WiMAX Forum Network Architecture

(Stage 3: Detailed Protocols and Procedures)

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Copyright © 2005-2007 WiMAX Forum. All Rights Reserved.

Table of Contents

25

1   **List of Figures**

41

List of Tables

1 **Revision History**

February 1, 2006	Initial draft
March 27, 2006	Added contributions accepted at the Paris F2F
April 9, 2006	Added contributions accepted at the KC F2F and teleconference on 4/5
	Following contributions have been incorporated to date:
	• 051104_NWG_Huawei_Skeleton for Stage 3 Specification - approved.doc
	• 060306_NWG_stage3_SECAAA.doc
	• 060227_Stage3_InitialNetworkEntry_accepted_v01
	• 060223_SFIDmanagement_accepted.doc
	• 060223-Stage3-QoS.doc
	• 060207_NWG_Huawei_ND&S part of Stage 3 Specification_r3.doc
	• 060215-CSN-Anchored-MM-stage-3-Starent-BW-R2.doc
	• 060125_NWG_Huawei_Stage 3 ND&S Behavior SDLr1.rtf
	• 060223_Stage3_EAPoverR6auth_accepted.doc
	• 060222_Stage3_R6AnchoredASN_Mobility_ProfileC_accepted.doc
	• 060106_NWG_Motorola_00_PC_Relocation_r4.doc
	• 051216_NWG_Motorola_01_Paging_Information_TLV_inclusion_r4.doc
	• 060106_NWG_ZTE_Stage3_TOC_Update_Proposal.doc
	• 060106_NWG_Cisco_Stage3_TLV_Anchored ASN.doc
	• 051104_NWG_Huawei_CATR_Accounting proposal for Accounting Procedure-r1.doc
	• 051102-Stage3-Transport.doc
	• 051102-Stage3-Message-Format-2.doc
	• 060212_stage3_NWG_IM_Paging_updated_baseliner5.doc
	• 060213_NWG_Stage3-Accounting_r4_accepted.doc
	• 060330_NWG_Huawei_comments for 060223-Stage3-QoS-r2.doc
	• 060329_NWG_Nortel_VendorSpecificTLV[1].Accepted.doc
	• 060325_NWG_IPv6_over_IPCS_04.doc
	• 060324_NWG_Stage3-baseline draft for CSN anchored Mobility Management-r3-huawei.doc
	• 060330_Updated Stage3_NWG_IM_Paging_Accepted_KC.doc
	• 060330_NWG_Huawei_comments for 060223-Stage3-QoS-r2_Accepted.doc
	• 060330_NWG_Stage3-RRM-combined_rev_Accepted.doc
	• 060324_NWG_Siemens_Stage3-DHCP-Server-in-CSN.doc
April 22, 2006	Added the following contributions:
	• 060222_Stage3_R6AnchoredASN_Mobility_ProfileC_accepted
	• 060306-CMIP6-stage-3-Starent-Bridgewater-R3_accepted
	• 060328_NWG_stage3_Huawei_Prop_for_AK_PMK_PMK2_SN_usage ,AK context and Re-authent r3a_accepted

July 2006	Added the following contributions:
	• 060417_Updated Stage3_NWG_IM_Paging_baseline_V&V
	• 060418_NWG_Motorola_PMIP_call_flows_DHCP_proxy_in_ASN
	• 060418_Stage3_CSN_Mobility_PMIP_relocation_v2
	• 060419_NWG_Nortel_Initial_Service_Flow.d5
	• 060423_NWG_Huawei_Stage3_Accounting_Update_r7
	• 060501_NWG_SEC-Stg3_Lu-Huawei_AK_Caching_Solution – Comment 644 R4.doc
	• 060502_Stage3_AnchoredASN_Mobility_R4_v5
	• 060507_NWG_Samsung_CMIP4_Relocation_Procedure
	• 060507_NWG_Alcatel_Huawei_Comments for Stage3_InitialNetworkEntry-r2
	• 060511_NWG_Huawei_Stage 3 Paging procedure updated text
	• 060511_NWG_Huawei_Stage 3 Idle Mode Entry procedure updated text
	• 060511_NWG_Huawei_Stage 3 LU updated text
	• 060511_NWG_Huawei_Stage 3 LU updated text r4_Mot_update_r0
	• 060516_NWG_Siemens_IWKupdate_stage3_r3_accepted
	• 060517_ASN_Anchored_MM Profile-C_Comments_ZTE.doc (errors with specific figures and table)
	• 060518_NWG_Intel_Stage 3 MIP operation for Idle mode
	• 060519_NWG_Nortel_Stage_3_Accounting_Comments
	• 060525_NWG_MOT_MN-FA_Support
	• 060525_NWG_Nortel_RRM_Characteristics_Definition
	• 060525_NWG_Samsung_BW_MIP_Key_Hierarchy_Corrections
	• 060531-Vnv- Comment#1230 text
	• 060601_NWG_SEC_Stage 3 Changes for AK Caching Solution – Comment 1444_Lu.doc
	• 060607_NWG_MOT_RegRev_Support_Cmnt_1577r1
	• 060615_Text_for_Nextwave_PIM_Comments_r2
	• 060620_NWG_Nortel_PAG_V&V_Comment_849_v1
	• 060625_ Stage3_ Alvarion_MSK_key_lifetime_in_Access-Accept
	• 060626_NWG_Stage3 ASN MM for Profile A_Harmonized_r9
	• 060627_NWG_Nortel_MS Info_Context_Req_Alcatel_cisco_r3
	• 060628_Siemens_updating_doubleEAP_termination(Lucent comments)_r1.doc
	• 060705_NWG_Huawei_ Stage 3 Network Discovery and Selection Rewrite
	• 060707_NWG_Stage_3_Section5.6_QoS_Correction (SiemensNortelNokia) final Clean.doc
	• 060709_Siemens_Samsung_fixing_MNHA_Distribution_r1.doc (implemented those section that were not yet revised under other contributions)
	• 060709_Siemens_Samsung_fixing_MNHA_Distribution_Impact_on_CSNMM_r1
	• 060710_NWG_Stage3-CSN MM call-procedures-Huawei-ZTE-Motorola
	• 060710_NWG_Stage3_NetworkExit
	• 060712_Stage3Section8_v5
	• 060714_NWG_Stage-3+RRM-small-changes-accepted
	• 060714_NWG_Stage3-RRM-Intel_comments_acceptedr2
	• 060714_NWG_Stage3-RRM-ProfB_w_Lu_Nextwave_harm-accepted

	• 060720-CMIP6-stage-3-update-Starent-Bridgewater-Nokia
	• 060720-NWG- Stage3 IPv6Updates-v4.doc
	• 061906NWG_V&vcomment1204_LU_r1.doc
	• 070906-CMIP6-stage-3-update-Starent-Bridgewater-Nokia
	• Stage3_Section4_corr-1
March 2007	Added the following contributions:
	• 060515_NWG_Siemens_Stage3_DataPlane-r2.doc
	• 060822_NWG_Telsima_Stage3_TransportOperationRulesConsistency_01.doc
	• 060823_Stage3_Alvarion_Move_TLVs_from_5.6.6_to_6.4.2_v2.doc
	• 060823_Stage3_Alvarion_MS_NW_Exit_protocol_v1.doc
	• 060823_NWG_Nortel_MSInfo.doc
	• 06-08-27_NWG_Nortel_RRM_Reporting_Characteristics_Definition_Updates-REV6.doc
	• 060911_NWG_Huawei_Comments for Stage3_ExitNetwork
	• 060911-NWG-VV-FA-relocation-in-idle-mode-Huawei-Intel-Nextwave-r5_NW_Comments.doc
	• 060915_NWG_Siemens_Stage3_7-3-2_Ethernet-CS-r6.doc
	• 060915-VnV-Stage-3-Starent-QoS_richardUpdate.doc
	• 060925_Nokia Stage 3 SF2 QoS-Section 6.3
	• 060925_Nokia Stage 3 SF2 QoS-Section 6.4
	• 061006_NWG_Alcatel_CARC_Data plane_R4_ interoperability.doc
	• 061009-SF_BW_15.doc
	• 061009_Stage3-InterAsnHoAuthUpdate_v1.doc
	• 061009_Stage3-VariousTLVs_v2.doc
	• 061010_Stage3_Ericsson_RRM_Spare_Cap_Rep_Failure_Indicator_TLV_v2_accepted.doc
	• 061013_Siemens_Stage3_Comment459_FuncTypes.doc
	• 061019_NWG_Nortel_Siemens_RRM_Error_Handling-REV2.doc
	• 061102_Stage3_INE_Sections_5.4.2_and_5.5.1_update_v6.doc
	• 061103_Stage3_Reauthentication_Sections_5.4.1.9_update_v7.doc
	• 061103_Stage3_Reauthentication_Sections_5.4.1.9_update_v8.doc
	• 061106_NWG_MOT_ASN_HO_Action_Sec5.doc
	• 061106_NWG_MOT_ASN_HO_Prep_Sec5.doc
	• 061107_Nextwave_SF_Comment_1104r2-accepted.doc
	• 061109_Nextwave_Comment_1997v2
	• 061109_Nextwave_RRM_Message_Reorgv1.doc
	• 061109_Nextwave_Section 5.10.3 Re-write v4
	• 061121_NWG_SEC-Stg3_Changes WiMAX-3GPP2 IWK Lucent (R12).doc
	• 061127_Nokia ISF Classifier UpdateComment2841.doc
	• 061204_NWG_stage3_Idle_mode_exit_rewrite.doc
	• 061205_NWG_Stage3_IPv6_04.doc
	• 061207_NWG_Telsima_Stage3_RRM_Section_5_9_5_1_ver02_accepted.doc
	• 061207-NWG-V&V-Accounting-Section5.4.3-r1.doc
	• 061208_Siemens_Comment426_QoS_errorhandling_r4.doc

	• 061210_NWG_AlvarionUsadeOfSrcAndDstIds_v1_accpepted.doc
	• 061211_NokiaAccountingTriggerStage3.doc
	• 061211-NWG- IPv6-Issue-Resolutions-v1.doc
	• 061211_NWG_MOT_ASN_UC_HO_Sec5.doc
	• 061211_Siemens_rearrangedSFhandlingDescr_r2.doc
	• 061212-NWG-V&V-RRM_DCD-UCD-TLVs-Huawei-Siemens-r2.doc
	• 061212_Siemens_Stage3_QoS_messages_r3.doc
	• 061213NWG_IMPage_IM_Entry_Sec5_re-write-ALU.doc
	• 061213_NWG_Huawei_ Stage 3 Network Discovery and Selection Rewrite FINAL.doc
	• 061218_Nextwave_Comment_1106
	• 061219_NWG_NORTEL_ASN_HO_Cancel_r1.1.doc
	• 061221-SF_BW_38_Prepaid.doc
	• 061219_Siemens_reservationAction_commenr2936.doc
	• 061220_NWG_Sec 5.5.2.2.2-ALU comment1322
	• 061221_Siemens_QoS_Mobility_Comment1986_r2.doc
	• 061227_NWG_Profile_C_HO_Sec9_r9.doc
	• 061227_NWG_R6_ASN_MM_Sec_9.1.4.v8.doc
	• 061229_Stage3_all_QoS_TLVs_r2.doc
	• 070101_Stage3_RRM-comments-incorp.doc
	• 070101_Stage3-SpareCapacityIndicator-v0
	• 070102R5_SEC_Stage_3_Section_5.3_Consolidated_Edits.doc
	• 070104_NWG_Section-rewrite-5.4--5.4.1.1.doc
	• 070104_Siemens_NWG Stage 3_sec54187_modified.doc
	• 070105_NWG_Section-rewrite-5.4.1.8--5.4.1.8.6.doc
	• 070108_MOT_NWG_LocationUpdate_Baseline.doc
	• 070116_NWG_R6_ASN_MM_UtilityProcedures.doc
	• 070116_NWG_Stage3_Section5.3.2_Edit_r1.doc
	• 070115_MOT_NWG_Utility_Call_Flows_r1.doc
	• 070116_NWG_Stage3_Section5.3.3_Edit_r1.doc
	• 070116_NWG_Stage3_Section5.4.2_Edit.doc
	• 070118_Stage3_DHCP_Relay_R4_TLVs_r1.doc
	• 070120_Paging and Idle mode_intro.doc
	• 070122_NWG_Siemens_section584_update.doc
	• 070122R3 v1.0 NWG RADIUS VSA BW.doc
	• 070124_Stage3-Context_TLVs_v2.doc
	• 070130_Errors_in_editorial_application_of_ND&S section.doc
	• 070130_NWG_Fujitsu_Failure_Indication_Handling_V&V_Comments.doc
	• 070130_NWG_Fujitsu_Failure_Indication_Handling_V&V_Comments_r2.doc
	• 070130_NWG_Nortel_ R4_R6_Combined_Accounting_Ext.doc
	• 070131_NWG_EAP_Methods_v3_2.doc
	• 070131_HO_Messages_and_TLVs_for_Section_5_r7-JS
	• 070201_NWG_Starent_ASN_Error_Handling.doc

	• 070206_NWG_Stage3_Hawaii_Draft_RRMreview.doc • 070209-NWG-V&V-Stage3_Clarification_Accounting_r1 • 070210_NWG_Huawei_Stage3_CSNMM_error handling.doc • 070211_NWG_Stage3_Section8_text-r2.doc • 070213_NWG_Siemens_section535_update.doc • 070214_NWG_Stage3_Section1_text-r2.doc • 070215_R6_LU_message_tables.doc • 070215_NWG_SEC_AuthzPolicy.doc • 070215_NWG_SEC_remove5.3.3.5.doc • 070216_NWG_Nokia_Transport_Section_4_Updated.doc • 070221_MOT_NWG_Power_Down_Updates.doc • 070222R2_NWG_Transport_Section_4.doc • 070228_Figure_5-20.vsd • 070228_Figure_5-21.vsd • 070228R1_Hotlining_Rewrite.doc • 070228R2 RADIUS Messages and Attributes • 070305-NWG-Siemens_VV_section5.3_correction • 070307_NAI_Decoration.doc • 070307_NW_Comment_357_Supporting_File.doc (sections 5.7 and 5.10 only) • 070307R1_SPI_Cleanup.doc • 070307_Stage3_INE_Section_5.5.1_update_v9.doc • 070307_timer_max_expiry_actions_NW_Samsung • 070307_ZTE_Proposed_SF-Info_TLV_Changes_v6.doc • 070314_Stage3_AuthRelay_EAP_Complete_update_v1.doc • MS Info.doc • R6_Data_Path_De-Reg_Operation.doc • Stage3 CSNMM Implementation.doc • 5.13.4_R4_Data_Path_De-Reg_Procedure-R1.doc
July 11, 2007	• Implemented all Stage 3 accepted contributions from 00000_r016_NWG-Rel-1[1].0.0-CR-Tracking-Spreadsheet.xls

1

1 # 1. Introduction and Scope

2 This document describes the detailed procedures, call flows, messages, timers, TLVs and attributes for the WiMAX
3 end-to-end network specification. Details specified in this document supersede corresponding text in Stage 2.

4 ## 1.1 Relationship between Stage 2 and Stage 3

5 This document builds on the Stage 2 document in two dimensions:

6 - Procedures, call flows, messages, timers, TLVs and attributes are specified, based on the framework in
7 Stage 2.

8 - Whereas Stage 2 is a functional specification, Stage 3 describes normative mapping of procedures and
9 messages for each of the ASN profiles defined in Stage 2. Wherever applicable, mandatory and optional
10 messages and parameters are defined in this document.

11 ## 1.2 Scope

12 This is Release 1.0.0 of the NWG specification. In this Release, the specification covers stationary and mobile
13 WiMAX clients connecting to a mobile WiMAX network. The specification is based on Stage 1 requirements from
14 the SPWG. This document is the basis for NWIOT specifications.

15 ## 1.3 Terminology

16 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
17 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below,
18 taken from IETF RFC 2119.

19 Note that the force of these words is modified by the requirement level of the document in which they are used.

20 - MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute
21 requirement of the specification.

22 - MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition
23 of the specification.

24 - SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in
25 particular circumstances to ignore a particular item, but the full implications must be understood and
26 carefully weighed before choosing a different course.

27 - SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid
28 reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full
29 implications should be understood and the case carefully weighed before implementing any behavior
30 described with this label.

