by including the Context Purpose Indicator TLV (with bit #11 set).

STEP 8

For PMIP4, the Anchor Authenticator in the pre-registered ASN-GW starts the MIP registration with the target ASN-GW/FA by sending *FA_Register_Req* message. This message contains a fully formed Registration Request (RRQ) message with CoA field in the RRQ message set to the CoA of the Target FA which is received in *Anchor_DPF_Relocate_Req* message in step 7. The source address of the RRQ message is that of the MS and the destination address is the target CoA or the FA if the target FA address is different from the target CoA. In addition, *FA_Register_Req* message contains the FA-HA MIP key if this key is used. This message is sent to the Target ASN, whose address was identified as the source address of the *Anchor_DPF_Relocate_Req* message in step 7. A timer $T_{FA\_Reg\_Req}$ is started for *FA_Register_Rsp* message from the Target ASN-GW.

For PMIP6, if the Anchor Authenticator in the pre-registered ASN-GW grants the relocation request, the Anchor Authenticator derives and returns the requested MAG-LMA-PMIP6-Key (valid for the specific MAG, LMA and MN tr iplet o nly) in t he *Anchor_DPF_Relocate_Rsp* message t o t he Target A SN-GW/MAG. A t imer $T_{Anchor\_DPF\_Relocate\_Rsp}$ is started for *Anchor_DPF_Relocate_Ack* message from the Target ASN-GW.

STEP 9

For PMIP4, after receiving *FA_Register_Req* message, the Target ASN-GW/FA stops $T_{Anchor\_DPF\_Relocate\_Req}$ and relays the RRQ message to the HA.

For PMIP6, after receiving *Anchor_DPF_Relocate_Rsp*, the Target ASN-GW/MAG stops $T_{Anchor\_DPF\_Relocate\_Req}$ and sends a Proxy Binding Update (PBU) message to the LMA. If in-band protocol security is enabled, then the PBU message includes a valid MAG-LMA derivation in the MN-HA mobility message authentication option.

STEP 10

For PMIP4, the HA responds with the Registration Response (RRP) message to the Target ASN-GW/FA and creates the transport tunnel between itself and the Target ASN-GW/FA.

For PMIP6, the LMA responds with the Proxy Binding Acknowledgement (PBA) message to the Target ASN-GW/MAG and creates the transport tunnel between itself and the Target ASN-GW/MAG. If in-band signaling protection is enabled, PBA message includes the correct MN-HA mobility message authentication option.

STEP 11

For PMIP4, the Target ASN-GW relays the MIP RRP encapsulated in a *FA_Register_Rsp* message to the Anchor Authenticator in the pre-registered ASN-GW. The Anchor Authenticator updates the FA in its record and stops $T_{FA\_Reg\_Req}$. Upon receipt of the *FA_Register_Rsp* message, the PMIP4 Context at the Anchor Authenticator is updated with the new Registration Lifetime.

For PMIP6, upon receiving the PBA message, the Target ASN-GW/MAG sends an *Anchor_DPF_Relocate_Ack* message updating the Anchor Authenticator regarding the PBU registration status and stops $T_{Anchor\_DPF\_Relocate\_Rsp}$.

STEP 12

The DPF in the Target ASN-GW confirms data path establishment and sends *Path_Req_Rsp* message to the BS. Timer $T_{R6\_Path\_Reg\_Rsp}$ is started. Also, once the BS receives this message, Timer $T_{R6\_Path\_Reg\_Req}$ is stopped

STEP 13

The BS sends RNG-RSP message to the MS.

STEP 14-15

The BS sends *CMAC_Key_Count_Update* message to the Preregistered ASN-GW via the Target ASN-GW.

STEP 16-17

The Preregistered ASN-GW responds to the target BS by sending the *CMAC_Key_Count_Ack* message (via Target ASN-GW if Target ASN-GW and Preregistered ASN-GW are different)

STEP 18

The BS sends *Path_Reg_Ack* message to the Target ASN-GW.

STEP 19

When R6 *Path_Reg_Ack* is received at the Target ASN-GW it sends a R4 *Delete_MS_Entry_Req* message to Pre-Registered ASN-GW (hosting the Anchor PC) in order to delete the Idle mode entry associated with the MS. Timer $T_{R4\_Del\_MS\_Entry\_Req}$ is started at this point by the Target ASN-GW to monitor the response for this message. This step is optional if the Target ASN-GW and the Pre-Registered ASN-GW are co-located.

STEP 20

Upon the receiving *Delete_MS_Entry_Req*, the Pre-Registered ASN-GW (hosting the Anchor PC) sends *Delete_MS_Entry_Rsp* to the Target ASN-GW. Timer $T_{R4\_Del\_MS\_Entry\_Req}$ is stopped at the Target ASN-GW.

6.2.4.2 Phase 4b: Pseudo-Active mode SR Handover Execution Procedure

When the SR MS is in Pseudo-Active mode and decides to handover towards the BS, it performs the "SR Handover Action" procedure toward WiMAX. The procedure is similar to Handover Action scenario 1 described in section 4.7.2.2.2 of [1]. The only difference is that in this case Preregistered ASN-GW will trigger the Proxy Binding Update (PBU) anytime after a successful data path registration.

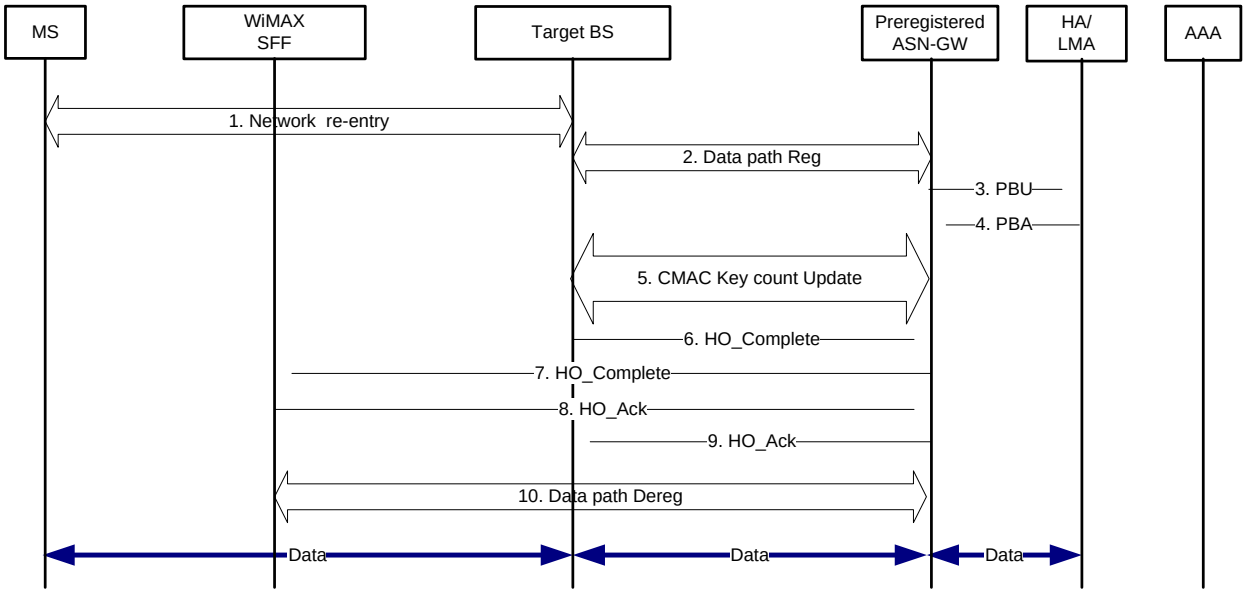


Figure 7-7 – Phase 4b: Pseudo-Active mode SR Handover Execution Procedure

6.3 WiMAX® Quick Re-Entry

While the WiMAX® network retains the MS context for a period of "Retain-Time" it is possible that the MS may attempt to re-enter the WiMAX network again without going through the Pre-registration stage (since context still exists). The procedure of an MS quickly entering the WiMAX network is described in Figure 7-8