2. References

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

[2]   IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

[3]   RFC 4282, The Network Access Identifier

[4]   IEEE 802.16g draft

[5]   RFC 2104, HMAC: Keyed-Hashing for Message Authentication

[6]   RFC 3748, Extensible Authentication Protocol (EAP)

[7]   RFC 4017, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs

[8]   RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)

[9]   RFC 2869, RADIUS Extensions

[10] RFC 2866, RADIUS Accounting

[11] WiMAX End-to-End Network Systems Architecture (Stage 2)

[12] RFC 791, Internet Protocol

[13] RFC 815, IP datagram reassembly algorithms

[14] ITU-T Rec. E.212, The international identification plan for mobile terminals and mobile users

[15] RFC 3344, IP Mobility Support for IPv4

[16] RFC 966, Host Groups: A Multicast Extension to the Internet Protocol

[17] EAP-TLS, B. Aboba and D. Simon, PPP EAP TLS Authentication Protocol (EAP-TLS), RFC2716

[18] EAP-AKA, J. Arkko et al, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), RFC4187

[19] EAP-TTLS, Paul, Funk, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), draft-ietf-pppext-eap-ttls-05

[20] MSCHAPv2, G. Zorn, Microsoft PPP CHAP Extensions, Version 2, RFC2759

[21] RFC 4285

[22] RFC 2131

[23] RFC 3046

[24] RFC 3993

[25] RFC 2132

[26] RFC 3543

[27] RFC 2865

[28] RFC 3576

[29] RFC 3775

[30] RFC 3776

[31] RFC 4030

1   [32] RFC 4283

2   [33] RFC 3736

3   [34] RFC 2462

4   [35] RFC 2868

5   [36] RFC 3012

6   [37] draft-ietf-pppext-eap-ttls-05.txt

7   [38] draft-yegani-gre-key-extension-02.txt (within a week)

8   [39] draft-ietf-mip6-hiopt-02.txt

9   [40] draft-ietf-16ng-ipv6-over-ipv6cs-01.txt

10   [41] draft-ietf-radext-ieee802-00.txt

11   [42] draft-ietf-16ng-ipv6-over-ipv6cs-01.txt

12   [43] draft-ietf-16ng-ip-over-eth-over-802.16-01.txt

13   [44] draft-ietf-mip4-gen-ext-01.txt

14   [45] draft-ietf-mip6-ikev2-ipsec-08.txt

15   [46] RFC 4284

16   [47] RFC 2548

17   [48] RFC 3588

18   [49] RFC 2494

19   [50] RFC 3315

20   [51] RFC 4372

21   [52] RFC 3513

22   [53] RFC 3879

23   [54] RFC 3041

1 3. Message Primitives Format and Transport Protocol

2 This section is applicable to message primitives defined for ASN reference points R4, R6 and R8.

3 3.1 Message Header and Body

4 The message header starts immediately after the UDP transport header and is followed by message body. Message
5 format (illustrated for IPv4 addresses) is as follows

0	8	16	24	27	31
Version	Flags	Function Type	OP ID	Message Type	
Length		MSID			
MSID					
Reserved					
Transaction ID		Reserved			
Destination Identifier TLV					
Source Identifier TLV					
TLVs					

6

7 **Figure 3-1 – Message Format**

8 The fields have the following meaning:

9 • Version: Protocol version number. This field is 1-byte long. The current version number is 1.

10 • Flags: 1 byte long.

r	r	r	r	r	r	T	R

11

12 **Figure 3-2 – Flags Format**

13 − R: Reset Next Expected Transaction ID.

14 − T: If this bit is set, Source and Destination Identifier TLVs are included in the message.

15 − r: Reserved bits, have to be set to zero. Receiver SHALL ignore all 'r' bits.

16 • Function Type: This field is 1 byte long and indicates individual functions, for example, HO Control.

17 • OP ID: This field is 3 bits long and indicates Operation Type, as follows:

18 − 000: Invalid value, SHALL not be used

19 − 001: Request/Initiation (start of 2-way or 3-way transaction)

20 − 010: Response (response to Request/Initiation)

21 − 011: Ack (finishes 3-way transaction)

22 − 100: Indication (1-way transaction)

23 − 101, 110, 111: reserved

- **Message Type:** This field is 5 bits long and indicates the message type corresponding to the function type, for example, *HO_Req*.

- **Length:** The length of the message (including the entire header) in bytes. This field is 2 bytes long.

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

- **Reserved:** 32 bits, SHALL be set to 0.

- **Transaction ID:** The transaction ID is an unsigned 16 bit value. If the transaction ID is 0, the packet should be dropped and not processed.

  The transaction ID is used to identify messages that are part of the same 2-way or 3-way transaction, and to identify messages that are out-of-order. Transaction ID usage:

  - Transaction ID SHALL be unique for the tuple: {Source, Destination, MSID, Function Type}.

  - Transaction ID for the first transaction for tuple {Source, Destination, MSID, Function Type) SHALL be set to random non-zero value

  - Transaction ID SHALL be the same for a given Request/Initiation-Response-Ack sequence of messages in case of 3-way handshaking or Request/Initiation-Response sequence in case of 2-way handshaking. All retransmissions SHALL also set the same transaction ID.

  - For every new transaction for the tuple {Source, Destination, MSID, Function Type} the transaction ID SHALL be incremented by 1 modulo 65536. If increment operation gives zero value, transaction ID SHALL be set to "1".

  - "R" bit should only be set (if set) in the first message of the transaction (Request/Initiation/Indication). Retransmitted message(s) SHALL have the same "R" bit setting as an original one. Transaction Messages that have the "R" bit set will reset any previous outstanding/unprocessed transactions for particular tuple {Source, Destination, MSID, Function Type) to prevent race conditions. The receiver of the message with "R" bit set SHALL discard any outstanding or unprocessed transactions for the same tuple {Source, Destination, MSID, Function Type} and set the Next Expected Transaction ID to the Transaction ID of the received message incremented by 1 modulo 65536. If the increment operation gives zero value, then Next Expected Transaction ID SHALL be set to 1. For any tuple {Source, Destination, MSID, Function Type} there SHALL only be one outstanding transaction with the "R" bit set.

  - For the purpose of transaction state synchronization between Source and Destination, the Transaction ID for all function types SHALL be set by the Source to random non-zero value and "R" bit SHALL be set to "1" in the following cases:

    o This is the first transaction for the specified function type after MS (identified by MSID in the header) state change from Active to Idle.

    o This is the first transaction for the specified function type after MS (identified by MSID in the header) state change from Idle to Active. Trigger in BS is receiving RNG-REQ from MS with Ranging Purpose Indicator bit#0 set to zero and PC ID TLV included.

    o This is the first transaction for the specified function type after new MS (identified by MSID in the header) is detected by the sender of the transaction. Trigger can be any network entry/re-entry or handover of a new MS.

  - Source is allowed to initiate multiple concurrent transactions for the same tuple {Source, Destination, MSID, Function Type) at any given point in time. Any transaction without "R" bit set and with Transaction ID greater than the Next Expected Transaction ID is termed being out-of-order transaction. When out-of-order transaction is received, the receiver may discard the message or start timer $T_{missing}$ for every missing transaction if such timer was not set before by another out-of-order transaction; the receiver may aggregate multiple timers into a single one if all these timers represent a single contiguous block of missing transactions; for the purpose of simplicity in behavior description we will use a timer per missing transaction. This timer SHALL be stopped/cancelled if corresponding missing

1   transaction is received before the timer expiration, or any transaction with "R" bit is received for the
2   same tuple {Source, Destination, MSID, Function Type}. When the timer Tmissing expires,
3   corresponding missing transaction is declared lost and the receiver shall discard any subsequent
4   messages associated with that transaction.

5   • Reserved: Bits SHALL be set to 0.

6   • Destination Identifier TLV: Variable-length identifier of the Destination Entity, as defined in [11]; i.e., ID
7   of the Network Node which hosts the Functional Entity which is the intended destination of the message
8   body.

9   Receiver of the message should check Destination Identifier TLV in the header. If Destination Identifier
10   indicates the receiver's Identifier, receiver should process the message. Otherwise receiver should relay the
11   message to Destination Identifier without any change.

12   • Source Identifier TLV: Variable-length identifier of the Source Entity, as defined in [11]; i.e., ID of the
13   Network Node which hosts the Functional Entity that is the originator of the message body.

14   • TLVs: Type-Length-Value encoding of information elements, following the header.

15   3.1.1 Usage of Source Identifiers and Destination Identifiers TLV

16   The Source Identifiers and Destination Identifiers TLVs identify the logical entities associated with the processing
17   of the messages. The Source Identifier and Destination Identifier TLVs, when included, SHALL be the first TLVs
18   in the message as shown in Figure 3-1.

19   Source Identifier and Destination Identifier TLVs SHALL be included if ID in DST TLV is not equal to the
20   destination IP address

21   The Source and Destination Identifier TLVs are used to allow message delivery between WiMAX Entities that do
22   not have direct IP connectivity between them. Figure 3-3 gives an example of the ASN separated into two IP Clouds
23   each of which uses private IP Address space. IP messages within each cloud are delivered using IP routing
24   mechanisms. However the messages between the clouds cannot rely on IP routing. Instead the WiMAX Entities
25   located on the border between the clouds relay the messages using Source and Destination ID TLVs.
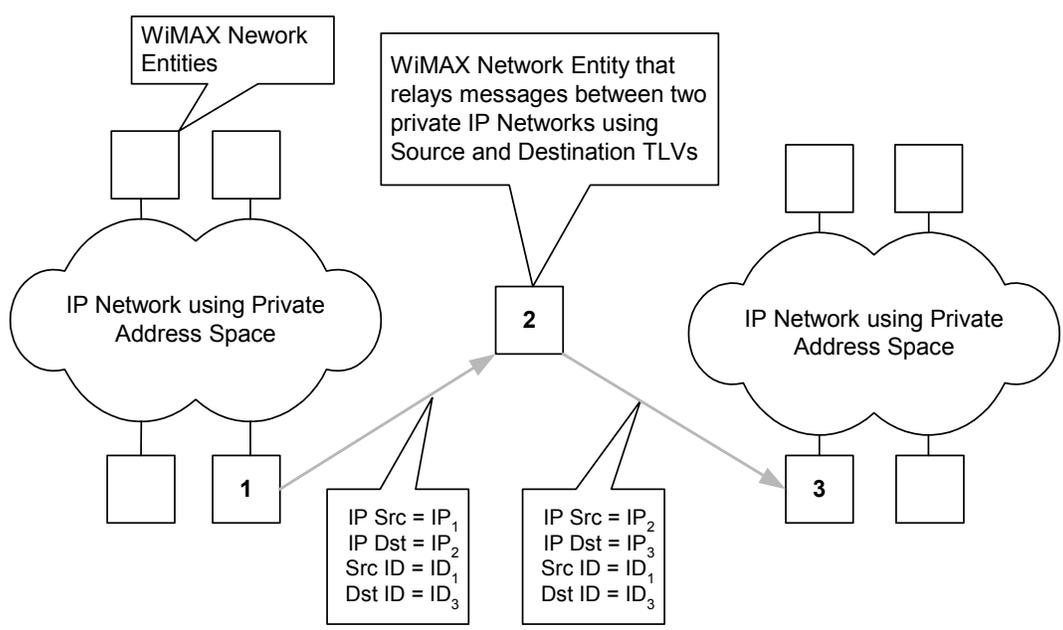
27   **Figure 3-3 – Example of ASN Separated into Two Private IP Clouds**

1   A WiMAX Entity, which relays messages basing on Source and Destination IDs, SHALL be capable of translating
2   every ID into the corresponding IP Address within each IP routable cloud connected to this entity. This translation is
3   shown on Figure 3-3, which shows Entity 1 sending a message to Entity 3 via Entity 2.

4   The relaying entity terminates and regenerates UDP IP datagrams and doesn't modify the WiMAX Header.

5   Mapping IDs onto IP Addresses is an implementation issue.

6   Only the messages that are destined to a single entity MAY use the Source and Destination Identifier TLVs.

7   The Source and Destination Identifiers, if used, SHALL be unique across a network in which entities can
8   communicate using these Identifiers.

3.1.2   Transport Protocol Usage

10   The protocol SHALL be based on UDP and SHALL use IANA reserved port 2231 (WiMAX port) over reference
11   points R4, R6 and R8.

12   UDP checksum is mandatory when used with IPv4.

13   All transactions SHALL be initiated with the destination port set to the WiMAX Port. Sender SHALL use the
14   WiMAX reserved port as source and destination port in all messages..

3.2   Transport Protocol

16   The Stage 2 model consists of functional entities communicating with their peers to realize specific control
17   functions. For instance, a paging controller functional entity communicates with a paging agent entity using paging
18   messages. The Stage 2 specification permits possible variations in how functional entities can be collocated in an
19   implementation. Thus, it also becomes necessary in Stage 3 to specify messaging between functional entities. When
20   functional entities are collocated, a specific implementation MAY aggregate or optimize control messaging.

21   Figure 3-4 illustrates the essential aspects of control messaging between functional entities. Here, communication
22   between peer elements of two functional entities A and B are shown. Each peer entity is realized in a Network Node
23   (e.g., a BS), which has connectivity to an L2 or L3 network. The figure shows that whereas peer functional entities
24   A and B are collocated in the same physical implementation on one side, they are located in different
25   implementations on the other side. The figure also shows communication between peer functional entities. Whereas
26   functional entity A1 on the left communicates with more than one peer on the right, functional entity B1 on the left
27   communicates with the single peer B2 on the right. For the peer entities to communicate there SHALL be a path
28   between the corresponding physical implementations, for instance, direct IP connectivity or a tunnel.

1
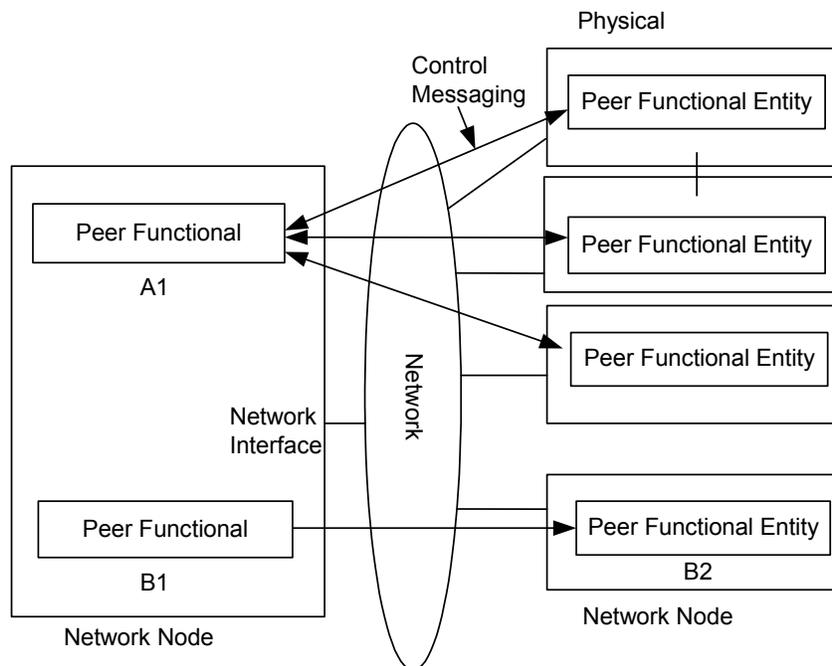
Figure 3-4 – Communication Model

3 UDP/IP SHALL be used as the transport protocol for communication between peer functional entities. The peer
4 functional entity (FE) at each end is addressed by the ID of the Network Component which hosts the FE, in
5 combination with the Function Type (e.g. QoS, HO, R3MM) which is part of the WiMAX NWG Message Header
6 (section 3.1). The list of Function Types is given in Table 5-1. This IP address SHALL be one of the IP addresses
7 assigned to the corresponding physical implementation. The UDP/IP messages between peer entities MAY be
8 tunneled between the corresponding physical implementations, but this is transparent to the functional entities.

9 When messages between functional entities are relayed by an intermediary, the messaging is still point-to-point, first
10 between the source and the relay, then between the relay and the destination. Thus, it is adequate to support point-to-
11 point messaging between any two peer entities.

12 Functional entities which are collocated in the same physical implementation are addressed by a single IP address.
13 Similar implementation on both sides MAY combine messaging between the collocated functional entities into a
14 single UDP message (using a single port number).

15 The adjacencies between peer entities are assumed to be configured in the physical implementations. In later
16 releases, automatic discovery procedures MAY be specified. Any security requirement for peer communication is
17 assumed to be met at the network layer (e.g., encrypted tunnels) or at the higher layer (e.g., encrypted messages).

18 The protocol stack representation for control message communication is shown in Figure 3-5. The L2/L3
19 connectivity represents the communication path between the functional entities. The IP layer packets between the
20 functional entities will be encapsulated in specific manner depending on the nature of the connectivity (for instance,
21 GRE encapsulation for GRE tunnels). The outer envelope of the encapsulated packet would then have addressing
22 information that enables the intervening L2/L3 network to deliver the packet to the appropriate physical
23 implementation.

1
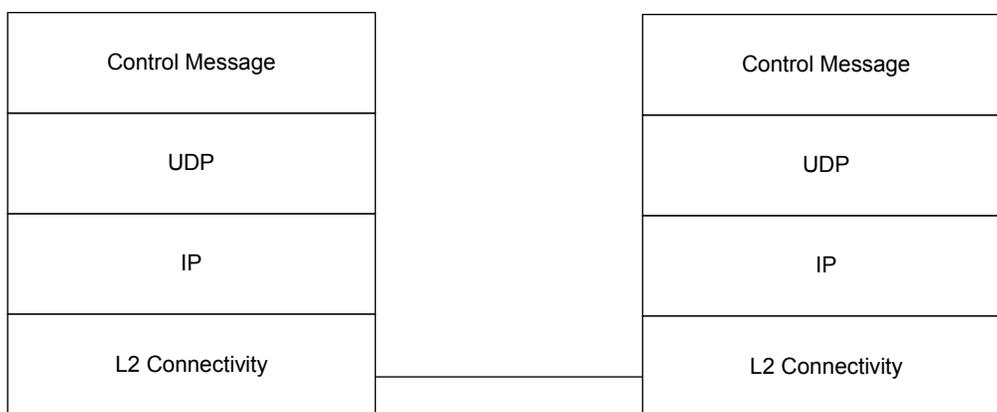
2   **Figure 3-5 – Protocol Layers**

3 ## 3.3   Transport Requirements

4 ### 3.3.1   Reliable Message Delivery

5 Messages between functional entities need to be delivered reliably. Reliability mechanisms (such as retransmissions,
6 acknowledgements, message identification and graceful handling of duplicate messages) SHALL be incorporated at
7 the application level to ensure reliable message delivery.

8 ### 3.3.2   Message Size and Fragmentation

9 The size of a UDP message is limited to 65535 bytes. The size of messages between functional entities SHALL
10 therefore be less than this. Larger messages SHALL be fragmented at the application. As the size of UDP messages
11 MAY be limited by the path MTU size, fragmentation as defined by [12] & [13] SHALL be supported.

12 ### 3.3.3   ASN Bearer Plane MTU Size

13 The default MTU size to/from the MS SHALL be 1400 bytes. The MTU size SHALL be configured less than or
14 equal to 1400 bytes.

15 ## 3.4   Error Handling

16 ### 3.4.1   ASN Control Message Processing

17 Table 3-1 captures the behavior for handling failure or unexpected conditions during ASN control message
18 processing.

19   **Table 3-1 – Message Processing Error Cases**

	Failure Case	Action
1	No response received from peer after sending Request/Response message	Retransmit until max retries exhausted.
2	Request message not understood by the receiver (decode error, corrupted packet etc)	Send response with Failure Indication TLV.
3	Response or Ack message not understood by the receiver (decode error, corrupted packet etc)	Discard the message, no response generated.
4	Duplicate Message (matching TID being processed)	Discard the message, no response generated.
5	Out of order message (old TID: TID = X received when	Discard the message, no response

	Failure Case	Action
	TID > X was expected)	generated.
6	Out of order message (skipped TID: TID = Y > X received when the next expected TID = X)	Process the message normally. The receiver starts timer $T_{missing}$ awaiting the missing transaction.
7	Unrecognized TLV found in message	Ignore TLV, process message
8	Mandatory TLV not included in the message Inconsistent message or incomplete message	Send response with Failure Indication TLV
9	Duplicate TLVs included in a message	Keep first TLV and ignore other occurrences, process message
10	Unexpected TLV in message	Ignore TLV, process message
11	Unexpected message received: Message received in unexpected state, Function or Node	Discard the message, no response generated.
12	Request to terminate or delete context or datapath that does not exist	Send response with Success or other code to prevent repeated requests

1 After a message is processed successfully at the receiver, a "success" indication to the sender is implicit in the reply
2 generated to the message received i.e., a *Path_Reg_Rsp* in reply to *Path_Reg_Req* etc.

3 For the error conditions when a reply needs to be generated by the receiver back to the sender, the Failure Indication
4 TLV can be used to indicate the proper error code. There will be some common error codes across all message types
5 (like decode error, poorly formed message etc) and there will also be error conditions specific to each Function type
6 (like Path Registration, IM entry, HO control etc).

7 The "reply" message used to indicate the error to the receiver will depend on the specific Function and Message
8 Type that encountered the error. Each functional area SHALL independently identify the message behavior, error
9 codes and any follow up action required of the sender for failure cases.

10 3.4.2   Asynchronous Error Indication to Peers

11 When an internal error is encountered on a Functional Entity that needs action on a Peer Functional entity, the error
12 condition SHALL be indicated to the peer asynchronously with a message for faster cleanup or recovery. These
13 types of errors can often result in loss of state on a session so there may be no retransmissions possible from the
14 sender.

15 The message used to indicate the error to the peer will depend on the specific function that encountered the error.
16 Each functional area defines the error handling. The error code will be indicated using the Failure Indication TLV
17 included in a error indication message for the function.

4. Control Plane Protocols and Procedures

Note: For all messages defined in Release 1.0.0, the ordering of mandatory and optional TLVs is not enforced by the sender or receiver.

Default and min/max values for timers (unless already specified) will be defined in future releases of this specification.

This section specifies ASN Profile agnostic control plane protocols and procedures. Any references to the R6 reference point in this section are identically applicable to ASN Profiles A and C and not applicable to Profile B ASNs. Section 7 describes control plane protocols and procedures specific to R6 that are different for ASN Profiles A and C.

Note: For messages or attributes that need an Enterprise number or Vendor ID, use 24757 as assigned by IANA for the WiMAX Forum.

4.1 Network Entry Discovery and Selection/Re-selection

4.1.1 General

In a WiMAX network, a full network entry discovery and selection/re-selection procedure includes four steps:

    a.   NAP Discovery

    b.   NSP Discovery

    c.   NSP Enumeration and Selection

    d.   ASN Attachment based on NSP Selection

The procedure is applicable to the first time use, initial network entry, network re-entry, or when an MS transitions across NAP coverage areas. The procedure defines the method for discovering, identifying and selecting a WiMAX network, but does not define the actual network entry procedure once the network has been selected.

4.1.2 Detailed Procedure

The following sub sections define the detailed procedure for network entry discovery and selection.

4.1.2.1 NAP Discovery

An MS detects available NAP(s) by scanning and decoding DL-MAP of ASN(s) on detected channel(s). The most significant 24 bits (MSB 24 bits) of the "Base Station ID" SHALL be used as Operator ID, which is the NAP Identifier. NAP discovery is based on the procedures defined in IEEE Std 802.16 [1] and out of the scope of this specification. Operator ID/NAP ID allocation and administration method, and field formatting are defined in IEEE Std 802.16. If information useful in MS discovery of NAP, including previously detected and retained values, and/or stored information such as channel, center frequency, and PHY profile is available in configuration information, it MAY be used to improve efficiency of NAP discovery.

4.1.2.2 NSP Discovery

The NAP MAY support more than one NSP. Also, the NAP may be required to present separate NSP identifier(s) for regulatory or other deployment reasons, even if only one NSP is associated with the NAP, and even if the NAP identifier and NSP identifier are the same value. For networks that require NSP identifier distinction, the network SHALL signal to the MS that, in addition to NAP ID, a list of one or more NSP identifiers is required to completely identify the network and provide adequate information for the MS to make a network selection decision. The list of NSP IDs presented over the air interface as part of SII-ADV and/or SBC-RSP SHALL be uniform across all Base Stations of the same NAP ID. The advertised NSP ID list SHALL contain only NSPs that are directly connected to the NAP's network and with which the NAP has a direct business relationship, but not those that can be reached only through another NSP. The network SHALL set the first bit (in transmission order) of the LSB of Base Station ID (NSP Identifier Flag) to a value of '1' to indicate that separate enumeration of one or more NSP identifiers is required to completely identify the network for network selection purposes.

1
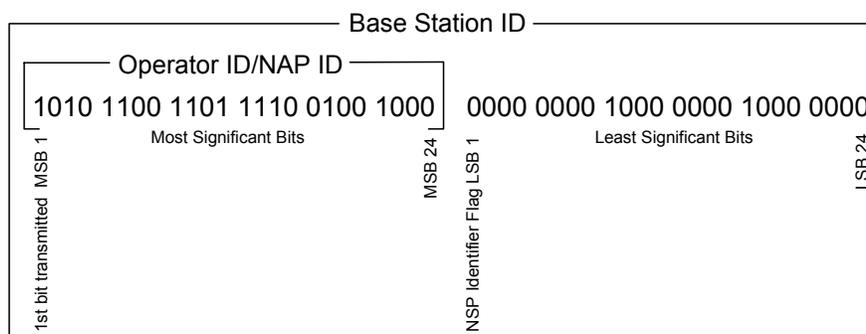
2   **Figure 4-1 – Base Station ID Format for Network Discovery and Selection**

3   In the NAP+NSP deployment case where there is only one NSP associated with the NAP and where no regulatory or
4   deployment reasons compel separate presentation of an NSP identifier, NAP identifier alone is sufficient to
5   completely identify the network. The NAP SHALL identify this case by setting NSP Identifier Flag to a value of '0'.
6   In this case, when the MS detects the identifier of a NAP, the MS knows the identifier of associated NSP and no
7   more identification operations SHALL be performed.

8   NSP ID is formatted as a 24 bit field that follows the format shown in Figure 4-1:

9   **Table 4-1 – NSP ID 24-bit Format for Network Discovery and Selection**

Status	Binary	Hex	Decimal	Notes
Unused	000000000000000000000000	000000	0	25% of the 24-bit space (all numbers beginning with bits "00") is allocated for IEEE-assignable OIDs, except 0, which is excluded. This provides 4194303 (222-1) OIDs.
First IEEE-assignable OID	000000000000000000000001	000001	1	
Last IEEE-assignable OID	001111111111111111111111	3FFFFF	4194303	
First reserved OID	010000000000000000000000	400000	4194304	Reserved for future use. Includes all numbers beginning with bits "01", "10", and "11" except those beginning with "1111". In all, 11,534,336 numbers (11/16 of the space) are reserved.
Last reserved OID	111011111111111111111111	EFFFFF	15728639	
First E.212-based OID	111100000000000000000000	F00000	15728640	All E.212-derived OIDs begin with bits "1111". The next 10 bits represent the three-digit MCC; the next 10 bits represent the MNC.
Last E.212-based OID	111111111001111111100111	FF9FE7	16752615	
First public OID	111111111001111111101000	FF9FE8	16752616	The 24,600 largest numbers in the space, all starting with "1111", are reserved for the public OID pool.
Last public OID	111111111111111111111111	FFFFFF	16777215	

10   When using the IEEE-assignable OID for NSP ID format, the OID value SHALL be allocated and administered by
11   the IEEE Registration Authority (RAC)[1]. When using the E.212-based OID method for NSP ID format, the values
12   for MCC & MNC SHALL be defined, allocated and administered by using the method as described in ITU-T
13   Recommendation E.212[2], and mapped to the number space as defined by the IEEE Registration Authority.

---

[1] IEEE Registration Authority, IEEE Standards Department, 445 Hoes Lane, Piscataway NJ 08854; Phone: (732) 465-6481; Fax: (732) 562-1571; http://standards.ieee.org/regauth/index.html; Email: IEEE Registration Authority.

[2] ITU-T Recommendation E.212 (05/2004, including Erratum 1 [10 /2004]), "The international identification plan for mobile terminals and mobile users," May 2004 http://www.itu.int/rec/T-REC-E.212/en

1   Selection of the method used for NSP ID format is implementation specific.

2   If the network transmits a list of NSP IDs, the network MAY also transmit a list of Verbose NSP Names over the air
3   interface as part of SII-ADV and/or SBC-RSP. In response to an SBC-REQ that includes an SIQ TLV with bit#1
4   value set to '1', the network SHALL transmit a list of Verbose NSP Names along with the list of NSP IDs, over the
5   air interface either as part of SII-ADV or SBC-RSP. When transmitted as part of SII-ADV, the network SHALL
6   transmit the message in the frame specified by the SII-ADV Message Pointer TLV included in SBC-RSP. The MS
7   SHALL use the list of verbose NSP names to assist the subscriber or potential subscriber to select a network for
8   attachment using the 'Manual Mode' selection method. The MS SHALL use the NSP Change Count TLV to
9   determine if there has been a change in any value of the NSP ID List or Verbose NSP Name List, and the MS
10   SHALL replace the previously stored information when a change in NSP Change Count is detected and new NSP ID
11   information is acquired.

12   When the NSP Identifier Flag is set to '1', the MS SHALL sequentially perform NSP Discovery with each NAP for
13   the purpose of discovering the supported NSPs. The list of available NAPs MAY be further categorized as 'User
14   Controlled NAP Identifier list' and/or 'Operator Controlled NAP Identifier list' (categorization and prioritization of
15   NAP ID lists is a deployment detail and beyond the scope of the Release 1.0.0 specification). If such categories of
16   lists are available, selection MAY proceed as follows:

17   • If the "User Controlled NAP Identifier list" is available in the MS, each NAP in the "User Controlled NAP
18   Identifier list" in the MS (in priority order):

19   – if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored
20   in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is
21   equal to the value of NSP Change Count stored in the SS, then the supported NSPs and Verbose NSP
22   Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP
23   Names, SHALL be added to the "list of available NSPs",

24   – if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information
25   stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from
26   networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL
27   obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name
28   List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through
29   unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-
30   REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS
31   transmittal of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with bit
32   0 set to a value of '1' and bit 1 set to a value of '1' during network entry to solicit BS transmittal of
33   NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested
34   NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The
35   identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of
36   available NSPs". After obtaining and storing the identifiers of supported NSPs, the MS SHALL restart
37   the ND&S process.

38   • If the "Operator Controlled NAP Identifier list" is available in the MS, each NAP in the "Operator
39   Controlled NAP Identifier list" in the MS (in priority order):

40   – if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored
41   in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is
42   equal to the value of NSP Change Count stored in the SS, then the supported NSPs and Verbose NSP
43   Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP
44   Names, SHALL be added to the "list of available NSPs",

45   – if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information
46   stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from
47   networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL
48   obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name
49   List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through
50   unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-
51   REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS
52   transmittal of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with bit

1   0 set to a value of '1' and bit 1 set to a value of '1' during network entry to solicit BS transmittal of
2   NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested
3   NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The
4   identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of
5   available NSPs". After obtaining and storing the identifiers of supported NSPs, the SS SHALL restart
6   the ND&S process.

7   • If neither "User Controlled NAP Identifier list" nor "Operator Controlled NAP Identifier list" is available in
8   the MS, each NAP in implementation specific order:

9   − if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored
10   in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is
11   equal to the value of NSP Change Count stored in the MS, then the supported NSPs and Verbose NSP
12   Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP
13   Names, SHALL be added to the "list of available NSPs",

14   − if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information
15   stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from
16   networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL
17   obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name
18   List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through
19   unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-
20   REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS
21   transmittal 1 of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with
22   bit 0 set to a value of '1' and bit 1 set to a value of '1' during network entry to solicit BS transmittal of
23   NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested
24   NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The
25   identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of
26   available NSPs". After obtaining and storing the identifiers of supported NSPs, the SS SHALL restart
27   the ND&S process.

28   In the case of automatic NSP Enumeration and Selection the MS SHALL stop performing NSP Discovery with
29   other NAPs once a direct connection to the home NSP has been found.

30   ### 4.1.2.3   NSP Enumeration and Selection

31   Two WiMAX network selection modes are defined, manual and automatic.

32   The MS SHALL produce a list of available NSPs as discovered through NSP Discovery in the available NAPs, as
33   identified in NAP Discovery. The NSP Enumeration List is used for both manual and automatic selection.

34   The signal quality SHALL NOT be used as a parameter for NSP Selection.

35   #### 4.1.2.3.1 Manual Mode

36   The NSP Enumeration List SHALL be presented to the user for selection. If available, each NSP Enumeration List
37   entry SHALL present only the Verbose NSP Name to the user for selection. If more than one NAP is capable of
38   being used to establish a direct connection with a NSP, the MS MAY indicate each of the candidate NAPs along
39   with the NSP or Verbose NSP Name to the user. If displayed, NSPs or Verbose NSP Name from the list of available
40   NSPs SHALL be presented in the following order:

41   a. Home NSP;

42   b. If the "User Controlled NSP Identifier list" is available, NSPs or their corresponding Verbose NSP Names in
43   the "User Controlled NSP Identifier list" in the MS (in priority order).

44   c. If the "Operator Controlled NSP Identifier list" is available, NSPs or their corresponding Verbose NSP
45   Names in the "Operator Controlled NSP Identifier list" in the MS (in priority order).

46   d. Any other NSP or their corresponding Verbose NSP Names in random order.

47   Upon selection and successful authentication to the selected NSP, the MS SHALL indicate the Selected NSP.

1   If no NSP is found, the MS behavior is implementation dependent.

2   **4.1.2.3.2 Automatic Mode**

3   For Automatic Mode, without user intervention the MS SHALL select a NAP that has a direct connection to the
4   Home NSP. If more than one NAP is capable of being used to establish a direct connection with a NSP, the MS
5   SHOULD select a NAP by using "User Controlled NAP Identifier list" or "Operator Controlled NAP Identifier list".
6   If a NAP that has direct connection to the Home NSP is not found, then the MS SHALL attempt to select a NAP that
7   has connection to one of the NSPs in the Preferred NSPs lists. The order that the MS follows for selection from the
8   NSP Enumeration List is determined by the "User Controlled NAP Identifier list" and "Operator Controlled NAP
9   Identifier list", if available in configuration information.

10   The MS SHALL select and attempt to authenticate with an available and allowable NSP, in the following
11   precedence:

12   a.   Home NSP;

13   b.   If the "User Controlled NSP Identifier list" is available, NSPs in the "User Controlled NSP Identifier list" in
14   the MS (in priority order).

15   c.   If the "Operator Controlled NSP Identifier list" is available, NSPs in the "Operator Controlled NSP Identifier
16   list" in the MS (in priority order).

17   d.   Any other NSP in random order.