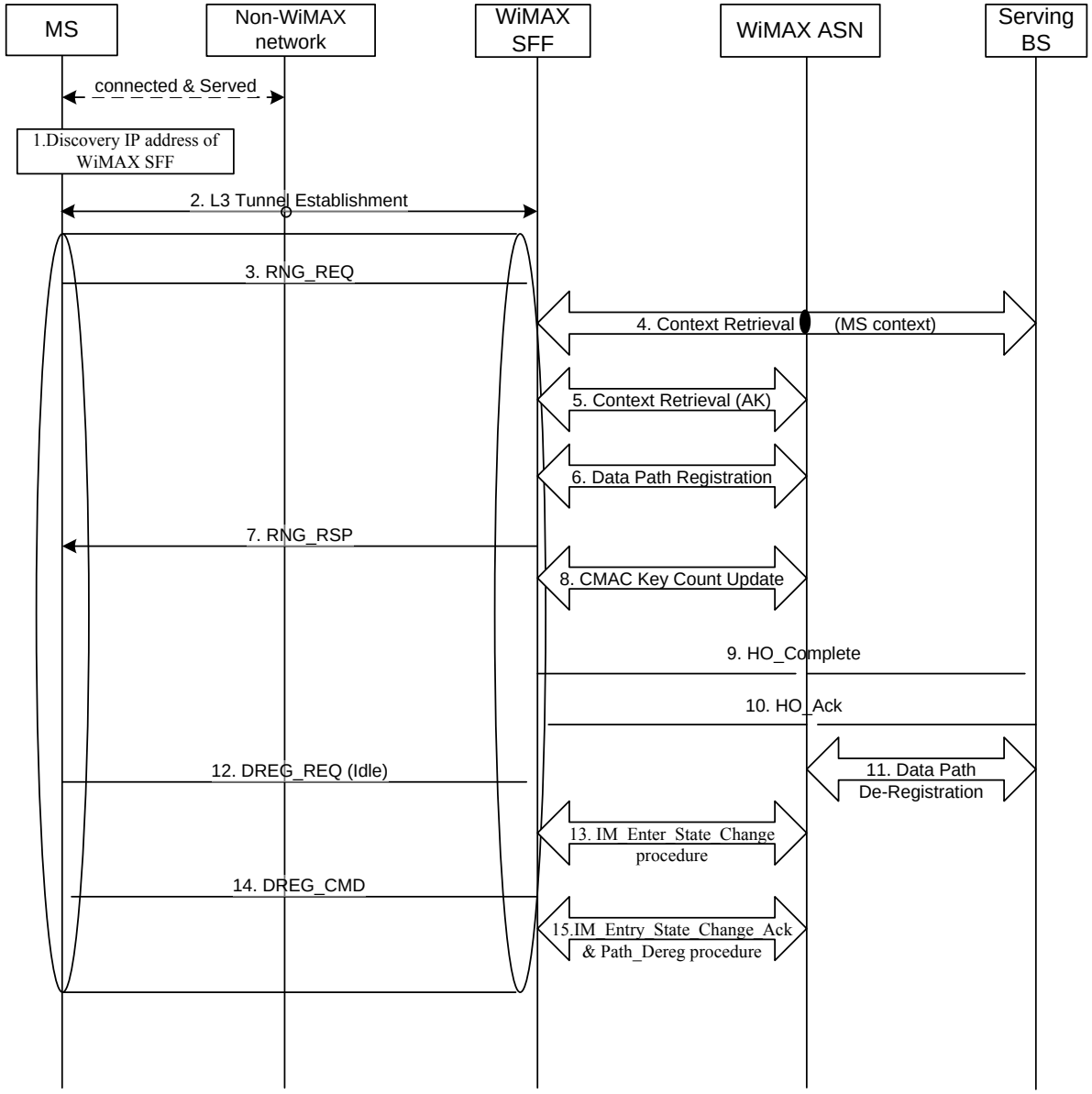


Figure 7-8 – SR WiMAX® Re-entry procedure

STEP 1

The MS discovers the IP address of a WiMAX® SFF.

STEP 2

The MS establishes an IP tunnel to the WiMAX® SFF. Once established, all of the WiMAX signaling between the MS and the WiMAX SFF are delivered through this WiMAX SFF tunnel. The WiMAX SFF may send a DCD message which includes the BSID of the WiMAX SFF to the MS via this WiMAX SFF tunnel

STEP 3

The MS sends a RNG_REQ message to the WiMAX SFF with reentry indication. It also indicates the last WiMAX serving BSID. If the MS knows the BSID of the WiMAX SFF, a new AK for the WiMAX SFF can be calculated by the MS. In this case, a HMAC/CMAC tuple shall be included in the RNG_REQ message. In case the MS doesn't know the BSID of the WiMAX SFF, the MS may send a RNG_REQ message without a HMAC/CMAC tuple and in the R9 header, set the B bit to '1', and include the old WiMAX serving BSID or alternatively a random BSID value. The WiMAX SFF shall respond with a RNG_RSP message rejecting such RNG_REQ and set the B bit to '1', and includes its own BSID value in the R9 header. Once the MS gets the BSID of the WiMAX SFF from the R9 header, the MS calculates the new AK and resends another RNG_REQ message to the WiMAX SFF which this time includes a HMAC/CMAC tuple. Please see section 8 for the detail of R9 protocol

STEP 4

The WiMAX SFF initiates a Context Request procedure with the last Serving BS to retrieve the context information for the MS. See section 4.12 of [1]for this procedure. The last Serving BS responds by sending the context information which includes the Anchor Authenticator ID and Anchor ASN-GW ID of the MS.

STEP 5

The WiMAX SFF requests AK context for the MS by initiating a Context Request procedure with the Authenticator ASN-GW of the MS. See section 4.12 of [1] for this procedure.

STEP 6

The WiMAX SFF initiates data path registration for the MS with the Anchor ASN-GW of the MS. See section 4.12 of [1] for this procedure.

STEP 7

The WiMAX SFF uses the Authenticator context to authenticate the MS message. The WiMAX SFF sends a RNG-RSP message to the MS.

STEP 8

The WiMAX SFF initiates a CMAC Key Count Update procedure with the Authenticator ASN-GW to update it with the latest CMAC Key Count. See section 4.12 of [1] for this procedure.

STEP 9

Upon completion, the WiMAX SFF SHALL send a *HO_Complete* message to the last serving BS to acknowledge the completion of the handover. Upon receipt of the *HO_Complete* message, the last Serving WiMAX BS releases the MS context.

STEP 10

The last Serving BS sends a HO_Ack message to the WiMAX SFF.

STEP 11

Upon completing the Data Path Registration procedure with the WiMAX SFF, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the last Serving BS. This step may occur any time after step 6. See section 4.12 of [1] for this procedure.

Upon receiving the HO_Complete message, if the last Serving BS still has a data path with Anchor ASN-GW, the last Serving BS initiates a Data Path De-Registration procedure with the Anchor ASN-GW.

For details of steps 3 to 11, refer to 4.7.3.1 of [1].

STEP 12-15

Based on operator policy and as described in section 5.4, the MS may transition to the WiMAX Pseudo-Idle mode through the WiMAX SFF tunnel. The procedure from step 13 to step 15 are the same as figure 4-161 in section 4.10.5.1 of [1]. Once the Pseudo-Idle mode entry is successful, the MS may periodically send location update (LU) message to maintain or reset the Pseudo-Idle mode timer.

6.4 SR MS Mode Transition Procedures

Single radio non-WiMAX® to WiMAX® inter-RAT handover includes network and SR MS support for three additional modes of service in addition to the existing WiMAX Active and Idle modes of service as described in section 5.3. The following section explains the procedures and triggers for mode transition -

1. **NULL Mode transition procedures:** If the SR MS initiates WiMAX pre-registration in NULL mode with the WiMAX network via the WiMAX SFF tunnel and the WiMAX network accepts the WiMAX pre-registration, the WiMAX SFF stores the SR MS's context and together, the WiMAX network and the SR MS transition from NULL to Pseudo-Active mode. If the WiMAX network rejects the SR MS pre-registration, then depending on the rejection cause (for e.g.: resources not available) the SR MS remains in NULL mode and may retry after some timer interval. If the pre-registration rejection cause indicates SR HO not supported, the SR MS SHALL remain in NULL mode. If upon completion of a WiMAX pre-registration the WiMAX network requires the SR MS to immediately complete a SR inter-RAT HO, the network SHALL set the Pseudo-Active mode timer to zero.

2. **Pseudo-Active Mode Transition procedures:** The WiMAX SFF starts a Pseudo-Active mode timer upon SR MS entry into Pseudo-Active mode. The SR MS may perform one of the following actions while in Pseudo-Active mode -

    a. The SR MS may initiate inter-RAT handover at any time during Pseudo-Active mode by completing WiMAX MS initiated handover procedures over the air with a target WiMAX BS as per section 4.7.2.2.2 of [1]. If the inter-RAT handover request is accepted by the WiMAX network, the SR MS transitions from Pseudo-Active mode to Active mode. If, for any reason, the inter-RAT handover is rejected, the SR MS SHALL remain in the Pseudo-Active mode and may retry inter-RAT handover after some time interval.

    b. The SR MS may also initiate Pseudo-Idle mode entry via the WiMAX SFF. If the MS initiated Pseudo-Idle mode entry is accepted by the network, the SR MS transitions from Pseudo-Active mode to Pseudo-Idle mode. If, for any reason, the Pseudo-Idle mode entry is rejected by the WiMAX network, the SR MS SHALL remain in the Pseudo-Active mode.

    Upon expiry of the Pseudo-Active mode timer, the WiMAX SFF and SR MS SHALL complete one of the following procedures:

    a. The WiMAX network through the WiMAX SFF tunnel requests the SR MS to complete inter-RAT handover by triggering a network initiated inter-RAT handover. This is accomplished by sending a MOB_BSHO-REQ message via the WiMAX SFF tunnel to the SR MS. If the SR MS agrees to perform an inter-RAT handover to the WiMAX network, it completes network initiated handover procedures via over the air signaling procedures with a WiMAX target BS as per section 4.7.2.1.5 of [1]. If the SR MS rejects the WiMAX network initiated inter-RAT handover by sending a HO-IND message, the WiMAX SFF may subsequently request the SR MS to enter Pseudo-Idle mode if the network supports an alternate option. If the SR MS rejects the inter-RAT handover (MOB_BSHO-REQ) request and an alternate option is not supported, the WiMAX SFF SHALL send a session release indication to the SR MS via the WiMAX SFF tunnel and release the WiMAX SFF context created during session pre-registration. The WiMAX SFF releases the resources allocated to the SR MS for Pseudo-Active mode support. The session release notification (e.g. DREG) serves to notify the SR MS that its pre-registered context has been released from the WiMAX network. The SR MS SHALL then transition to a NULL mode.