18   Upon selection and successful authentication to the selected NSP, the MS SHALL indicate the Selected NSP.

19   If no NSP is found, the MS behavior is implementation dependent.

20   **4.1.2.4   ASN Attachment**

21   Following a decision to select an NSP, an MS indicates its NSP selection by attaching to an ASN associated with the
22   selected NSP, and by providing its identity and home NSP domain in form of NAI (see section 4.4.1.3). The ASN
23   uses the realm portion of the NAI to route AAA transactions for the MS. The MS SHALL use its NAI with
24   additional information when presented (also known as decorated NAI described in IETF [3]) to influence the routing
25   choice of the next AAA hop when the home NSP realm is only reachable via another mediating realm (e.g., a visited
26   NSP).

27   The NSP identifiers received from the detected networks are 24-bit format which still need to be mapped into realms
28   of corresponding NSPs. If the "Mapping table between 24-bit NSP identifiers and NSP realm" is available in the
29   configuration information stored in the MS and the identifiers of supported NSPs received from networks are in the
30   list, then these identifiers are mapped locally.

31   If the MS does not have the realm of a visited NSP stored in the configuration information such that the MS can
32   construct a properly formatted EAP Information Request with appropriate routing decoration to influence the
33   routing choice of the next AAA hop, then the MS MAY include the Visited NSP ID TLV in the SBC-REQ message
34   to solicit BS transmittal of the Visited NSP Realm TLV in the SBC-RSP message, as specified in Std IEEE 802.16.

35   **4.1.3   Configuration Information**

36   This sub section describes the content and function of configuration information, which is stored in MS and used by
37   MS to assist network entry discovery and selection. Detailed file format of configuration in MS is out of the scope of
38   this specification.

39   Configuration information SHOULD include items as follows:

40   1) User/Operator controlled NAP Identifier list

41   •   Determining priority order of performing NSP Discovery procedure among if there are more than one
42   available NAP.

43   •   If a selected NSP MAY be reached through more than one NAP, the list is used to select a NAP in the case
44   of automatic NSP Enumeration and Selection phase.

45   •   The user controlled NAP Identifier list has higher priority than the operator controlled NAP Identifier list.

1 2) User/Operator controlled NSP Identifier list

2   • In the case of automatic NSP Enumeration and Selection mode, the lists are used to select a NSP with
3   highest priority among all available NSPs discovered during NSP Discovery phase.

4   • In the case of manual NSP Enumeration and Selection mode, the lists are used to determine the order of
5   presenting available NSPs to a user.

6   • The user controlled NSP Identifier list has higher priority than the operator controlled NSP Identifier list.

7 3) NAP/NSP mapping list

8   • Indicating the supported NSPs, with corresponding Verbose NSP Names, per NAP.

9 4) NSP Change Count

10   • Indicating whether the list of supported NSPs or Verbose NSP Names for a NAP is changed

11 5) Mapping table between 24-bit NSP identifiers and corresponding realm of the NSPs

12 6) Physical information: Information useful in NAP Discovery including channel, center frequency, and PHY
13   profile,

14 7) Security parameters: Security parameters are related to ASN attachment phase, and its definition is out of scope
15   of this sub section but may include identifying credentials that uniquely identify the user to a NSP for
16   authentication purposes.

17 8) Network deployment mode

18   • Indicating the Network deployment mode of each NAP, i.e. NAP+NSP mode or NAP sharing mode.

19 **4.1.4 SDL**

20 Figure 4-2 provides a more detailed presentation of the network entry discovery and selection process. Support of
21 the detailed method presented in the SDL is recommended, but not required.

Begin

Prior Connect Info — No → Config Info — No →

Column 1 (Prior Connect Info):

Prior Connect Info — Yes → Select & Scan Channel using Prior Connect Info

Iterate → While Connect Info Remaining

Failover

Detect Service — No → (While Connect Info Remaining)

Detect Service — Yes → Sync to DL & obtain DCD counter & NSP Change Count counter

Prior DCD counter valid — No → Wait, Scan & obtain DCD & UCD

Prior DCD counter valid — Yes → Decode DL-MAP and obtain NAP ID & BS ID

NAP ID & BS ID valid — No → (While Connect Info Remaining)

NAP ID & BS ID valid — Yes → Prior NSP Change Count valid

Prior NSP Change Count valid — No → On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List

NSP List obtained — No → RNG-REQ/RSP sequence

NSP List obtained — Yes → Visited Realm valid

Visited Realm valid — Yes → (Restart ND&S)

Visited Realm valid — No → SBC-REQ; SBC=RSP or SII-ADV with NSP list and Verbose NSP Name List → Restart ND&S

Prior NSP Change Count valid — Yes → ND&S Complete → Continue Network Entry

Column 2 (Config Info):

Config Info — Yes → Select & Scan Channel using Config Info

Iterate → While Config Info Remaining

Failover

Detect Service — No → (While Config Info Remaining)

Detect Service — Yes → Sync to DL & obtain DCD & UCD & DCD counter & NSP Change Count counter

Decode DL-MAP and obtain NAP ID

NAP ID Valid — No → (While Config Info Remaining)

NAP ID Valid — Yes → NSP Identifier Flag='0'

NSP Identifier Flag='0' — No → On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List

NSP List obtained — No → RNG-REQ/RSP sequence

NSP List obtained — Yes → Visited Realm valid

Visited Realm valid — Yes → NAP ID + NSP ID valid

Visited Realm valid — No → SBC-REQ, SBC-RSP or SII-ADV with NSP list and Verbose NSP Name List → NAP ID + NSP ID valid

NSP Identifier Flag='0' — Yes → NAP ID + NSP ID valid

NAP ID + NSP ID valid — No → (While Config Info Remaining)

NAP ID + NSP ID valid — Yes → ND&S Complete → Continue Network Entry

(Restart ND&S)

Column 3 (Scan Channel):

Scan Channel

Iterate → While Channels Remaining

Failure → ND&S Complete

Detect Service — No → (While Channels Remaining)

Detect Service — Yes → Sync to DL & obtain DCD & UCD & DCD counter & NSP Change Count counter

Decode DL-MAP and obtain NAP ID

RNG-REQ/RSP sequence

SBC-REQ/RSP or SII-ADV (with NSP list and Verbose NSP Name List if NSP Identifier Flag = '1')

NSP Identifier Flag = "0" — No → Restart ND&S

NSP Identifier Flag = "0" — Yes → Automatic NSP Select / Manual NSP Select

ND&S Complete → Continue Network Entry

1

1   **Figure 4-2 – Network Discovery and Selection SDL**

2   **4.1.4.1   Process Flow Descriptions**

3   Begin: Begin ND&S process; for instance, due to MS power-up

4   **Process for detection and selection based on stored configuration information of prior base**
5   **stations**

6   Prior Connect Info: The MS assesses the presence of stored configuration information (see section 4.1.3)

7   •   if the MS has stored configuration information of prior base stations' PHY characteristics, suitable and
8   useful for reducing the channel scanning and synchronization options, then the MS uses this information to
9   selectively search for those base stations in 'Select & Scan Channel using Prior Connect Info'

10   •   else if the MS does not have prior base stations' PHY characteristics, the MS defaults to selection and
11   detection based on more general, account subscription defined configuration information through 'Config
12   Info'

13   Select & Scan Channel using Prior Connect Info: The MS conducts channels selection and detection of available BS
14   using the stored configuration information

15   Detect Service: the MS attempts to detect a base station with the expected PHY characteristics on the tested channel

16   •   if the MS detects a base station operating with the expected PHY characteristics on the tested channel, the
17   MS proceeds to 'Sync to DL & obtain DCD counter & NSP Change Count counter''

18   •   else if the MS fails to detect a BS on the channel, and while untested channels based on the stored
19   configuration remain, the MS repeats the 'Select & Scan Channel using Prior Connect Info' process,
20   iterating to the next channel and BS for assessment; if no untested channels remain, the MS proceeds with
21   detection and selection based on 'Config Info'

22   Sync to DL & obtain DCD counter & NSP Change Count counter': The MS synchronizes to the DL transmissions
23   and obtains the DCD counter from the DL-MAP, and the NSP Change Count counter, when present, from the DCD

24   Prior DCD counter valid: The MS assesses the validity of the detected DCD counter

25   •   if the MS determines that the detected DCD counter value matches the stored, expected DCD counter
26   value, then the MS continues to 'Decode DL-MAP and obtain NAP ID & BS ID'

27   •   else if the MS determines that the detected DCD counter is different than the stored, expected DCD counter
28   value, the MS SHALL 'Wait, Scan & obtain DCD & UCD'

29   Wait, Scan & obtain DCD & UCD: For MS that detect a DCD counter different than the stored, expected DCD
30   counter value, the MS wait and listen for the transmission of the updated DCD & UCD

31   Decode DL-MAP and obtain NAP ID & BS ID: The MS listens for and decodes DL-MAP, obtaining the NAP ID
32   and the BS ID

33   NAP ID & BS ID valid: The MS tests the detected NAP ID & BS ID

34   •   if the MS determines that the detected NAP ID & BS ID matches the stored, expected values, the MS
35   continues with 'Prior NSP Change Count valid'

36   •   else if the MS determines that the detected NAP ID or BS ID does not match the stored, expected values,
37   and while untested channels based on the stored configuration remain, the MS repeats the 'Select & Scan
38   Channel using Prior Connect Info' process, iterating to the next channel and BS for assessment; if no
39   untested channels remain, the MS proceeds with detection and selection based on 'Config Info'

40   Prior NSP Change Count valid: When NSP Change Count is present in DCD, the MS tests the detected NSP Change
41   Count

42   •   if the MS determines that the detected NSP Change Count matches the stored, expected value, the MS
43   continues with 'ND&S Complete'

1   •   else if the MS determines that the detected NSP Change Count does not match the stored, expected value,
2   then the MS continues with 'On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name
3   List'

4 On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List: During a vendor specific interval
5 timer, the MS listens for the BS transmittal of the SII-ADV message with the NSP List of one or more NSP IDs and
6 Verbose NSP Names

7 NSP List obtained: The MS tests for receipt of the list of NSP IDs

8   •   if the MS obtained the list of NSP IDs, proceed to 'Visited Realm valid'

9   •   else the MS uses the SBC query process to obtain the NSP List, proceed with 'RNG-REQ/RSP sequence'

10 RNG-REQ/RSP sequence: The MS conducts RNG-REQ/RSP as defined in IEEE Std 802.16

11 SBC-REQ; SBC-RSP or SII-ADV with NSP List and Verbose NSP Name List: The MS conducts SBC-REQ
12 message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS transmittal of NSP
13 List TLV, either through an SII-ADV broadcast or SBC-RSP unicast transmission, and may include SIQ TLV with
14 bit 1 set to a value of '1' during network entry to solicit BS transmittal of Verbose NSP Name List TLV, to be
15 transmitted along with NSP List TLV; the process returns to 'NSP List obtained'

16 Visited Realm valid: If the MS requires a Realm to properly decorate an EAP Information Request, while roaming
17 to a Visited NSP

18   •   if the MS has a valid, stored Realm for the targeted Visited NSP, then the process continues to 'ND&S
19   Complete'

20   •   else the process continues to 'Restart ND&S'

21 Restart ND&S: The MS restarts the ND&S process, using the detected and stored information to expedite the ND&S
22 process

23 ND&S Complete: The MS has successfully completed the network detection and selection process and 'Continue
24 Network Entry'

25 Continue Network Entry: The MS proceeds with network entry (see section 4.5)

26 Process for detection and selection based on general, account subscription defined stored
27 configuration information

28 Connect Info: The MS assesses the presence of stored configuration information (see section 4.1.3)

29   •   if the MS has stored configuration information of base stations' PHY characteristics programmed values
30   obtained as part of the account subscription, suitable and useful for reducing the channel scanning and
31   synchronization options, then the MS uses this information to selectively search for those base stations in
32   'Select & Scan Channel using Connect Info'

33   •   else if the MS does not have prior base stations' PHY characteristics by subscription programmed values,
34   the MS defaults to selection and detection based on the physical scan capabilities of the MS device through
35   'Scan Channel'

36 Select & Scan Channel using Connect Info: The MS conducts channels selection and detection of available BS using
37 the stored configuration information

38 Detect Service: the MS attempts to detect a base station with the expected PHY characteristics on the tested channel

39   •   if the MS detects a base station operating with the expected PHY characteristics on the tested channel, the
40   MS proceeds to 'Sync to DL & obtain DCD & UCD'

41   •   else if the MS fails to detect a BS on the channel, and while untested channels based on the stored
42   configuration remain, the MS repeats the 'Select & Scan Channel using Connect Info' process, iterating to
43   the next channel and BS for assessment; if no untested channels remain, the MS proceeds with detection
44   and selection based on 'Scan Channel'

1   Sync to DL & obtain DCD & UCD & DCD counter & NSP Change Count counter:: The MS synchronizes to the DL
2   transmissions listens for the transmission of the updated DCD & UCD

3   Decode DL-MAP and obtain NAP ID: The MS listens for and decodes DL-MAP, obtaining the NAP ID

4   NAP ID valid: The MS tests the detected NAP ID

5   • if the MS determines that the detected NAP ID matches the stored, expected values, the MS continues with
6   'NSP Identifier Flag = '0''

7   • else if the MS determines that the detected NAP ID does not match the stored, expected value, and while
8   untested channels based on the stored configuration remain, the MS repeats the 'Select & Scan Channel
9   using Connect Info' process, iterating to the next channel and BS for assessment; if no untested channels
10   remain, the MS proceeds with detection and selection based on 'Scan Channel'

11 NSP Identifier Flag = '0': The MS tests for requirement for assessment of the NSP ID

12 • if the detected NSP Identifier Flag = '0' indicating that no separate NSP ID is required to completely
13   identify the network and provide adequate information for the MS to make a network selection decision,
14   then the MS continues with 'NAP ID + NSP ID valid'

15 • else if the detected NSP Identifier Flag = '1' indicating that one or more separate NSP IDs are required to
16   completely identify the network and provide adequate information for the MS to make a network selection
17   decision, then the MS continues with 'On Timer Listen for SII-ADV msg with NSP List'

18 On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List:: During a vendor specific interval
19 timer, the MS listens for the BS transmittal of the SII-ADV message with the NSP List of one or more NSP IDs and
20 Verbose NSP Names

21 NSP List obtained: The MS tests for receipt of the list of NSP IDs

22 • if the MS obtained the list of NSP IDs, proceed to 'Visited Realm valid'

23 • else the MS uses the SBC query process to obtain the NSP List, proceed with 'RNG-REQ/RSP sequence'

24 RNG-REQ/RSP sequence: The MS conducts RNG-REQ/RSP as defined in IEEE Std 802.16

25 SBC-REQ; SBC-RSP or SII-ADV with NSP list and Verbose NSP Name List:: The MS conducts SBC-REQ
26 message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS transmittal of NSP
27 List TLV, either through an SII-ADV broadcast or SBC-RSP unicast transmission, and may include SIQ TLV with
28 bit 1 set to a value of '1' during network entry to solicit BS transmittal of Verbose NSP Name List TLV, to be
29 transmitted along with NSP List TLV; the process returns to 'NSP List obtained'

30 Visited Realm valid: If the MS requires a Realm to properly decorate an EAP Information Request, while roaming
31 to a Visited NSP

32 • if the MS has a valid, stored Realm for the targeted Visited NSP, then the process continues to 'NAP ID +
33   NSP ID valid'

34 • else the process continues to 'Restart ND&S'

35 Restart ND&S: The MS restarts the ND&S process, using the detected and stored information to expedite the ND&S
36 process

37 NAP ID + NSP ID valid: The MS uses the detected NAP ID and NSP ID, comparing it to stored configuration
38 information, testing for a valid combination of NAP ID and NSP ID that will connect the MS to its home CSN for
39 authentication during network entry

40 • if the NAP ID and NSP ID detected will connect the MS to its home CSN for authentication during
41   network entry, the process proceeds to 'ND&S Complete'

42 • else while untested channels based on the stored configuration remain, the MS repeats the 'Select & Scan
43   Channel using Connect Info' process, iterating to the next channel and BS for assessment; if no untested
44   channels remain, the MS proceeds with detection and selection based on 'Scan Channel'

45 ND&S Complete: The MS has successfully completed the network detection and selection process and 'Continue
46 Network Entry'

1 Continue Network Entry: The MS proceeds with network entry (see section 4.5)

2 **Process for detection and selection based on physical scan capabilities of the MS device; not**
3 **dependent on stored configuration information**

4 Scan Channel: The MS scans all available channels, limited only by the physical scan capabilities of the MS device;
5 not dependent on stored configuration information

6 Detect Service: the MS attempts to detect a base station on the tested channel

7 • if the MS detects a base station operating on the tested channel, the MS proceeds to 'Sync to DL & obtain
8 DCD & UCD'

9 • else if the MS fails to detect a BS on the channel, and while untested channels based on the physical scan
10 capabilities of the MS device remain, the MS repeats the 'Scan Channel' process, iterating to the next
11 channel for assessment; if no untested channels remain, the MS proceeds with detection and selection based
12 on 'ND&S Complete' and a result of failure

13 Sync to DL & obtain DCD & UCD: The MS synchronizes to the DL transmissions listens for the transmission of the
14 updated DCD & UCD

15 Decode DL-MAP and obtain NAP ID: The MS listens for and decodes DL-MAP, obtaining the NAP ID

16 RNG-REQ/RSP sequence: The MS conducts RNG-REQ/RSP as defined in IEEE Std 802.16

17 SBC-REQ/RSP or SII-ADV (with NSP list and Verbose NSP Name List if NSP Indentifier Flag = '1'): The MS
18 conducts SBC-REQ; if NSP Identifier Flag = '1', then MS transmits SBC-REQ including SIQ TLV with bit 0 set to
19 a value of '1' during network entry to solicit BS transmittal of NSP List TLV, either through an SII-ADV broadcast
20 or SBC-RSP unicast transmission, and may include SIQ TLV with bit 1 set to a value of '1' during network entry to
21 solicit BS transmittal of Verbose NSP Name List TLV, to be transmitted along with NSP List TLV; depending on
22 the vendor implementation, the process proceeds with 'Automatic NSP Select' or 'Manual NSP Select'

23 NSP Identifier Flag = '0': The MS tests for requirement for assessment of the NSP ID

24 ▪ if the detected NSP Identifier Flag = '0' indicating that no separate NSP ID is required to completely
25 identify the network and provide adequate information for the MS to make a network selection decision,
26 then the MS continues with with 'Automatic NSP Select' or 'Manual NSP Select', depending on the vendor
27 implementation

28 ▪ else if the detected NSP Identifier Flag = '1' indicating that one or more separate NSP IDs are required to
29 completely identify the network and provide adequate information for the MS to make a network selection
30 decision, then the MS proceeds to 'Restart ND&S'

31 Restart ND&S: The MS restarts the ND&S process, using the detected and stored information to expedite the ND&S
32 process

33 Automatic NSP Select: The MS conducts automatic NSP selection (see section 4.1.2.3)

34 Manual NSP Select: The MS conducts manual NSP selection (see section 4.1.2.3)

35 ND&S Complete: The MS has successfully completed the network detection and selection process and 'Continue
36 Network Entry'

37 Continue Network Entry: The MS proceeds with network entry (see section 4.5)

38 ## 4.2 IPv4 Addressing

39 Functional entities and architecture for IPv4 addressing are described in Stage 2 section 7.2.1. Details on how IPv4
40 addressing is performed via DHCP, PMIP4, and CMIP4 are described in Stage 3 section 4.8. IPv6 addressing details
41 are described in Stage 3 section 4.11.