    Note: The SR MS may reject network initiated inter-RAT handover by requesting Pseudo-Idle mode entry instead (e.g. DREG). The WiMAX network may accept or reject the SR MS request.

b. The WiMAX network through the WiMAX SFF tunnel requests the SR MS to enter a Pseudo-Idle mode by triggering a network initiated Idle-mode entry procedure via the WiMAX SFF tunnel to the SR MS as per section 4.10.5.1 of [1]. If the SR MS agrees to transition to Pseudo-Idle mode, the WiMAX SFF SHALL start the Pseudo-Idle mode timer. If the SR MS rejects the Pseudo-Idle mode entry request, the WiMAX network may subsequently request the SR MS to complete inter-RAT handover to the WiMAX network if it supports an alternate option. If the SR MS rejects Pseudo-Idle mode entry and an alternate option is not supported, the WiMAX network SHALL send a session release indication to the SR MS via the WiMAX SFF tunnel and releases the WiMAX SFF context created during session pre-registration. The WiMAX network releases resources allocated to the SR MS for Pseudo-Active mode support. The session release notification (e.g. DREG) serves to notify the SR MS that its pre-registered context is being released from the WiMAX network. The WiMAX network SHALL then transition the SR MS to the NULL mode.

c. The WiMAX network sends a session release indication (e.g. DREG) to the SR MS via the WiMAX SFF tunnel and releases WiMAX SFF context created during session pre-registration and all WiMAX resources allocated to the SR MS for Pseudo-Active mode support. The session release notification serves to notify the SR MS that its pre-registered context has been released from the WiMAX network. The WiMAX network and SR MS SHALL then transition to a NULL mode.

3. **Transition from Pseudo-Idle Mode:** Upon successful transition to a Pseudo-Idle mode the WiMAX SFF SHALL start the Pseudo-Idle mode timer. If the SR MS sends a Location Update (LU) via the WiMAX SFF tunnel to the WiMAX network, the WiMAX SFF MAY reset the Pseudo-Idle mode timer. The SR MS may initiate inter-RAT handover to the WiMAX network from Pseudo-Idle mode at any time by sending a RNG_REQ over the air to a WiMAX Target BS. If the WiMAX network accepts the inter-RAT handover request from the SR MS, the WiMAX network and SR MS transition from Pseudo-Idle mode to Active mode. If for any reason the inter-RAT handover is rejected, the SR MS may remain in the Pseudo-Idle mode. Upon expiry of the Pseudo-Idle mode timer, the WiMAX network and SR MS SHALL complete one of the following procedures:

a. The WiMAX SFF requests the SR MS to complete inter-RAT handover by initiating a network initiated Pseudo-Idle mode exit procedure via the WiMAX SFF tunnel to the SR MS. If the SR MS agrees to inter-RAT handover into the WiMAX network, it completes the Pseudo-Idle mode exit procedure via over the air signaling with a WiMAX Target BS. If the SR MS rejects the WiMAX WiMAX SFF initiated Pseudo-Idle mode exit request by sending DREG-REQ, the WiMAX SFF SHALL send a session release indication to the SR MS via the WiMAX SFF tunnel and release WiMAX SFF context created during session pre-registration and all the WiMAX resources allocated to the SR MS for Pseudo-Idle mode support. The session release notification serves to notify the SR MS that its pre-registered context has been released from the WiMAX network. The SR MS SHALL then transition to a NULL mode.

b. The WiMAX network sends a session release indication to the SR MS via the WiMAX SFF tunnel and releases the WiMAX SFF context created during the pre-registration session and all the WiMAX resources allocated to the SR MS for Pseudo-Idle mode support. The session release notification serves to notify the SR MS that its pre-registered context has been released from the WiMAX network. The WiMAX network and the SR MS SHALL then transition to the NULL mode.

The following additional procedure is supported for Transition from Active Mode to Pseudo-Active Mode in case of a SR HO from WiMAX to a non-WiMAX network:

Immediately after a SR MS completes a handover to a non-WiMAX network, the MS may enter a Pseudo-Active mode without going through the pre-registration procedure. This can be accomplished after the MS initiates a context transfer from the old serving BS to a WiMAX SFF via an established tunnel between the SR MS and the WiMAX SFF. If the WiMAX SFF agrees to save the MS context for a configurable “Retain Time”, then during this time period, the MS can transition from an Active mode to a Pseudo Active mode. If the WiMAX SFF rejects the request, the SR MS SHALL transit to the NULL mode.

Figure 7-9 below illustrates the SR MS mode selection and its transition diagram while operating in a non-WiMAX network.

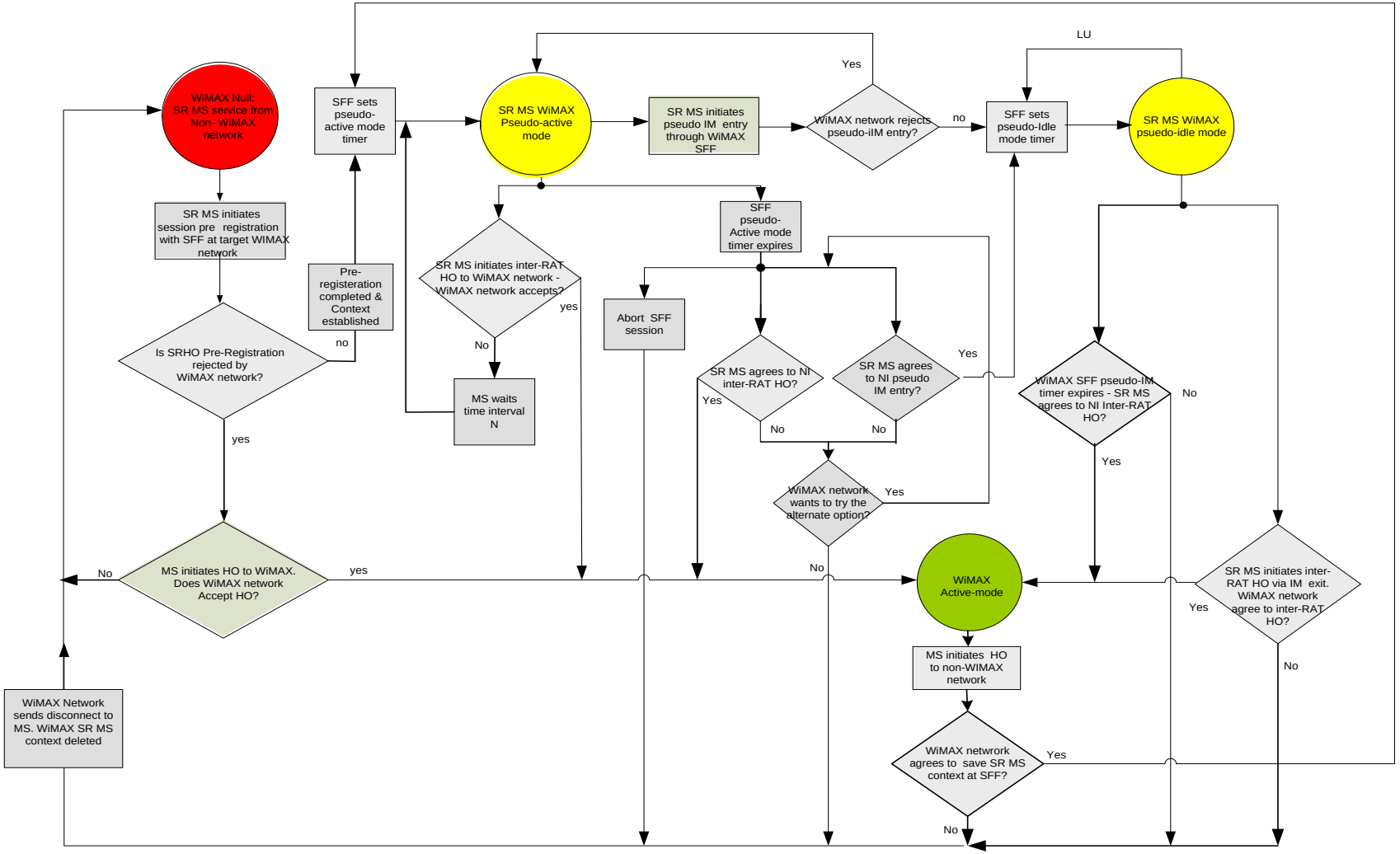


Figure 7-9 – SR MS mode selection and transition

7 Message Format

7.1 R9: UE/MS – WiMAX® SFF Messages

R9 runs over IP/UDP. Figure 8-1 shows the Protocol Stack between MS and WiMAX SFF

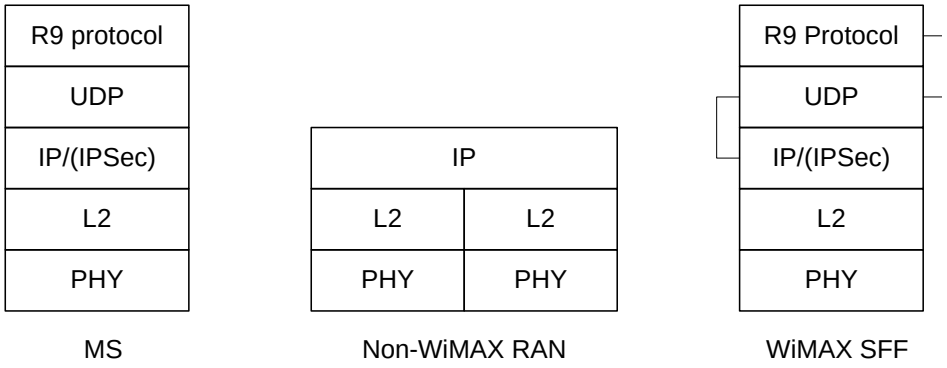


Figure 8-1 – Protocol Stack between MS and WiMAX SFF

Table 8-1 defines the R9 protocol header and the message fields.