4.3 WiMAX Key Hierarchy and Distribution

The MS is assumed to be provisioned with one or more credentials. Details of provisioning mechanisms is outside the scope of this specification.

There are two types of credentials. A device credential is used for authenticating the terminal device to the network. A subscriber credential is used for authenticating the subscriber of the WiMAX access service to the network.

A device credential MAY also be used as a subscriber credential. That is possible when the subscriber is identified by the MAC address of the device. In that special case, a single credential provisioned in the device can be used for authenticating both the device and the subscriber at the same time.

Credentials may come in different forms, such as username-password pair, SIM card, X.509 certificates, etc. They may be based on a pre-shared secret key or a public-private key pair. Secret/private keys SHALL be stored securely and SHALL NOT be transported outside the device. When a pre-shared secret key is used, it is assumed that the network responsible for authentication has a copy of the same key..

The MS SHALL be authenticated by the HNSP using its subscriber credential. Additionally, the HNSP MAY perform authentication on the device credential as well. Aside from the HNSP actions, the NAP MAY perform authentication of the device credential. See section 4.4.1.1 for more details.

The MS and the network perform authentication using EAP ([6]). The EAP method selected SHALL be capable of producing MSK and EMSK (except for the EAP performed by NAP during Double EAP procedure is not required to produce EMSK).

MSK and EMSK generated from the EAP authentication are used to derive other keys (e.g., PKMv2 and Mobile IP keys).

HNSP authentication generates both the MSK and EMSK. These keys are available to the MS and the EAP authentication server in the HCSN. The MSK is also transported to the NAS in the serving ASN.

Only the MSK (not EMSK) generated from the NAP authentication is needed. This key is available to the MS, and the EAP authentication server and the NAS in the ASN.
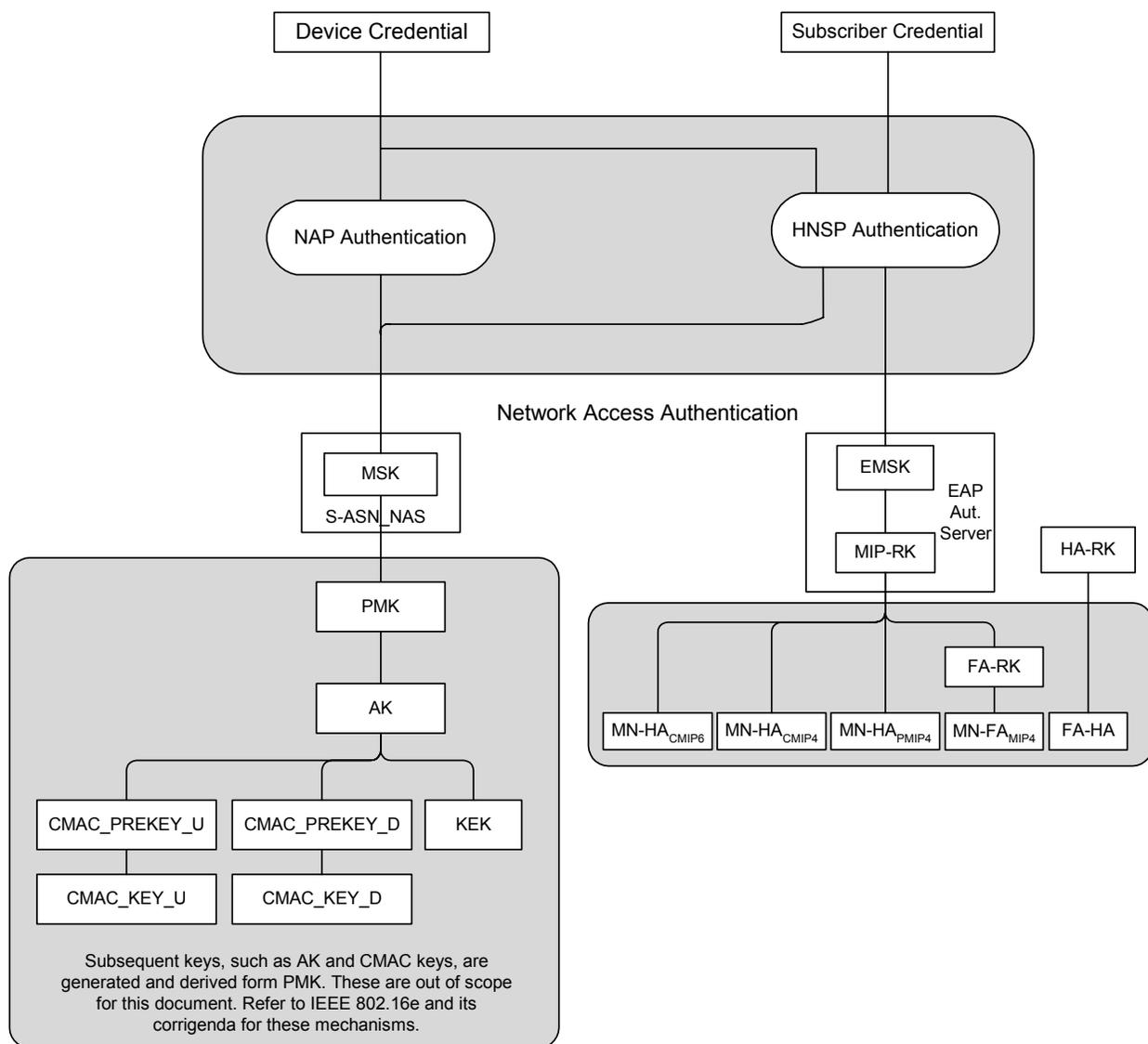
Figure 4-3 – WiMAX Key Hierarchy

3 The MS is assumed to be provisioned with the appropriate credential(s). When pre-shared secret keys are used,
4 corresponding EAP authentication servers SHALL be provisioned with the same keys.

5 The MSK(s) is transported by the AAA protocol to the NAS in the serving ASN. The MSK(s) is used to derive the
6 keys for protecting the interface between the MS and the BS (R1).

7 The EMSK stays in the EAP layer in the MS and the EAP Authentication server. The MIP-RK is derived from the
8 EMSK and is used for protecting Mobile IP signaling.

9 The HA-RK is randomly generated by the HA-assigning AAA server and transported to the NAS in the serving
10 ASN by the AAA protocol...

4.3.1   Mobile IP Root Key (MIP-RK)

12 The Mobile IP Root Key (MIP-RK) is generated at the EAP-Authentication Server which is collocated with the
13 HAAA and at the EAP-Peer located in the MS.

4.3.1.1   Key Generation

The 64 octet MIP-RK SHALL be generated from the EMSK using the following formula:

> MIP-RK-1 =   HMAC-SHA256(EMSK , usage-data | 0x01)

> MIP-RK-2 =   HMAC-SHA256(EMSK, MIP-RK-1 | usage data | 0x02)

> MIP-RK = MIP-RK-1 | MIP-RK-2

> where:

>> usage-data = key label + "\0" + length

>> key label = miprk@wimaxforum.org   in ASCII

>> length = 0x0200 the length in bits of the MIP-RK expressed as a 2 byte unsigned integer in network order

The lifetime of MIP-RK MUST be set to the lifetime of EMSK.

The MIP-RK is stored in the HAAA. At the HAAA each user session is associated with a single MIP-RK.

The MIP-RK is used to generate mobility keys (see section 4.3.5).

Security Parameter Indices required for MIP are generated from the MIP-RK as follows:

> MIP-SPI = the 4 most significant bytes of HMAC-SHA256(MIP-RK "SPI CMIP PMIP")

If the MIP-SPI value is smaller than 256, then this value SHALL be increased by 256.

In order to prevent potential collisions between values of SPI generated using this procedure, the process defined in Sec. 4.3.1.1.1 SHALL be used. Once all conditions in Sec. 4.3.1.1.1 are satisfied, e.q. all collisions with any active SPI values related to current MIP session are avoided, the new set of SPI values associated with the MIP-RK is created for this MIP session, as follows:

SPI-CMIP4 = MIP-SPI

SPI-PMIP4 = MIP-SPI + 1

SPI-CMIP6 = MIP-SPI + 2

The value of MIP-SPI + 3 is reserved for future use as SPI-PMIP6.

When the lifetime of the MIP-RK expires the lifetime of the SPIs derived from it SHALL also expire.

4.3.1.1.1   Collision Prevention for SPI Values

The following procedure prevents collision between SPI values used for different Mobility keys, for example, mobility keys used by other access technologies, during the same Mobile IP session. The procedure SHALL be executed as follows:

a.   First, if the absolute value of the difference between the MIP-SPI and any currently active SPI is less than 4, the MIP-SPI value SHALL be incremented by FOUR until the current condition is satisfied.

b.   Next, if the MIP-SPI value is less than THREE smaller than the maximum possible value of SPI (232 - 1), the MIP-SPI value SHALL be incremented by 259.

c.   Last, the process specified in Step 1 SHALL be applied again until the condition specified in Step 1 is satisfied.

The process is depicted in Figure 4-4.

1
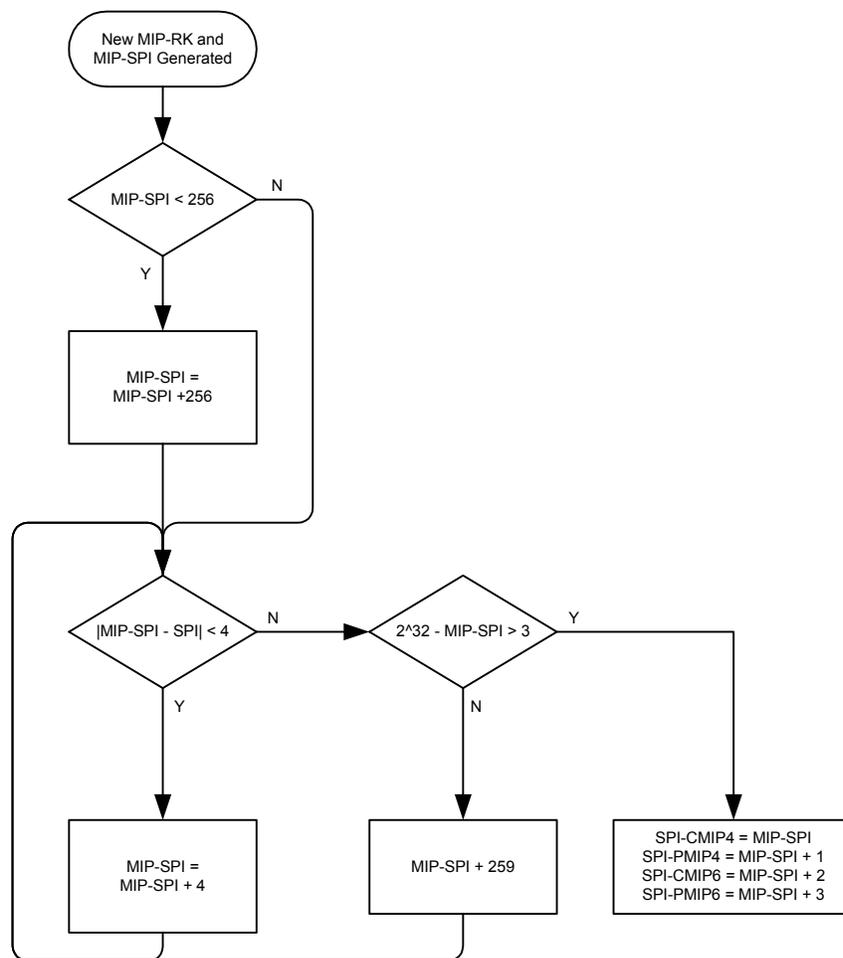
Figure 4-4 – SPI Collision Avoidance Mechanism

4.3.1.2   Key Distribution

As specified above, the MIP-RK key is derived at the MS and the HAAA at the CSN and does not get distributed outside those entities.

The SPI-CMIP4 is derived at the MS and at the HAAA at the CSN. It is used by the CMIP MS, HA, and HAAA to identify the MN-HA key used to compute the MN-HA Authentication Extension in the RRQ message. In addition, SPI-CMIP4 is distributed to the NAS during Access Authentication, in RADIUS attribute FA-RK-SPI to identify the FA-RK key. FA-RK key and FA-RK-SPI will be used to further derive MN-FA key and MN-FA-SPI as indicated in section 4.3.5.1, to compute the MN-FA Authentication Extension in the RRQ message.

The SPI-PMIP4 is derived at the HAAA at the CSN and is distributed to the Key Receiver in the NAS. It is used by the Proxy MIP Client, HA, and HAAA to identify the MN-HA key used to compute the MN-HA Authentication Extension in the Proxy MIP RRQ message.

HOME CSN
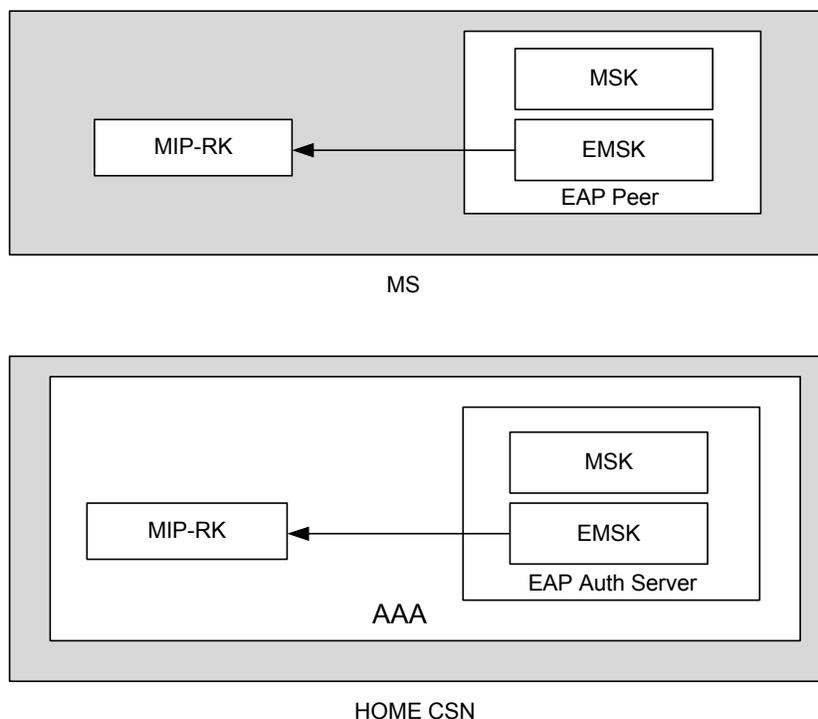
Figure 4-5 – Key Distribution

4.3.1.3 Key Deprecation

Any Mobile IP key (MIP-RK, MN-HA, FS-RK, MN-FA, HA-RK, FA-HA) SHALL be deleted before its lifetime expires.

In the case when the MS re-authenticates and a new MIP-RK is generated, old MIP-RK and its derivatives (MN-HA, MN-FA) SHALL be deprecated as soon as any one of the new keys' mutual use is successfully confirmed via a two-way signaling exchange that is signed with the new key. For example, a Mobile IPv4 registration request and response signed by the new MN-HA key derived from the new MIP-RK SHALL be used by the MN and HA to deprecate the old MN-HA key, and by the MN and HAAA to deprecate the old MIP-RK even though the key timers haven't expired yet. Similarly, two-way use of MN-FA key SHALL prompt MN and FA to deprecate the old MN-FA key.

Additionally, MIP-RK, MN-HA, and MN-FA keys SHALL be deprecated as soon as the MS session terminates (i.e., ASN generates the final RADIUS Accounting Stop).

HA-RK and FA-HA keys SHALL be deleted only after their lifetime expires.

4.3.2 AK Key

The AK key is derived from the PMK key at the NAS (MSK was transported to the NAS via the AAA infrastructure). For double-EAP based device and user authentication, the AK is derived from both keys MSK and MSK2 of the two EAP authentications. AK is derived using the method specified in [2] where PMK and EIK are generated. EIK SHALL be used to protect EAP user authentication based on the keys generated during device authentication in the double-EAP case, over R1.

4.3.2.1 Key Generation

MSK and MSK2 are each 512 bits long. PMK and PMK2 are each 160 bits long.

PMK is derived from the MSK (and MSK2 if available). The PMK and EIK derivation from the MSK during first EAP method is as follows:

```
1      EIK | PMK = truncate (MSK, 320)
```

2   The PMK2 derivation from the MSK2 during second EAP method is as follows:

```
3      PMK2 = truncate(MSK2, 160)
```

4   AK will be derived by the MS and the NAS from the PMK, and PMK2 for the double-EAP case.

```
5      If (PMK and PMK2)
6         AK = Dot16KDF ( PMK XOR PMK2, MS MAC Address | BSID |"AK", 160)
7      Else
8         AK = Dot16KDF( PMK, MS MAC Address | BSID | "AK", 160);
9      Endif
```

10   4.3.2.2   Key Lifetime

11   AK lifetime equals the MIN(PMK remaining lifetime, PMK2 remaining lifetime).

12   Before AK lifetime expires, MS SHOULD initiate EAP re-authentication.

13   AK lifetime is transferred from Authenticator to BS as part of the AK Context. After BS receives the HO-IND with
14   Resource Retain Flag set to '0', or Resource Retain Timer expires, or it receives *HO_Complete* message from
15   backbone network, BS SHALL remove the AK and its contexts even before its lifetime expires.

16   4.3.3   AK SN, PMK SN, PMK2 SN Usage and AK Context

17   4.3.3.1   Clarification of AK SN, PMK SN and PMK2 SN

18   PMK SN and PMK2 SN are 4 bit values.

19   In Single-EAP, the least significant 2 bits of PMK SN are the sequence counter, and the most significant 2 bits
20   always set to zero. AK SN is equal to the PMK SN, only the least significant 2 bits are used, the most significant 2
21   bits SHALL always set to zero.

22   In Double-EAP, the least significant 2 bits of PMK SN and PMK2 SN are the respective sequence counters, and the
23   most significant 2 bits SHALL always set to zero.

24   4.3.3.2   PMK SN and PMK2 SN Usage in Initial Authentication

25   In Single-EAP, the least significant 2 bits of PMK SN SHALL be initialized to zero

26   In Double-EAP, the least significant 2 bits of PMK SN and the least significant 2 bits of PMK2 SN SHALL be
27   initialized to zero.

28   4.3.3.3   PMK SN and PMK2 SN Usage in Re-authentication

29   In Single-EAP, when re-authentication is successfully completed, the least significant 2 bits of PMK SN SHALL be
30   incremented by 1 modulo 4.

31   In Double-EAP, when the second EAP procedure in re-authentication is successfully completed, the least significant
32   2 bits of PMK SN and PMK2 SN SHALL be incremented by 1 modulo 4 respectively.

33   4.3.3.4   AK SN Derivation from PMK SN and PMK2 SN

34   AK SN is a 4 bit value. The least significant 2 bits SHALL be used as the sequence counter in both Single EAP and
35   Double EAP.

36   In Single-EAP, AK SN SHALL equal PMK SN.

37   In Double-EAP, AK SN SHALL be derived from the least significant 2-bits of PMK2 sequence number plus the
38   least significant 2-bits of PMK sequence number modulo 4.

39   Namely, AK SN= (PMK2 SN + PMK SN) module 4.

40   Note: The AK Context is defined in Table 133a of 802.16e.

4.3.4   CMAC Keys and Replay Protection for Management Messages

The IEEE 802.16e 7.5.4.4.1 defines a condition that SHALL be satisfied in order to prevent replay of MAC management messages, that is, at any given time the combination of the CMAC Packet Number Counter (CMAC_PN_*) and associated key used to generate the CMAC digest (CMAC_KEY_*) SHALL be unique. This section describes a method that satisfies this condition.

Both CMAC_KEY_U and CMAC_KEY_D are generated from the AK. In order to ensure efficient and secure protection from replays, the fresh values of these keys are generated for each system access.

The parameter that guarantees freshness of these keys is a 16-bit counter CMAC_KEY_COUNT. Maintenance of this counter by the MS and network, as well as the simplified process flowchart, are depicted in the following subsections.

For simplicity, in this section the CMAC_KEY_COUNT is also denoted as N. The value of this count maintained by the MS is denoted as $CMAC\_KEY\_COUNT_M$ or X, the count value maintained by the BS is denoted as $CMAC\_KEY\_COUNT_B$ or Y, and the value maintained by the Anchor Authenticator is denoted as $CMAC\_KEY\_COUNT_N$ or Z.

4.3.4.1   Maintenance of CMAC_KEY_COUNT$_M$ by MS

Upon successful completion of the PKMv2 Authentication or Re-authentication, and establishment of a new PMK, the MS SHALL reset the $CMAC\_KEY\_COUNT_M$ (X) to zero. In particular, this reset SHALL occur upon reception of the SA-TEK Challenge message. Upon the $CMAC\_KEY\_COUNT_M$ reaching a value of 65535, the MS SHALL initiate re-authetication. Note, that MS SHALL manage a separate $CMAC\_KEY\_COUNT_M$ for every active PMK context. Specifically, during reauthentication, after EAP completion, but before the new PMK activation, the old $CMAC\_KEY\_COUNT_M$ (as per old PMK) is used for CMAC generation of MAC control messages, while the new $CMAC\_KEY\_COUNT_M$ (which is initialized from zero) is used for CMAC generation for PKMv2 3-way handshake messages. The old $CMAC\_KEY\_COUNT_M$ is deleted together with the old PMK context. The count of zero SHALL be used to generate the CMAC_KEY_* keys that in turn are used to authenticate that message. Also at this time, the counts in the serving BS and Authenticator SHALL be set to zero and one respectively.

For each subsequent authenticated access to the new BS (i.e., a BS that the MS does not have current/active security context with active CMAC_PN_* counters), whenever the MS sends an initial RNG-REQ message to this BS, before the MS generates the CMAC Digest for the RNG-REQ message, the MS SHALL increment the $CMAC\_KEY\_COUNT_M$ counter (X++). The MS SHALL send the value of the $CMAC\_KEY\_COUNT_M$ (X) counter in a CMAC_KEY_COUNT TLV included in RNG-REQ message.

4.3.4.1.1 CMAC_Key_Count_Lock and CMAC_Key_Count_Unlock States

When the MS decides either to reenter the network, handover to a target BS, or perform a Secure Location Update, it enters its CMAC_Key_Lock state as part of this process. While in this state, its $CMAC\_KEY\_COUNT_M$ cannot be changed.   In other words, while in the CMAC_Key_Lock state, the MS SHALL use the same value of $CMAC\_KEY\_COUNT_M$ for all RNG-REQ messages sent to other potential target BSs. When the MS decides that it is either connected to the target BS, or declines handover and remains connected to its current serving BS, it enters its CMAC_Key_Unlock state.

While in the Key Lock state, the MS SHALL cache the values of the CMAC_PN_* counters corresponding to each potential target BS to which it had sent an RNG-REQ message.

4.3.4.2   Maintenance of CMAC_KEY_COUNT by the Network

In the network, the value of the $CMAC\_KEY\_COUNT_N$ (Z) is maintained by the Anchor Authenticator. The following sub-sections specify the counter-specific processing by involved network elements.

4.3.4.2.1 Processing of CMAC_KEY_COUNT by the BS

The BS MAY possess its own AK context associated with the MS, which includes the value of $CMAC\_KEY\_COUNT_B$ (Y). This value MAY be locally maintained, or obtained from the Anchor Authenticator. The BS MAY request the AK context from the Anchor Authenticator when MS enters the BS. The Anchor Authenticator MAY pre-populate the AK context in the BS in the active set as the part of HO preparation. The BS MAY retain the AK context for some time if the MS is expected to return to or re-enter this BS. It is however

1 strongly recommended that the AK context for an inactive MS is deleted in the BS soon after the MS has exited the
2 BS.

3 Upon successful completion of the PKMv2 Authentication or Re-authentication, and establishment of a new PMK,
4 the BS SHALL reset the CMAC_KEY_COUNT$_B$ (*Y*) to zero. The BS SHALL only reset the value to zero after
5 establishment of a new PMK. In particular, this reset SHALL occur immediately prior to the transmission of the
6 SA-TEK Challenge message. Note, that BS SHALL manage a separate CMAC_KEY_COUNT$_B$ for every active
7 AK context. Specifically, during reauthentication, after EAP completion, but before the new PMK activation, the old
8 CMAC_KEY_COUNT$_B$ (as per old PMK/ AK) is used for CMAC generation of MAC control messages, while the
9 new CMAC_KEY_COUNT$_B$ (which is initialized from zero) is used for CMAC generation for PKMv2 3-way
10 handshake messages. The old CMAC_KEY_COUNT$_B$ is deleted together with the old PMK/ AK context. The
11 count of zero SHALL be used to generate the CMAC_KEY_* keys that in turn are used to authenticate that
12 message.

13 If the BS does not possess the value of CMAC_KEY_COUNT$_B$ (*Y*) as will always be the case in the Uncontrolled
14 HO, it SHALL request and receive it from the Anchor Authenticator. As an example, the BS MAY use the
15 *Context_Req* / *Context_Rpt* transaction for this purpose.

16 If the BS obtains the AK Context including the CMAC_KEY_COUNT$_N$ (Z) from the Anchor Authenticator, the BS
17 SHALL set CMAC_KEY_COUNT$_B$ = CMAC_KEY_COUNT$_N$ (Y = Z).

18 Upon receiving the RNG-REQ message from the MS containing the CMAC_KEY_COUNT TLV, the BS SHALL
19 compare the received count value CMAC_KEY_COUNT$_M$ with the CMAC_KEY_COUNT$_B$ (*X<>Y*).

20 If CMAC_KEY_COUNT$_M$ < CMAC_KEY_COUNT$_B$, and the RNG-REQ message is received as a part of reentry
21 or HO, the BS SHALL send the RNG-RSP message rejecting an access and indicating that MS SHALL conduct full
22 re-authentication.

23 If CMAC_KEY_COUNT$_M$ ≥ CMAC_KEY_COUNT$_B$, the BS SHALL do the following:

24 The BS SHALL use the CMAC_KEY_COUNT$_M$ to compute a temporary value of CMAC_KEY_U$_T$, and use the
25 CMAC_KEY_U$_T$ to validate the CMAC digest present in the RNG-REQ message.

26 If the CMAC digest is not valid, and the RNG-REQ message is received as a part of reentry, HO, or Secure Location
27 Update, the BS SHALL send the RNG-RSP message rejecting an access and indicating that MS SHALL conduct
28 full re-authentication. In addition, the BS MAY inform the Anchor Authenticator of a failed digest by using, for
29 example, the R6 *Context_Rpt* message, otherwise:

30 • If the CMAC digest is valid, and CMAC_KEY_COUNT$_M$ = CMAC_KEY_COUNT$_B$, the BS SHALL send
31   the RNG –RSP message to the MS allowing legitimate access. Once an access is completed, the BS
32   SHALL inform the Anchor Authenticator of the successful access by using, for example, the R6
33   *Context_Rpt* message.

34 • If CMAC digest is valid, and CMAC_KEY_COUNT$_M$ > CMAC_KEY_COUNT$_B$, the BS SHALL send the
35   RNG-RSP message to the MS allowing legitimate access. Once an access is completed, the BS SHALL
36   inform the Anchor Authenticator of the successful access by using for example, the R6 *Context_Rpt*
37   message and include the CMAC_KEY_COUNT$_M$ in the message.

4.3.4.2.2 Processing of CMAC_KEY_COUNT by the Anchor Authenticator

39 The Anchor Authenticator SHALL maintain the CMAC_KEY_COUNT$_N$ for every MS as part of its security
40 context, called the AK Context, and associated with the PMK. When the Anchor Authenticator for the MS is
41 relocated, and the associated AK context for the MS is deleted in the old Anchor Authenticator, the value of
42 CMAC_KEY_COUNT$_N$ is also deleted.

43 Upon successful completion of the PKMv2 Authentication or Re-authentication, and creation of a new PMK, the
44 Anchor Authenticator SHALL set the CMAC_KEY_COUNT$_N$ for the MS to 1. In particular, setting the count to 1
45 SHALL occur when the Authenticator receives indication about the successful completion of EAP-based
46 authentication. The Anchor Authenticator SHALL never set the value to zero and only reset the value to 1 after a
47 new PMK has been established.

48 Upon receiving the *Context_Req* message containg a request for the AK from the Key Receiver, the Anchor
49 Authenticator SHALL return the current value of the CMAC_KEY_COUNT$_N$ in the *Context_Rpt* message.

1 Upon receiving the indication of the successful access form the BS, for example, in the R6 *Context_Rpt* message
2 containing the $CMAC\_KEY\_COUNT_M$, the Anchor Authenticator SHALL compare it to the locally maintained
3 value of $CMAC\_KEY\_COUNT_N$ and select the largest of the two as the valid value of the count, such that

4 $$CMAC\_KEY\_COUNT_N = MAX(CMAC\_KEY\_COUNT_N, CMAC\_KEY\_COUNT_M)$$

5 in other words,

6 $$Z \ = \ MAX(\ Z, X \ )$$

7 The Anchor Authenticator SHALL then increment and retain the value of the $CMAC\_KEY\_COUNT_N$.

8 ### 4.3.4.3   Implications for Various Handover and Re-entry Scenarios

9 This section exemplifies several error case scenarios.

10 #### 4.3.4.3.1 Handover Cancellation

11 Handover Cancellation occurs before the Network Re-entry Phase. Since the Re-entry Phase has not yet happened,
12 there have been no messages between MS and the target BS, thus no CMAC_KEY_* keys based on the incremented
13 count have been used to generate message digests. Therefore, the CMAC_KEY_COUNT counters in the MS, BS,
14 and Authenticator remains un-incremented after cancellation. Operationally, none of the steps shown in the Process
15 Flowchart occurs, and replay protection based on currently active CMAC_KEY_* and CMAC_PN_* is in effect.

16 #### 4.3.4.3.2 Handover Failure

17 If the Network Re-Entry Phase proceeds partially, that is if the MS sends the RNG-REQ message but this message is
18 not received by the target BS, and therefore, the MS $CMAC\_KEY\_COUNT_M(X)$ is incremented to $(N + 1)$, but the
19 Authenticator's count (Z) remains un-incremented at $(N + 1)$. The MS would then presumably resume
20 communications with the serving BS and will just continue its CMAC_PN_* counters where they left off. The MS
21 will continue using the same CMAC_KEY_* keys that had been derived from the prior counter value of N, even
22 though its MS $CMAC\_KEY\_COUNT_M$ counter has been incremented.

23 However, during the next (successful) reentry, HO, or secure location update, the MS will again increment its
24 counter (X), this time to $(N + 2)$, but the target BS during the HO preparation phase will have its counter (Y) set to
25 $(N + 1)$ by the Authenticator. Nonetheless, when the target BS receives the RNG-REQ message, it will detect the
26 out-of-sync condition and set its counter to the value contained in that message, namely $(N + 2)$. It will then inform
27 the Authenticator of this new value and the Authenticator will re-sync its $CMAC\_KEY\_COUNT_N$ accordingly. So,
28 there is no negative impact, delay or otherwise, from this particular type of failure.