Table 8-1 – R9 Protocol Header

Octets	Bits 8	7	6	5	4	3	2	1
1	Reserved						B	MTI
2-7	MSID							
8-13	BSID							
14-*n*	802.16-2009 MAC PDU/R9 Control Message							

MTI (Message Type Indicator): This bit indicates the type of Message."0" indicates it is R9 Control Message, "1" indicates Encapsulated 802.16-2009 MAC Message. MTI is defined in Table 8-2

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

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

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

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

802.16-2009MAC PDU: If MTI is "1", Octet 14 through *n* (where n>14) contains Encapsulated 802.16-2009 MAC PDU. MAC PDUs are packed as specified in 802.16-2009 [15].

R9 Control Message: If MTI is "0", Octet 14 through *n* (where n>14) contains R9 Control Message.

Table 8-2 – MTI (Message Type Indicator) Value

MTI (Binary)	Meaning
0	**R9 Control Message**
1	**Encapsulated 802.16-2009 MAC PDU**

Table 8-3 – R9 Control Message Format (MTI=0)

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

Table 8-4 – Message Type (For MTI = 0)

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

Note: For R9 ERR_DLVRY message sent to the SR MS, Message Type Octet 16 of R9 indicates the cause value as defined in Table 8-5.

If MTI = 1, octet 14 through *n* (where n>14) contains Encapsulated 802.16-2009 MAC PDU. In this case Message Type value is as specified in Table 37 of 802.16-2009 specification [15].

Table 8-5 – Cause Values

Cause Value	Meaning	Notes
01H	System failure	This value shall only be used in the Error Notification message sent by the WiMAX SFF.
02H	SFF Rediscovery Required	This value shall be used when the WiMAX SFF is overloaded, going through maintenance or taken out of service by the network.
All Others	Reserved	

7.2 R6: WiMAX® SFF – ASN-Gateway Messages

As explained in section 7.2.2, during initial network entry, the ASN-GW shall be made aware that it is connecting to WiMAX SFF. As part of the *MS_Preatachement_Req,* the WiMAX SFF sends an "R6_Attachment_Type" TLV to inform the pre-registered ASN-GW that it is attaching to an MS via a WiMAX SFF. If the pre-registered ASN-GW receives *MS_Preattachment_Req* with R6_Attachment_Type set to "Attached with WiMAX SFF", it does not release the R6 connection after an ISF is established and a typical DHCP procedure is not invoked by the SR MS. If the ASN-GW doesn't receive R6_Attachment_Type, it assumes attachment with a normal (non-SFF) BS.

Table 4-42[2] – MS_PreAttachment_Req from BS to Authenticator

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier
R6_Attachment_Type	5.3.2.xxx	O	Informs ASN-GW if R6 attachment is with BS or WiMAX SFF. Note: R6_Attachment_Type must be included by the WiMAX SFF.
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>MS Security History	5.3.2.108	M	
>>Authorization Policy Support	5.3.2.21	M	Identifies the MS authorization policy.
>SBC Context	5.3.2.174	O	802.16e related MS session context.
>>Subscriber Transition Gaps	5.3.2.316	O	
>>Maximum Transmit Power	5.3.2.317	O	
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	O	
>>PKM Flow Control	5.3.2.319	O	
>>Maximum Number of Supported Security Associations	5.3.2.320	O	
>>Security Negotiation Parameters	5.3.2.321	O	

[2] Table 4-42 is reproduced from [1] with the additional IEs defined in this specification contained in unshaded rows

IE	Reference	M/O	Notes
>>Extended Subheader Capability	5.3.2.325	O	
>>HO Trigger Metric Support	5.3.2.326	O	
>>Current Transmit Power	5.3.2.327	O	
>>OFDMA SS FFT Sizes	5.3.2.328	O	
>>OFDMA SS demodulator	5.3.2.329	O	
>>OFDMA SS modulator	5.3.2.330	O	
>>The number of UL HARQ Channel	5.3.2.331	O	
>>OFDMA SS Permutation support	5.3.2.332	O	
>>OFDMA SS CINR Measurement Capability	5.3.2.333	O	
>>The number of DL HARQ Channels	5.3.2.334	O	
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	O	
>>OFDMA SS Uplink Power Control Support	5.3.2.336	O	
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	O	
>>OFDMA MAP Capability	5.3.2.338	O	
>>Uplink Control Channel Support	5.3.2.339	O	
>>OFDMA MS CSIT Capability	5.3.2.340	O	
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O	
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	O	
>>OFDMA SS modulator for MIMO Support	5.3.2.343	O	
>>OFDMA Parameters Sets	5.3.2.50	O	
>>MS MAC Version	5.3.2.106	M	MS reported MAC Version. If the reported MAC Version is lower than 7 or is not present and the home NSP domain in the form of NAI provided by the MS does not correspond to NSP configured in the network, the MS is not supporting ND&S and SHALL be connected to a default NSP-ID, (i.e. a default NSP-ID is pre-configured by the NAP in the NAS – ASN-GW).
BS Info	5.3.2.26	M	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	M	Serving BS ID.

IE	Reference	M/O	Notes
>BS Location	5.3.2.425	O	Location info of the serving BS which may be described as Lat/Long/Sector/Carrier information of BS. NAS may pass this info to H-AAA which can use it to authorize stationary access services.

During SR Handover Action Procedure (using Pseudo-Idle mode exit procedure), the pre-registered ASN-GW MUST inform its R6_Attachment_Type to target ASN-GW. In turn, the target ASN-GW SHALL initiate PBU/RRQ towards the LMA/HA.

Table 4-174[3] – IM_Exit_State_Change_Rsp over R4

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.
R6_Attachment_Type	5.3.2.xxx	O	Informs target ASN-GW if R6 attachment is with BS or WiMAX SFF. Note: R6_Attachment_Type must be included by the preregistered ASN-GW.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.
>AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence, EIK.
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	
>>AK SN	5.3.2.9	M	
>>CMAC_KEY_COUNT	5.3.2.34	M	
MS Info	5.3.2.103	M	
>SBC Context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005.
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	C-M	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation

[3] Table 4-174 is reproduced from [1] with the additional IEs defined in this specification contained in unshaded rows

IE	Reference	M/O	Notes
			parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>REG context	5.3.2.144	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is

IE	Reference	M/O	Notes
			included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>Authenticator ID	5.3.2.19	M	Anchor Authenticator of the MS.
>SF Info	5.3.2.185	O	
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
>>Direction	5.3.2.59	M	
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE Std 802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	

IE	Reference	M/O	Notes
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.
>>>Classification Rule Priority	5.3.2.32	CM	
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic	5.3.2.92	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
Rate			
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	

IE	Reference	M/O	Notes
>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
> Anchor ASN GW ID	5.3.2.10	M	Anchor DPF/FA of the MS.
> SA Descriptor (one or more)	5.3.2.170	O	Included in this message by the BS (if cached a priori by that BS) and is in response to bits set in the Idle mode retain information TLV received from the MS.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK

IE	Reference	M/O	Notes
			Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
Paging Information	5.3.2.119	M	
>IDLE Mode Retain Info	5.3.2.81	M	IDLE Mode Retain Info.
Refresh IP address trigger	5.3.2.375	O	Included for the BS to trigger IP address refresh on the MS via HO Process Optimization TLV Bit #13. Currently used only for Simple IP re-anchoring.

1

2 5.3.2.xxx R6_Attachment_Type

Type	600
Length in octets	1
Value	Bitmap. The values are: • 0x01 = Attached with WiMAX® SFF All other values are Reserved.
Description	R6_Attachment_Type must be set by WiMAX SFF in MS_preattachment_Req message and by preregistered ASN-GW in IM_Exit_State_Change_Rsp over R4 message. All reserved values should be treated as attachment with the BS.
Parent TLV(s)	None

3

Appendix A: Access Specific Aspects

A.1 Single Radio interworking from WiMAX® to Wi-Fi®

WiMAX® to Wi-Fi® single radio interworking architecture and handover call flows are described in WiMAX-Wi-Fi interworking specification [16].

A.2 Single Radio interworking from WiMAX® to 3GPP2 (HRPD)

WiMAX to 3GPP2 (HRPD) single radio interworking architecture and handover call flows are described in X.S0058 [9].

A.3 Single Radio interworking from WiMAX® to 3GPP (E-UTRAN & Pre-Release 8 3GPP Networks)

Note: The Single Radio scenario of the WiMAX network interworking with Release 8 UTRAN/GERAN connected to an EPC core is not covered in this version of this specification.

A.3.1 Single Radio Interworking with 3GPP E-UTRAN access system

This section defines the Network Reference Model Single Radio Interworking of the Mobile WiMAX system with E-UTRAN Access Networks.

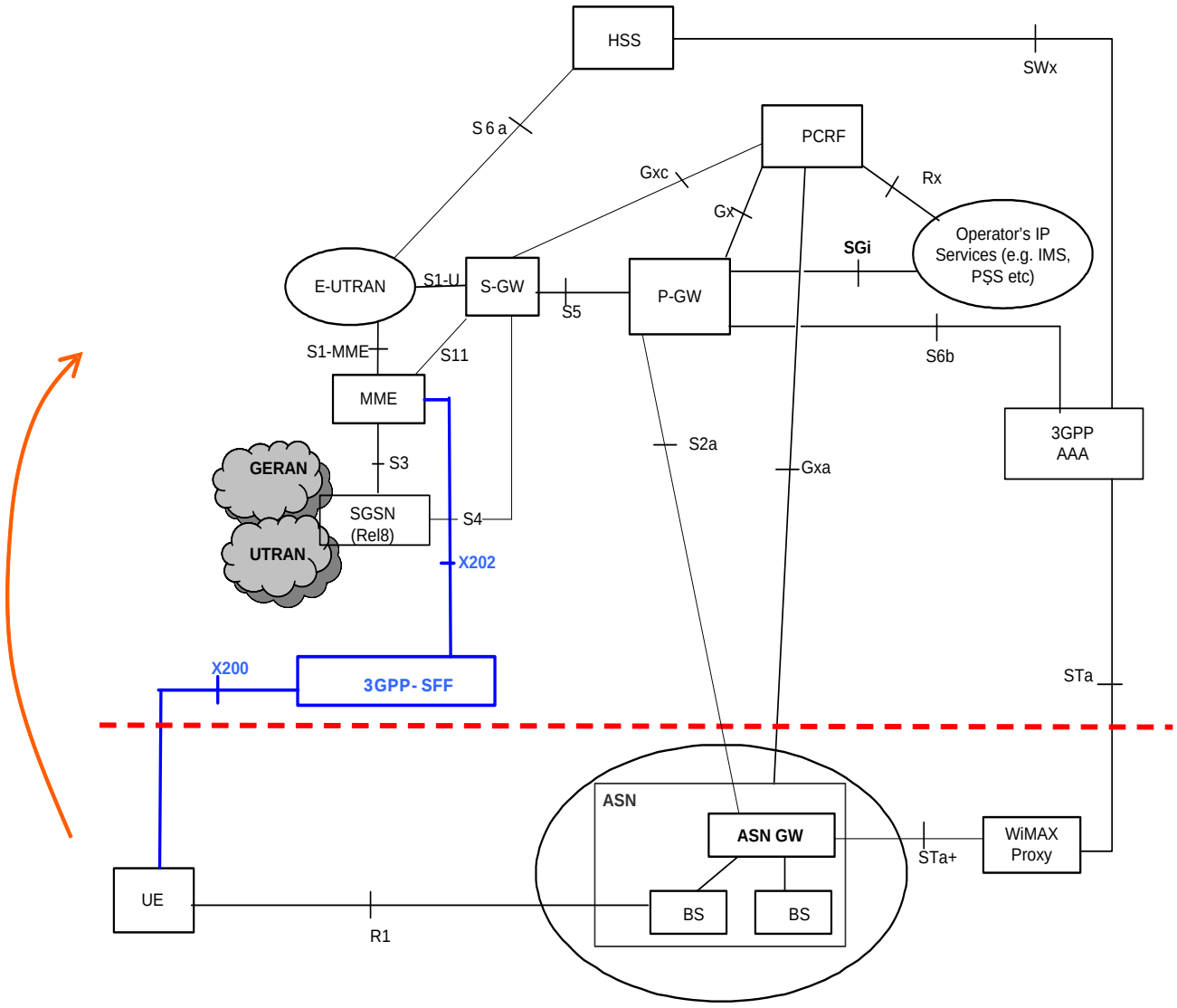


Figure A-1 – WiMAX® Single Radio Interworking Architecture (WiMAX to E-UTRAN Handover)

A.3.2 Single Radio Interworking with 3GPP Pre-Release 8 access systems

This section defines the Network Reference Model Single Radio Interworking of the Mobile WiMAX system with Pre-Release 8 3GPP Access Networks.

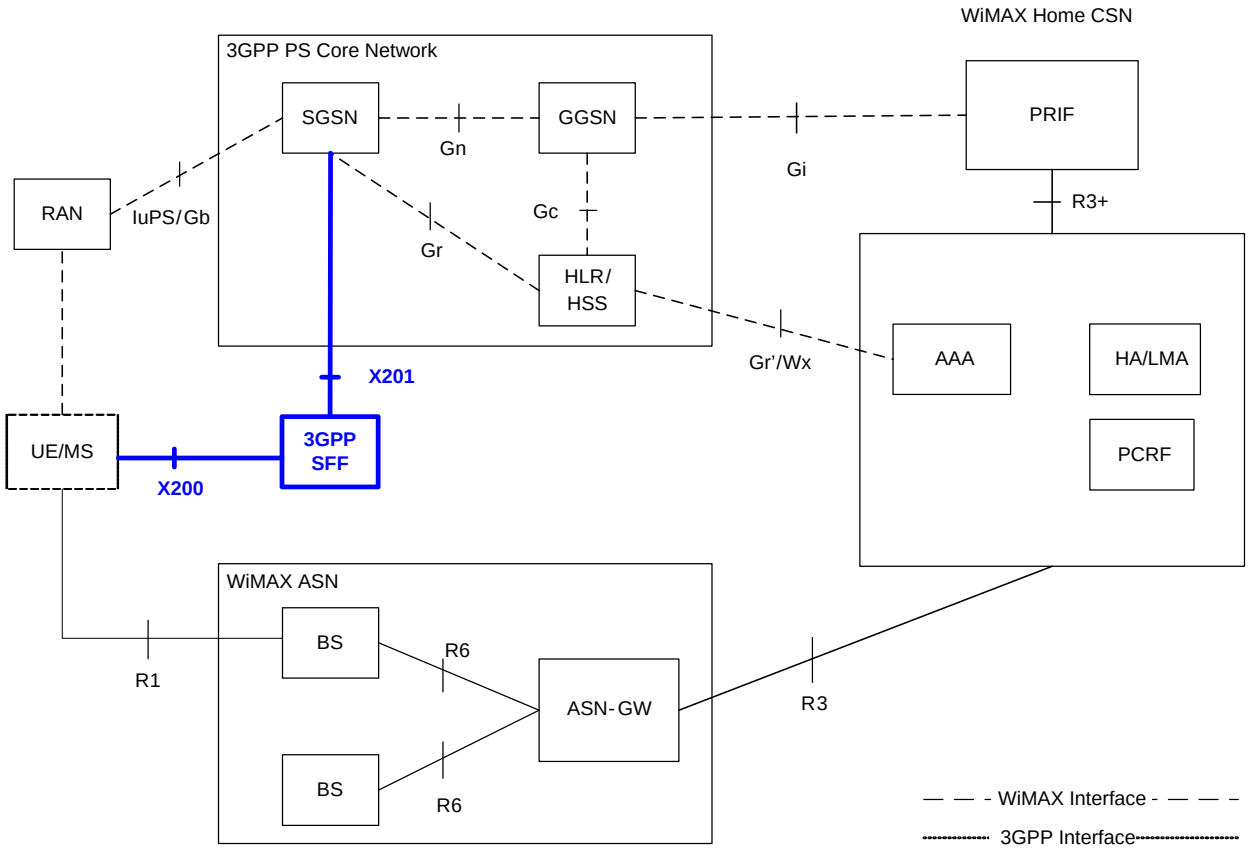


Figure A-2 – WiMAX® Single Radio Interworking Architecture (WiMAX to Pre-Release 8 3GPP Network access Handover)

A.3.3 Functional Elements

A.3.3.1 3GPP SFF

3GPP Signaling Forwarding Function (3GPP SFF) is a new functional element to support Single Radio handovers from WiMAX IP Access Network to E-UTRAN and Pre-Release 8 3GPP access networks. The 3GPP SFF supports layer 3 tunneling. The UE/MS communicates with the 3GPP SFF over the WiMAX Access Network in order to pre-register and execute the handover from the WiMAX Access Network to the E-UTRAN and Pre-Release 8 3GPP access network.