29 ### 4.3.4.4   Process Flowchart

30 This section shows a simplified process flowchart for reentry, handover, or Secure Location Update.
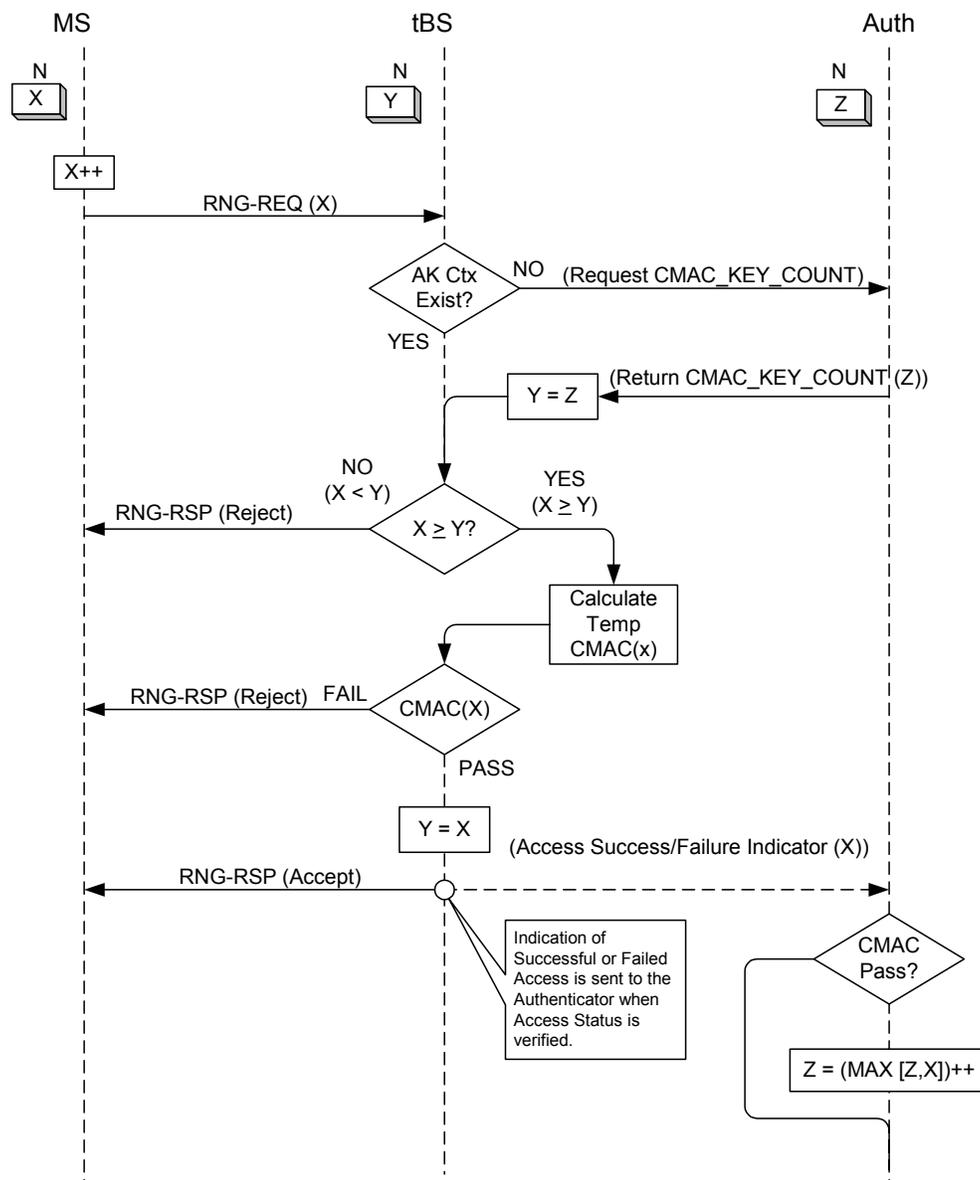
2   **Figure 4-6 – Replay Protection for Reentry, Handover, and Secure Location Update**

3   **4.3.5   MIP Keys**

4   MIP Keys used for Mobility Authentication are generated from the MIP-RK. These include keys for CMIP4, PMIP4
5   and CMIP6. The MIP keys are generated at the HAAA and at the MS. The keys generated at the HAAA are
6   transported to the HA, the Authenticator, and the PMIP client by the use of the AAA protocol when this is required.
7   Keys generated at the MS are not distributed.

8   **4.3.5.1   Key Generation**

9   The keys are generated as necessary from the MIP-RK. During Mobile IP re-registration (registration caused during
10   registration lifetime expiration) the mobility keys are not themselves refreshed.

11   When EAP-Re-authentication occurs, a new MIP-RK is generated, including the derived MN-HA and FA-RK
12   mobility keys.

1 The derivation of mobility keys are given below:

```
2    MN-HA-CMIP4 = H(MIP-RK,"CMIP4 MN HA" │ HA-IPv4 │ MN-NAI)
3    MN-HA-PMIP4 = H(MIP-RK,"PMIP4 MN HA" │ HA-IPv4 │ MN-NAI)
4    MN-HA-CMIP6 = H(MIP-RK,"CMIP6 MN HA" │ HA-IPv6 │ MN-NAI)
```

5 "During initial network entry, the MN may not know the HA-IPv4 address of the home agent it will be connected to,
6 and could use either ALL-ZERO-ONE-ADDR or a particular HA IPv4 address in its requested RRQ. Under this
7 case, the MN SHALL derive the MN-HA-CMIP4 key using that particular IPv4 address as the HA-IPv4 address in
8 the above formula and use this key for MN-HA authentication extension in the RRQ it sends to the FA. Once a RRP
9 with the success code is received from the FA, the MN SHALL recalculate the MN-HA-CMIP4 key using the HA
10 address in the Home Agent field and use this key for MN-HA authentication extension validation for the RRP. If the
11 MN-HA authentication extension is valid, the new MN-HA-CMIP4 key SHALL be in effect and the HA address in
12 the Home Agent field SHALL be taken as the assigned HA-IPv4 address."

13 As MN roams from one FA to another, its security association with HA stays unchanged, and therefore is bound
14 only to the HA-IP. MIP-RK is not known to the FA, and so FA is not capable of computing the MN-HA key.

15 The lifetime of all MN-HA keys SHALL be set to the lifetime of the MIP-RK.

16 The SPI values associated with MN-HA keys are generated at the time of generating MIP-RK, as specified in
17 section 4.3.1.1.

18 The derivation of FA-RK and MN-FA mobility keys are given below:

```
19    FA-RK = H(MIP-RK,"FA-RK")
20    MN-FA = H(FA-RK,"MN FA" │ FA-IP │ MN-NAI)
```

21 The FA-RK is generated by the HAAA and distributed to the authenticator as specified in section 4.3.5.2. It is used
22 by the authenticator to derive MN-FA keys as requested by the FA. If a handover to a new FA takes place without
23 re-authentication, the anchor authenticator holding the FA-RK is responsible to generate and provision MN-FA to
24 the new FA on request. The MN-FA key is derived based on the FA-IP address to separate keys between different
25 FAs for the same authentication session. The lifetime of FA-RK and MN-FA SHALL be set to the lifetime of the
26 MIP-RK.

27 The SPI associated with the MN-FA (MN-FA-SPI) is set to the same value of FA-RK-SPI distributed during Access
28 Authentication as in section 4.3.1.2.

29 The HA-RK and its context is created by the AAA server assigning the HA to an authenticating subscriber. The
30 context includes its SPI and lifetime. A different 160-bit random HA-RK is created for every HA.

```
31    FA-HA = H(HA-RK, "FA-HA" │ HA-IPv4 │ FA-CoAv4 │ SPI)
```

32 The SPI for any FA-HA key SHALL be set to the SPI of the HA-RK it is derived from.

33 The HA-RK is generated by the AAA server. It is distributed to the authenticator and to the HA as specified in
34 section 4.3.5.2 to derive FA-HA keys. A FA-HA key is generated by the authenticator for a specific FA-HA pair if
35 requested by this FA.

36 In contrast to FA-RK, the HA-RK and derived FA-HA keys do not depend on a MIP-RK generated as result of a
37 specific EAP authentication. Hence, they are not bound to individual user or authentication sessions, but to
38 Authenticator-AAA or FA-HA pairs, respectively. HA-RK and FA-HA keys are only generated on demand, but not
39 for each EAP (re-)authentication or MIP registration taking place. Nevertheless, HA-RK key along with the SPI and
40 lifetime values are delivered to the authenticator during network access authentication of a MS (i.e., it is
41 piggybacked). The lifetime and SPI of HA-RK is managed by the AAA server assigning the HA. It is the
42 responsibility of the HAAA to generate and deliver a new HA-RK to the authenticator prior to the expiration of the
43 HA-RK. During any EAP authentication procedure, if AAA finds that the remaining lifetime of HA-RK is less than
44 the new MSK lifetime assigned, Access-Accept message shall contain a new HA-RK and its context. AAA servers
45 shall make sure that HA-RK lifetime is longer than MSK lifetime. The same SPI value is used symmetrically (i.e.,
46 both in MIP RRQs and MIP RRPs).

H()	HMAC-SHA1 [5]
HA-IPv4	IP address expressed as a 32-bit value of the HA as seen from the FA and as reported in the

	Mobile messages.
FA_CoAv4	Address of the FA expressed as a 32-bit value as seen by the HA.
FA-IPv4	Address of the FA expressed as a 32-bit value as seen by the MS.
HA-IPv6	IPv6 address expressed as a 128-bit value of the HA as seen from the MN and as reported in the Mobile messages.
MN-NAI	User NAI provided in the MIP Registration Request

1   The lengths of the resulting keys are 160-bits.

2   **4.3.5.2   Key Distribution**

3   Table 4-2 describes where the mobility keys are generated and where they are transported.

4   **Table 4-2 – Mobility Keys Generation and Usage**

Key	Generated by	Used at
MN-HA-CMIP4	MN and HAAA	HA and MN
MN-HA-PMIP4	MN and HAAA	HA and PMIP4 client
MN-HA- CMIP6	MN and HAAA	MN and HA
FA-RK	MN and HAAA	MN and Authenticator
MN-FA	MN and Authenticator	FA and MN or PMIP4 client
HA-RK	HAAA	HA and Authenticator
FA-HA	HA and Authenticator	HA and FA

5   The keys that are used by the MN are generated by the MN and SHALL NOT be transported outside the MN. The
6   keys generated by the HAAA are transported to the HA or the Authenticator using RADIUS.

7   **4.3.5.2.1   Key Distribution for CMIP4**

8   In this section, key distribution for CMIP4 is described. This covers two scenarios, where in the first scenario
9   authenticator and FA are co-located and in the case of FA relocation, also the authenticator changes based on EAP
10   re-authentication. In the second scenario, no re-authentication takes place when the FA is relocated, so the anchor
11   authenticator is continued to be used, and provisions the new FA with the required mobility keys.

12   Figure 4-7 illustrates the key distribution for CMIP4.

1
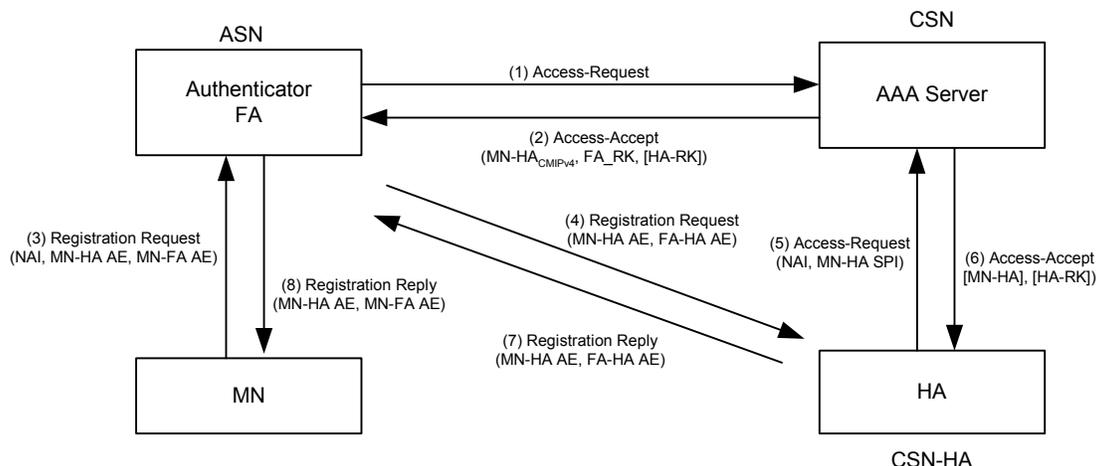
2 **Figure 4-7 – CMIP4 Key Distribution without FA relocation**

3   Note: Figure 4-7 uses the Mobile IP authentication extensions (AE) as examples. For information whether an AE
4   is M/O for a specific message, refer to section 4.8.

5 For CMIP, the MIPv4 Client resides in the MS and the FA resides in the ASN. The location of the HA is shown
6 such that it could be in the home network (in which case the AAA broker does not exists) or in a visited CSN in
7 which case there could be one or more AAA brokers between it and the HAAA server though it is not shown in
8 Figure 4-7.

9 The MIPv4 Client in the MS receives the MN-FA and MN-HA-CMIP4 keys along with the SPIs and lifetimes that
10 were generated by the MS from the MIP-RK key during EAP based Device/User Authentication.

11 The following key distribution scheme applies:

12 The authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept message as a result
13 of successful authentication. These include FA-RK, and HA-RK (with its SPI and lifetime). MN-HA-CMIP4
14 SHALL NOT be sent to the authenticator by the HAAA. The keys are transported over RADIUS and are encrypted
15 using the method defined in [36] section 3.5. The RADIUS message MAY be transported through zero or more
16 AAA brokers or proxies. The keys are stored at the authenticator.

17 At the time of CMIP4 procedures, the FA obtains the MN-FA key and, if required, the FA-HA key it needs from the
18 authenticator. If this is a new FA after re-location without re-authentication, the new FA receives the keys as part of
19 the *Context_Req* and *Context_Rpt* exchange with the anchor authenticator, as indicated in section 4.7. The
20 authenticator derives MN-FA from FA-RK and, if required, FA-HA from HA-RK according to the procedures given
21 in section 4.3.5.1.

1
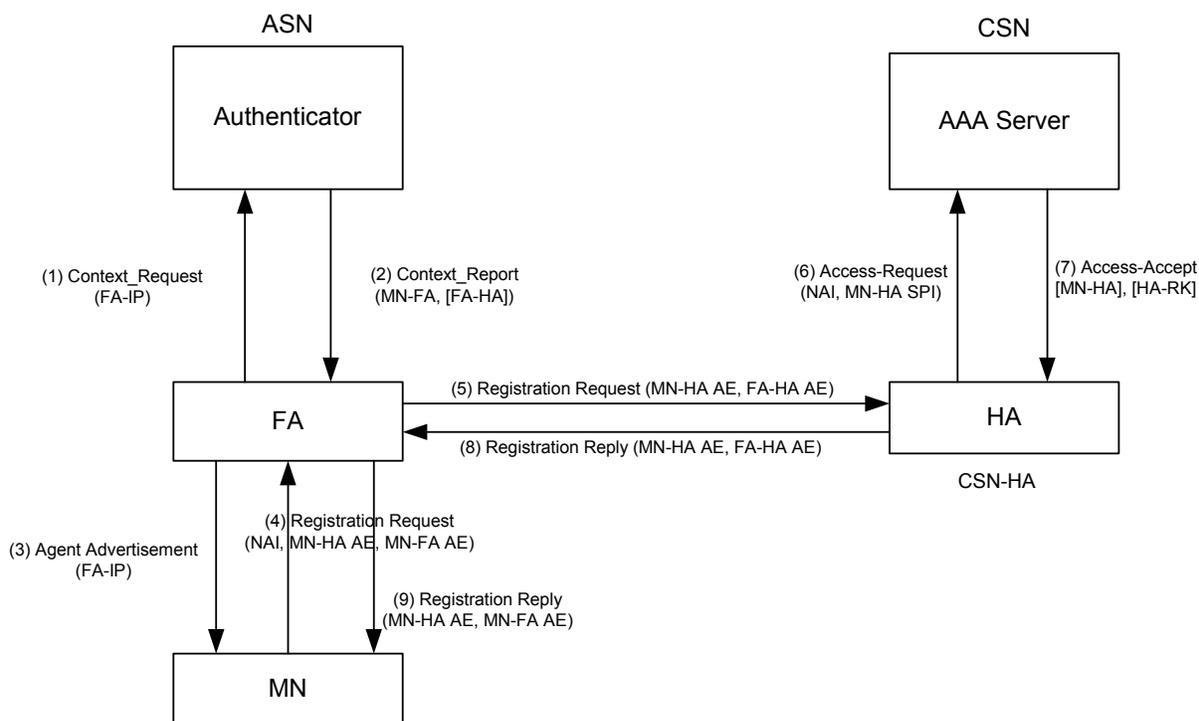
2

3 **Figure 4-8 – CMIP4 Key Distribution with FA Relocation**

4 The HAAA distributes the MN-HA key and the HA-RK key, if requested, to the HA using RADIUS Access-Accept.
5 For MN-HA, the HAAA sends the MN-HA-CMIP4 key to the HA when the SPI used in the MIP Registration
6 Request is associated with CMIP MN-HA key (equal to SPI-CMIP4). The HA requests and uses these keys for
7 verification of MN-HA AE and FA-HA AE according to the procedures described in section 4.8. Any new FA-HA
8 key is derived in the HA from HA-RK according to the procedures given in section 4.3.5.1.

9 **4.3.5.2.2 Key Distribution for PMIP4**

10 In this section, key distribution for PMIP4 is described. As for CMIP4 distribution, this covers two scenarios, where
11 in the first scenario authenticator and FA are co-located and in the case of FA relocation, also the authenticator
12 changes based on EAP re-authentication. In the second scenario, no re-authentication takes place when the FA is
13 relocated, so the anchor authenticator is continued to be used, and provisions the new FA with the required mobility
14 keys.