The 3GPP SFF facilitates pre-registration and authentication while the UE/MS is connected through the WiMAX Access Network prior to an active handover to the E-UTRAN and Pre-Release8 3GPP access networks.

For Single Radio Handover to Release 8 or later 3GPP networks, 3GPP SFF emulates functionality of eNodeB and connects to target MME (E-UTRAN HO) via the X202 Reference Point.

For Single Radio Handover to Pre-Release 8 3GPP access, the 3GPP SFF emulates the functionality of a RNC and connects to a target SGSN (GERAN/UTRAN HO) via the X201 reference point. 3GPP SFF may be co-located with SGSN and in this case X201 reference point is not exposed.

A.3.4 Reference Points

X200: This reference point supports secure communication between the UE and the 3GPP SFF through the mobile WiMAX IP access. It is used for pre-registration and for requesting resource preparation in the target 3GPP access network.

X201: When the 3GPP SFF emulates a RNC, this reference point has the same functionality as the Iu-PS/Gb (described in TS 23.060 [20]) and terminates at target SGSN. This reference point is not needed in case the 3GPP SFF act as a SGSN when co-located with the SGSN.

X202: This reference point has the same functionality as the S1-MME (described in TS 23.401 [3]) and terminates at MME.

A.3.5 3GPP SFF Discovery

Figure A-3 illustrates an example call flow for the discovery of the 3GPP SFF.

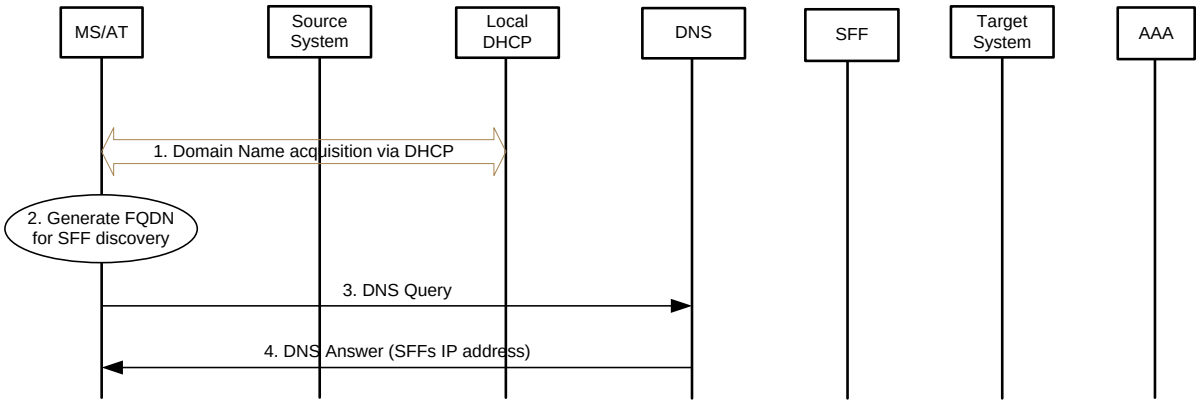


Figure A-3 – 3GPP SFF Discovery

4. The UE/MS acquires the domain name via DHCP message exchange. The DHCP procedure is done as in [11]
5. The UE/MS generates the FQDN for the 3GPP SFF with the domain name acquired in step 1. FQDN is generated as below:

   <3GPP-eNBID>.3GPP.SFF.<domain name>

6. The UE/MS sends a DNS query to the DNS Server including the FQDN.
7. The DNS server responds with a DNS answer including the 3GPP SFF's IP address.

A.3.6 WiMAX® to E-UTRAN Single Radio Handover procedure

This section describes Single Radio inter-RAT handover support from WiMAX network to 3GPP E-UTRAN access network.

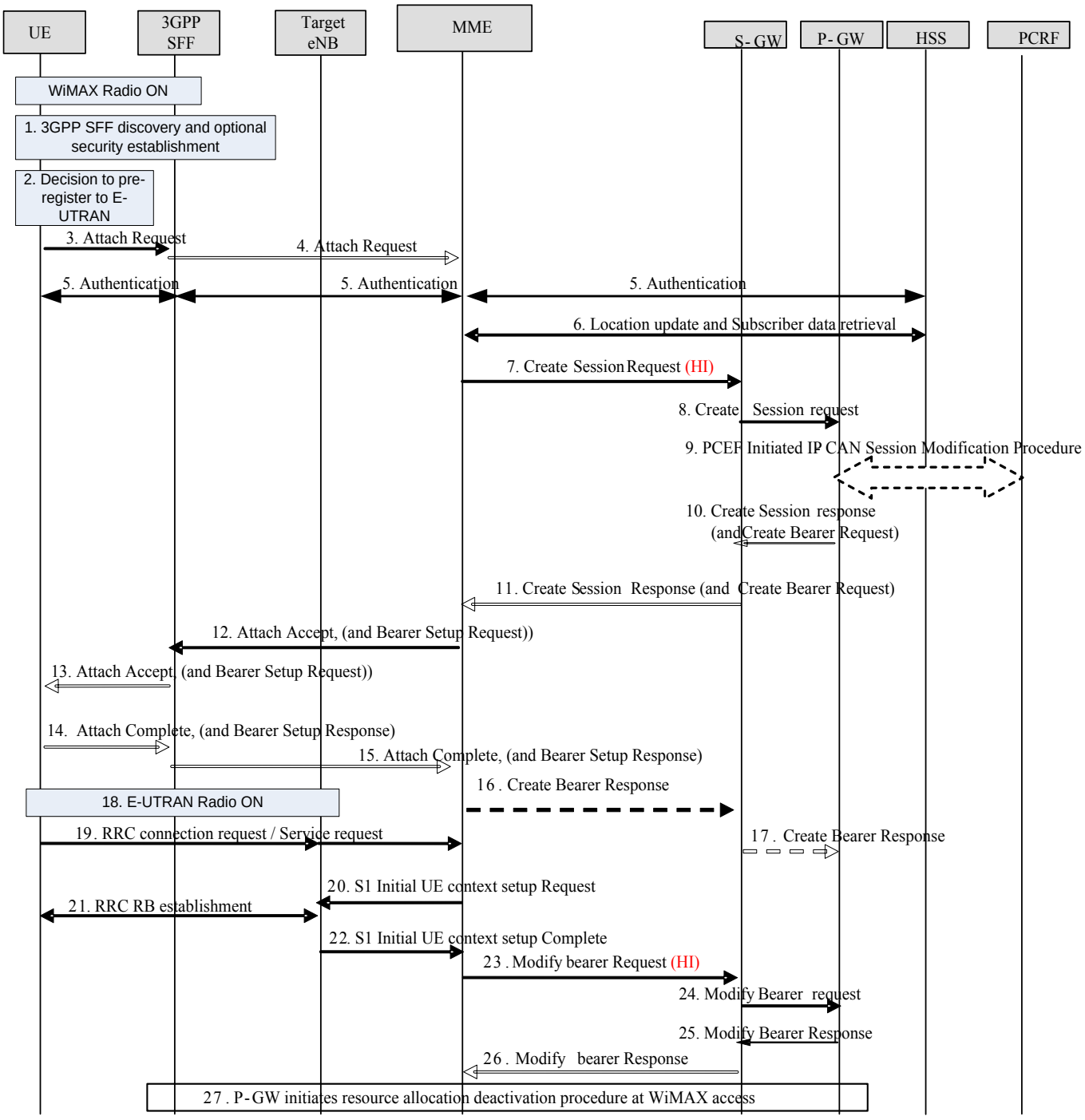


Figure A-4 – WiMAX® to E-UTRAN Single Radio Handover

1. The UE is registered with WiMAX and may have an ongoing data session established over WiMAX access. UE discovers the 3GPP SFF using 3GPP SFF discovery procedure as described in section A.3.5 .

   UE may optionally establish a secure IPSec tunnel with 3GPP SFF.

2. UE makes decision to pre-register to E-UTRAN.

3. The UE initiates the Attach procedure by transmission of a NAS Attach Request message over UE-3GPP SFF tunnel. Attach request may be encapsulated in Access Stratum message (e.g. RRC)

4. When receiving the attach message the 3GPP SFF selects an MME as per MME Selection procedure defined in TS 23.401[3].

5. If no UE context for the UE exists anywhere in the network, authentication must be performed. If UE was unknown to the target MME and the old MME, target MME will send an Identity Request to request the UE's IMSI prior to step 5. PDN GW identity is sent from HSS to MME in this step. These messages are tunnelled to/from the UE via the 3GPP SFF tunnelling mechanism.

6. If the MME has changed since the last detach, or if it is the very first attach, the MME sends an Update Location to the HSS. The HSS acknowledges the Update Location message by sending an Update Location Ack (IMSI, Subscription data) message to the MME.

7. The MME selects a Serving GW as described in TS 23.401 [3] and sends a Create Session Request (Handover Indication) message to the selected Serving GW. Since the Attach Type is "Handover" Attach, a Handover Indication parameter is included.

8. The Serving GW creates a new entry in its EPS Bearer table and sends a Create Session Request message (Handover Indication) to the PDN GW. Since the MME includes Handover Indication information in Create Session Request message, the Serving GW includes this information in Create Session Request message.

   Since Handover Indication is included, the PDN GW should not switch the tunnel from WiMAX IP access to 3GPP access system at this point.

9. Since Handover Indication is included, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [17] to obtain any new QoS policy and charging rules for all the active sessions as a result of the handover procedure.

   Since Handover Indication is included in step 7, the PDN GW stores the new PCC Rules for E-UTRAN access as well as the old PCC Rules for the Trusted or Untrusted Non-3GPP IP access and still applies the old PCC Rules for charging.

10. The PDN GW responds with a Create Session Response message to the Serving GW as described in TS 23.401 [3].The Create Session Response contains the IP address or the prefix that was assigned to the UE while it was connected to the WiMAX IP access.

11. The Serving GW returns a Create Session Response message to the new MME. The Create Bearer Request message may be sent together with the Create Session Response message.

12. Upon receiving the Create Session Response message, the MME sends an Attach Accept message (and the Bearer Setup Request message if Create Bearer Request message was received) to the UE over the X200 interface.

13. The 3GPP SFF forwards the Attach Accept (and the Bearer Setup Request message) to the UE.

14. The UE sends the Attach Complete message (and the Bearer Setup Response message) to the 3GPP SFF.

15. The 3GPP SFF forwards the Attach Complete message (and the Bearer Setup Response message) to the MME.

16. If Create Bearer Request message was sent by the Serving GW in step 11, the MME sends a Create Bearer Response message to Serving GW.

17. If Create Bearer Request message was sent by the PDN GW in step 10, the Serving GW sends a Create Bearer Response message to PDN GW.

18. Upon completion of the E-UTRAN Attach procedure, UE switches over to EUTRAN.

19. UE performs the NAS service request procedure. The UE sends NAS message Service Request towards the MME encapsulated in an RRC message to the eNodeB. The RRC message(s) that can be used to carry this NAS message are described in TS 36.300 [18]. The eNodeB forwards the NAS Service request message to MME. NAS message is encapsulated in an S1-AP: Initial UE Message. Details of this step are described in TS 36.300 [18].

20. The MME sends S1-AP Initial Context Setup Request message to the eNodeB.

21. The eNodeB performs the RRC radio bearer establishment procedure. The user plane security is established at this step. This step implicitly confirms the Service Request. This step is described in detail in TS 36.300 [18]. When user plane security has been established the EPS bearer state is synchronized between the UE and the network, i.e. the UE should remove any internal resources for bearers that are not set up.

    The uplink data from the UE can now be forwarded by eNodeB to the Serving GW. The eNodeB sends the uplink data to the Serving GW address and TEID provided in the step 20.

    For connectivity to multiple PDNs the UE initiates re-establishment of the additional PDN connections using the UE requested PDN connectivity procedure described in clause 5.6.1.

22. The eNodeB sends an S1-AP message Initial Context Setup Complete to the MME. This step is described in detail in TS 36.300 [18].

23. The MME sends a Modify Bearer Request message to the Serving GW by including the handover indicator.

24. Since the Handover Indication is included in step 23), the Serving GW sends a Modify Bearer Request message to the PDN GW to prompt the PDN GW to tunnel packets from WiMAX IP access to 3GPP access system and immediately start routing packets to the Serving GW for the default and any dedicated EPS bearers established.

    In this step, The PDN GW removes the old PCC Rules for the Trusted or Untrusted Non-3GPP IP access and applies the new Rules for E-UTRAN access for charging.

25. The PDN GW acknowledges by sending Modify Bearer Response to the Serving GW.

26. The Serving GW acknowledges by sending Modify Bearer Response message to the MME.

27. The UE sends and receives data at this point via the E-UTRAN system. PDN gateway initiates resource deactivation towards WiMAX access.

A.3.7 WiMAX® to Pre-Release 8 3GPP NetworkSingle Radio Handover procedure

This section describes Single Radio inter-RAT handover support from WiMAX network to 3GPP Pre-Release 8 access network. Figure A-4 provides call flows for a Single Radio Handover from a WiMAX network to a Pre-Release 8 3GPP network without SGSN relocation (i.e. the Source and Target SGSN are the same). In case the 3GPP SFF is co-located with the SGSN there will be no messages exchanged between the 3GPP SFF and the SGSN.

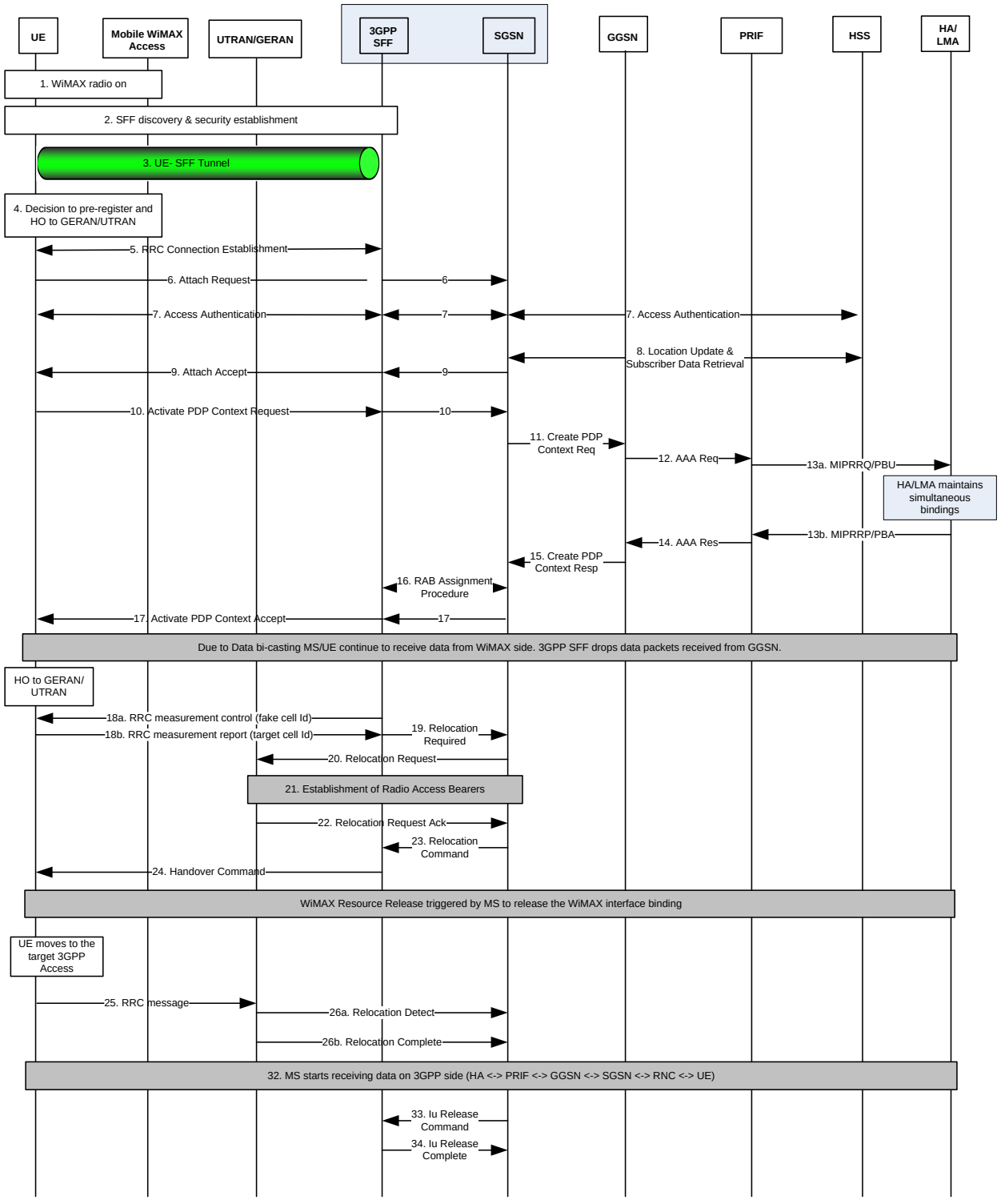


Figure A-5 – Single Radio Handover from WiMAX® to Pre-Release 8 3GPP Access without SGSN relocation

1. The UE is registered with WiMAX and may have an ongoing data session established over WiMAX access.
2. The UE discovers the 3GPP SFF using 3GPP SFF discovery procedure as described in section A.3.5 .
3. The UE may optionally establish a secure IPSec tunnel with 3GPP SFF.
4. The UE makes decision to pre-register to Pre-Release 8 3GPP access (GERAN/UTRAN).
5. If the 3GPP SFF is not co-located with the SGSN, the UE establishes a RRC connection over the UE-3GPP SFF tunnel.
6. The UE initiates the Attach procedure by transmission of a NAS Attach Request message over the UE-3GPP SFF tunnel. The Attach request may be encapsulated in Access Stratum message (e.g. RRC).
7. If no UE context for the UE exists anywhere in the network, an authentication must be performed. If the UE was unknown to the target SGSN and the old SGSN, the target SGSN will send an Identity Request to request the UE's IMSI prior to step 7. These messages are tunnelled to/from the UE via the 3GPP SFF tunnelling mechanism.
8. If the SGSN has changed since the last detach, or if it is the very first attach, the SGSN sends an Update Location to the HSS. The HSS acknowledges the Update Location message by sending an Update Location Ack (IMSI, Subscription data) message to the SGSN.
9. The SGSN sends attach accept to 3GPP SFF and the 3GPP SFF forwards it to the UE.
10. The UE initiates a PDP context activation procedure by sending Activate PDP Context Request message over the UE-3GPP SFF tunnel to the 3GPP SFF. When the 3GPP SFF is not co-located with the SGSN, the 3GPP SFF sends an Activate PDP Context Request to the SGSN. The MS uses a specific APN to indicate its WiMAX home CSN.
11. The SGSN, after validating the PDP Context Request successfully, sends Create PDP Context Request to the GGSN.
12. The GGSN sends an AAA Access Request message along with the IMSI to the PRIF identified by the APN. The AAA proxy function in the PRIF constructs an IMSI based NAI as defined in section 8 of Dual Radio WiMAX - Pre-Release 8 3GPP Interworking Specification [19]. The AAA proxy function in the PRIF also interacts with the home AAA in the WiMAX CSN to get the MN-HA, HA-IP and MN-HA-SPI. Interactions between PRIF and AAA in WiMAX CSN (for IPv4 and IPv6 PDP Context case) are specified in section 8 of Dual Radio WiMAX – Pre-Release 8 3GPP Interworking Specification [19].
13. The PRIF sends a PMIP4 RRQ to the HA with HoA set to all zero. The PMIP4 RRQ also contains the MS NAI, FA CoA, and MN-HA AE that is calculated with the MN-HA key. In case of IPv6 PDP context, the PRIF will send Proxy Binding Update (PBU) as specified in section 8.2 of Dual Radio WiMAX – Pre-Release 8 3GPP Interworking Specification [19]. The HA/LMA may interact with the AAA in the WiMAX CSN as per step 6-7 in section 8.1/8.2 of Dual Radio WiMAX – Pre-Release 8 3GPP Interworking Specification [19].

    Upon receiving the RRQ/PBU message, the HA/LMA assigns the same IP address (IPv4 HoA or IPv6 HNP) that is used by the MS in the WiMAX network. The HA/LMA creates simultaneous bindings for the UE and sends RRP/PBU back to the PRIF. Since HA/LMA maintains simultaneous bindings it doesn't initiate a release procedure or a binding revocation towards WiMAX access.
14. The PRIF sends IPv4 HoA or IPv6 HNP back to the GGSN in AAA Access Accept message.

15 – 17. The Create PDP Context procedure completes as per section 9.2.2 of 3GPP TS 23.060 [20]. In case the 3GPP SFF is not collocated with the SGSN, it involves a RAB assignment procedure between the SGSN and the 3GPP SFF. Due to data bi-casting, the MS/UE continues to receive data on the WiMAX side. The 3GPP SFF drops data packets it receives from the HA/LMA.

18. The MS/UE decides to handover to Pre-Release 8 3GPP Access network. The UE sends handover required message to the 3GPP SFF in order to start Single Radio handover to 3GPP access. If the 3GPP SFF is not co-located with the SGSN, the 3GPP SFF requests the UE to send the target 3GPP cell identity by sending a Measurement Control message that includes a fake cell Id. In response, the UE sends a Measurement Report message to the 3GPP SFF with the desired target 3GPP cell identity. Note that the Measurement Control message is not sent to control the measurement procedure in the UE but rather to trigger the transmission of the Measurement Report message and then allow the 3GPP SFF to initiate the relocation to an appropriate target cell.

19 – 34. In the case of RNC emulation, the 3GPP SFF sends a Relocation Required message (Relocation Type, Cause, Source ID, Target ID, Source RNC To Target RNC Transparent Container) to the SGSN. In the case of SGSN emulation, the UE sends the Relocation Required message to the 3GPP SFF which forwards it internally to the SGSN. The source SRNC shall set Relocation Type to "UE Involved". 3GPP SFF populates the Source RNC To Target RNC Transparent Container. Steps 19 – 24 are executed as per steps 2 – 8 of section 6.9.2.2.2 (Combined hard handover and SRNS Relocation procedure) of TS 23.060 [20].

After step 24, the UE triggers WiMAX resource release to remove the WiMAX interface bindings and switch on the 3GPP radio.

Steps 24 – 34 are executed as per steps 8 – 14 of section 6.9.2.2.2 9 (Combined hard handover and SRNS Relocation procedure) of TS 23.060 [20]. In the case of RNC emulation, the 3GPP SFF performs the role of Source RNC. There is no forwarding of data from 3GPP SFF to target RNC.

32. The MS/UE starts sending and receiving data on Pre-Release 8 3GPP Access. Figure A-6 provides call flows for a Single Radio Handover from WiMAX to Pre-Release 8 3GPP with SGSN relocation. These call flows are similar to the ones described in [20]section 6.9.2.2.2.

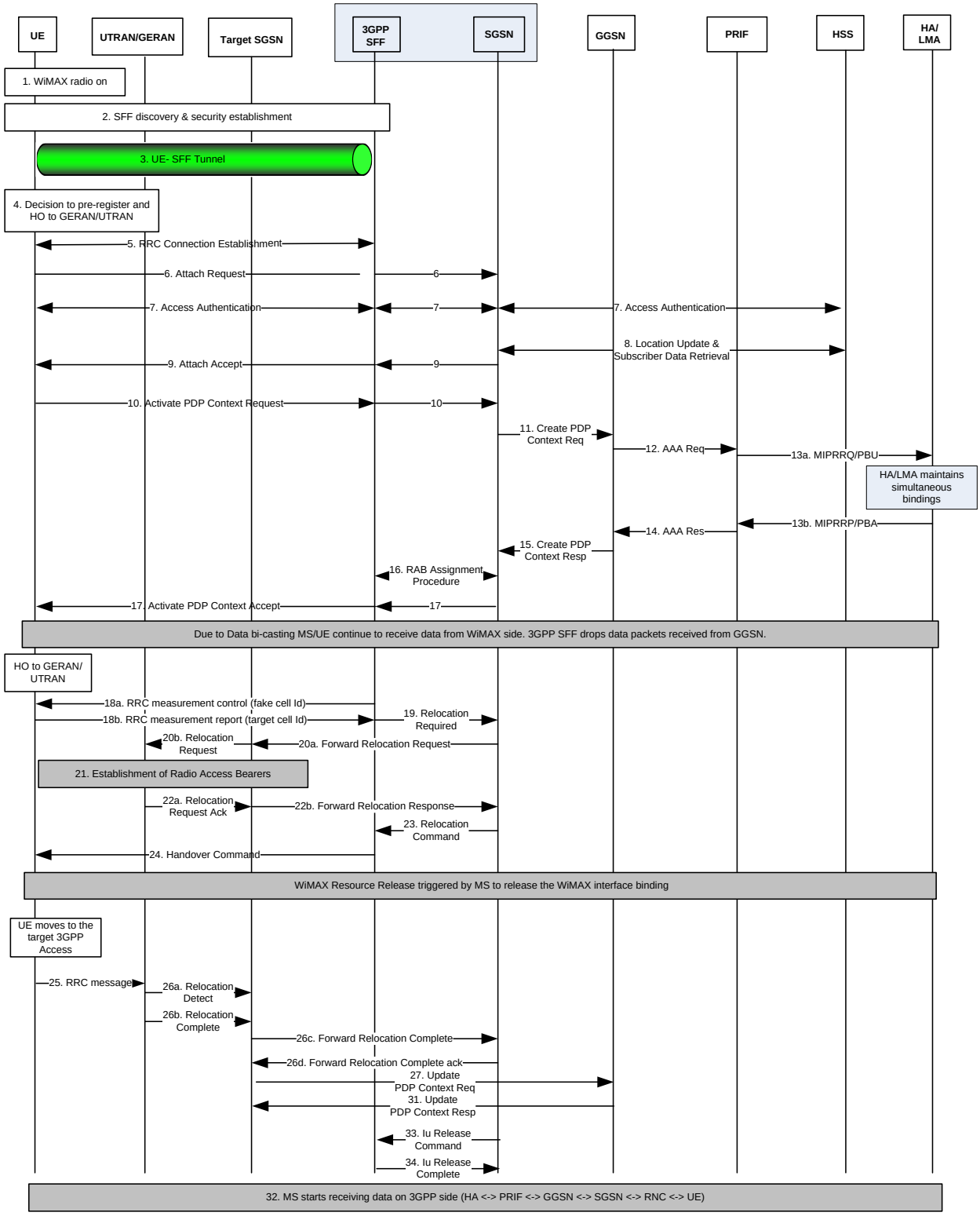


Figure A-6 – Single Radio Handover from WiMAX® to Pre-Release 8 3GPP access with SGSN relocation

The steps are similar to the ones described in Figure A-4 with the addition of steps 20, 22, 27, 31 informing the GGSN, after the Update PDP Context, to send packets to the Target SGSN instead of the Source SGSN. These steps are described in [20].