15 Figure 4-9 illustrates the key distribution for PMIP4 operations.

1
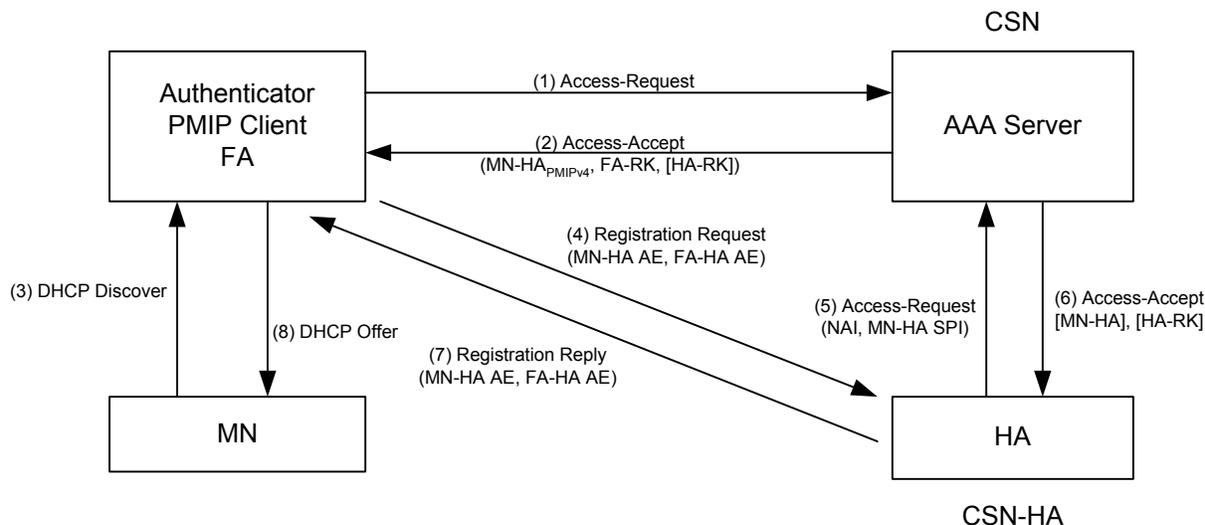
2   **Figure 4-9 – PMIP4 Key Distribution**

3   Note: Figure 4-9 uses the Mobile IP authentication extensions (AE) as examples. For information whether an AE
4   is M/O for a specific message, please refer to section 4.8.

5   For PMIP, the PMIP4 client and the FA reside in the ASN. The location of the HA is shown such that it could be in
6   the home network (in which case the AAA broker does not exists) or in a visited CSN in which case there could be
7   one or more AAA brokers between it and the HAAA server though it is not shown in Figure 4-9.

8   The PMIP4 client receives the MN-FA and MN-HA-PMIP4 keys along with the SPIs and lifetimes from the
9   Authenticator.

10   The following key distribution scheme applies:

11   The authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept message as a result
12   of successful authentication. These include MN-HA-PMIP4 , SPI-PMIP4 , FA-RK, and HA-RK (with its SPI and
13   lifetime).

14   At the time of PMIP4 procedures, the PMIP4 client obtains the MN-FA and MN-HA_PMIP4 keys, as well as the
15   SPI-PMIP4 , from the authenticator, and the FA obtains the MN-FA key and, if required, the FA-HA key from the
16   authenticator. If this is a new FA after re -location without re-authentication, the new FA receives the keys from the
17   anchor authenticator for PMIP4. The authenticator derives MN-FA from FA-RK and, if required, FA-HA from HA-
18   RK according to the procedures given in section 4.3.5.1.

19   The HAAA distributes the MN-HA key, associated SPI, and the HA-RK key, if requested, to the HA using RADIUS
20   Access-Accept. For MN-HA, the HAAA sends the MN-HA-CMIP4 key to the HA when the SPI used in the MIP
21   Registration Request is associated with CMIP4 MN-HA key (SPI = SPI-CMIP). A SPI value equal to SPI-PMIP4
22   indicates the MS is using PMIP, hence MN-HA-PMIP4 key is sent to the HA by the HAAA. The HA requests and
23   uses these keys for verification of MN-HA AE and FA-HA AE according to the procedures described in section 4.8.
24   Any new FA-HA key is derived in the HA from HA-RK according to the procedures given in section 4.3.5.1.

25   Upon HA-RK expiry, the procedures specified in section 4.8 SHALL apply.

26   **4.3.5.2.3 Key Distribution for CMIP6**

27   During Device/User authentication the MS and the Home AAA server derive the MIP-RK key from the EMSK key
28   resulting from the successful EAP authentication. Both the MS and HAAA compute the MN-HA- CMIP6 key and
29   store it. MN-HA- CMIP6 SHALL NOT be sent to the Authenticator by the HAAA.

30   When the MIP6-Client in the MS commences MIP6 procedures it obtains the MN-HA- CMIP6 key. It uses this key
31   to authenticate the Binding Update packet as defined by [21].

1 When the HA receives a Binding Update for which it does not have a security association, it sends an RADIUS
2 Access-Request to fetch the MN-HA key, to the HAAA. The HAAA provides the key to the HA in an Access-
3 Accept packet where the Key is encrypted using the procedures defined in [36] section 3.5. The RADIUS messages
4 MAY be transported between the HA and the HAAA via one or more AAA Brokers or proxies.

5 ### 4.3.5.3   Key Lifetime

6 Lifetime of EMSK, MSK and derived keys such as MIP-RK are the same.

7 MN-HA key lifetime is same as that of MIP-RK. The lifetime is transferred from Home AAA to Authenticator with
8 Session-Timeout Attribute which is specified in section 5.4 When MN-HA key is transferred, its lifetime SHOULD
9 be transferred as well.

10 The MN-HA key lifetime ends even before MIP-RK lifetime expires if MS and Home AAA perform EAP re-
11 authentication successfully. When the MN-HA key is recomputed a new SPI is associated with the MN-HA key, this
12 allows entities to detect that the key has changed.

13 The lifetime of FA-RK (FA Root Key) and its scope is same as that of MIP-RK.

14 MN-FA key lifetime has same scope of FA-RK key lifetime.

15 FA-HA key lifetime of FA is the remaining lifetime of HA-RK. The lifetime of the HA-RK is operator specific.

16 When MS moves to another FA, the FA SHALL remove FA-HA key and its context even before FA-HA key
17 lifetime does not expire.

18 ## 4.3.6   DHCP keys

19 DHCP keys used to secure the DHCP messages between the DHCP relay and DHCP server are generated from the
20 DHCP-RK. The DHCP-RK key generation is internal to the AAA server and is transported as necessary to the
21 authenticator and DHCP server using AAA protocol. From the DHCP-RK additional DHCP keys are derived which
22 are specific for each (DHCP Relay, DHCP server) pair and these keys are used to protect the DHCP messages
23 exchanged between the DHCP relays and the DHCP server.

24 In contrast to MIP-RK, the DHCP-RK and keys derived from it do not depend on a MSK or EMSK generated as
25 result of a specific EAP authentication. Hence, DHCP-RK and derived keys are not bound to individual user or
26 authentication sessions, but to a specific DHCP server and (DHCP relay, DHCP server) pairs. DHCP-RK is
27 generated only on demand, but not for each EAP (re-)authentication taking place. Nevertheless, DHCP-RK key
28 along with the key identifier and lifetime values are delivered to the authenticator during network access
29 authentication of a MS (i.e., it is piggybacked but otherwise unrelated to this specific MS). The lifetime and key
30 identifier of DHCP-RK is managed by the AAA server. It is the responsibility of the AAA server to deliver a new
31 DHCP-RK to the authenticator prior to the expiration of the DHCP-RK.

32 ### 4.3.6.1   Key Generation

33 The DHCP-RK is created by the AAA server assigning the DHCP server to an authenticating subscriber. A different
34 160-bit random DHCP-RK is generated for every DHCP server.

35 The AAA server also generates a key identifier and associates it with the DHCP-RK. Key identifier is defined in
36 [31]. Key identifier is unique within the scope of the single DHCP server. If several DHCP-RKs exist for a single
37 DHCP server at the same time, they SHALL have different key identifiers. DHCP-RKs belonging to different
38 DHCP servers may use the same key identifier. Apart from these constraints, the key identifier generation is internal
39 to the AAA server. The size of the DHCP-RK is 160 bits.

40 From the DHCP-RK an authenticator generates DHCP-key for a specific (DHCP Relay, DHCP Server) pair if
41 requested by this DHCP relay. The DHCP-key is also generated by the DHCP server when a DHCP message arrives
42 from a DHCP relay for which the DHCP server has no key yet.

43   DHCP-key = HMAC-SHA1(DHCP-RK, "DHCP AUTH" | DHCP-Relay-IP | DHCP-Server-IP)

44 The size of the DHCP key is 160 bits.

1 ### 4.3.6.2   Key Distribution

2 In this section, DHCP key distribution is described. Table 4-3 describes where the DHCP keys are generated and
3 where they are transported.

4 **Table 4-3 – DHCP Keys Generation and Usage**

Key	Generated by	Used at
DHCP-RK	AAA	Authenticator and DHCP server
DHCP key	Authenticator and DHCP server	DHCP relay and DHCP server

5 The keys generated by the AAA server are transported to the DHCP server or the Authenticator using the AAA
6 protocol. The keys generated by the authenticator are transported to the DHCP relay via WiMAX specific R4
7 signaling. The keys generated by the DHCP server are never transported outside of the DHCP server.

8 DHCP key distribution covers two scenarios. In the first scenario the authenticator and DHCP relay are co-located in
9 the same entity. In the second scenario, no re-authentication takes place when the MS moves to a different anchor
10 ASN hosting a new DHCP relay, so the anchor authenticator is continued to be used, and provisions the new DHCP
11 relay with the required keys.

12 Figure 4-10 describes the distribution of DHCP keys for the case when the DHCP relay is collocated with
13 authenticator:

14
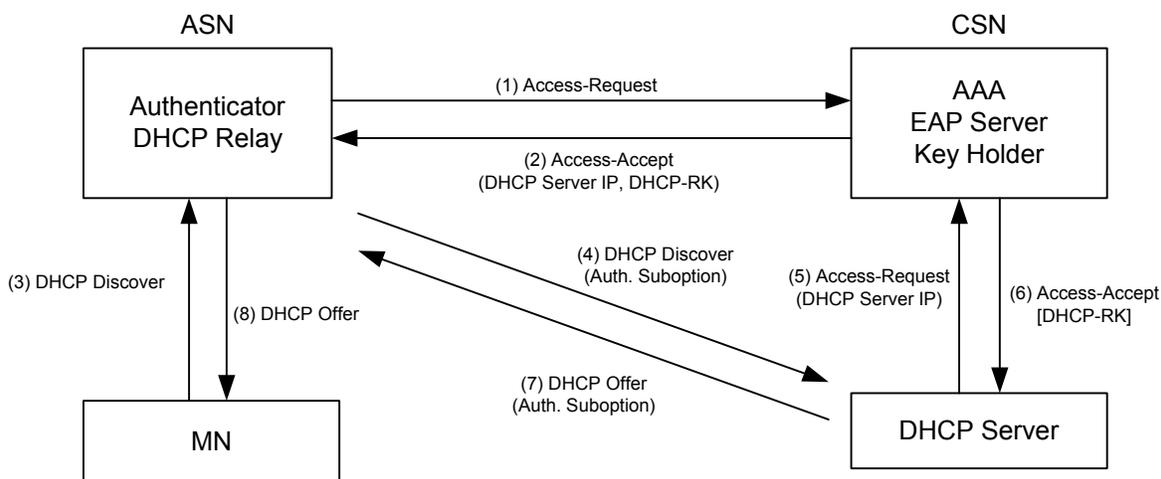
15 **Figure 4-10 – Initial DHCP Key Distribution**

16 The authenticator receives a DHCP server address and the DHCP-RK in the RADIUS Access-Accept message as a
17 result of successful subscriber authentication. In case several DHCP-RKs associated with the DHCP server are
18 available at the AAA server, the AAA server should include the DHCP-RK with the longest remaining lifetime in
19 the Access-Accept message. Besides DHCP-RK, the Access-Accept message contains also the lifetime and key
20 identifier of the DHCP-RK. The DHCP-RK is transported over RADIUS and is encrypted using the method defined
21 in [36] section 3.5. The RADIUS message MAY be transported through zero or more AAA brokers or proxies. The
22 keys are stored in the Key-holder in the authenticator at the ASN.

23 At the time of DHCP procedures, the DHCP relay obtains the derived DHCP key from the Key-holder at the
24 authenticator. The Key-holder derives the DHCP key specific to the requesting DHCP relay from the DHCP-RK, as
25 described in 4.3.6.1 and delivers the derived key, its lifetime and the key identifier associated with the DHCP-RK to
26 the DHCP relay. DHCP relay uses the received DHCP key to compute the authentication suboption as per [31] and
27 includes the suboption in the relayed DHCP message. When the DHCP server receives a message with
28 authentication suboption, it searches for the corresponding DHCP key in its local cache by DHCP relay address and
29 received key identifier. If the corresponding key is not found, the DHCP server derives a new DHCP key specific to

1 this DHCP relay from the DHCP-RK. It uses the received key identifier to select the right DHCP-
2 RK. If no DHCP-RK is found that is associated with the received key identifier, the DHCP server acquires the DHCP-RK from the
3 AAA server in the same way as the HA acquires the HA-RK, as described in section 4.8.4.2.1. The DHCP server
4 SHALL include the received key identifier in the Access-Request message. This will enable the AAA server to
5 select the right DHCP-RK in case several DHCP-RKs are available for this particular DHCP server at the AAA
6 server. If the key identifier is not known to the AAA server, the AAA server SHALL respond with the AccessReject
7 message. Having acquired the DHCP-RK, the DHCP server derives the DHCP-key specific to the DHCP relay and
8 stores it in its local cache. The lifetime of the derived key is limited to the lifetime of the DHCP-RK. DHCP server
9 then uses the derived DHCP key to verify the authentication suboption as per [31]. In case the verification fails, or if
10 AAA server responded with AccessReject, the DHCP server SHALL drop the incoming message, as per [31].

11 The DHCP server SHALL provide the DHCP response message with the authentication suboption, as per [31].

12 Figure 4-11 describes the distribution of DHCP keys for the case when the DHCP relay and authenticator are not
13 collocated:
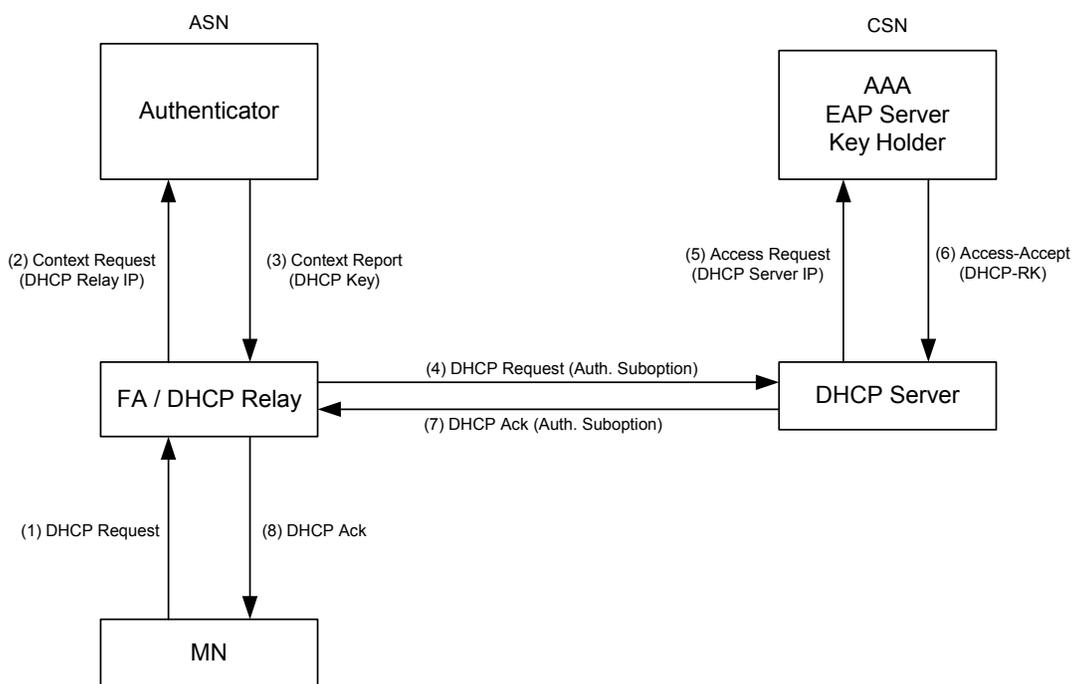
14

15 **Figure 4-11 – DHCP Key Distribution when Authenticator and DHCP Relay are not Collocated**

16 When the DHCP relay intercepts a DHCP message from the MS, it SHALL provide it with authentication
17 suboption, as per [31]. If the key corresponding to the DHCP server of the MS is not available at the DHCP relay,
18 the DHCP relay will request a key from the authenticator by sending the *Context_Req* message containing the
19 DHCP relay IP address TLV an empty DHCP-key TLV. The DHCP relay address included in the *Context_Req*
20 message SHALL be the same address that the DHCP relay will put into the giaddr field when relaying the DHCP
21 message to the server. The authenticator will derive the necessary key, as described in 4.3.6.1 and deliver the
22 derived key, its lifetime and the key identifier associated with the DHCP-RK to the DHCP relay in *Context_Rpt*
23 message. Having acquired the DHCP key, the DHCP relay proceed as described above in the scenario when the
24 DHCP relay and authenticator are collocated.

4.4 Authentication, Authorization and Accounting

4.4.1 Network Access Authentication and Authorization

27 Network access authentication is used for authorizing the MS to receive the WiMAX access service. The procedure
28 involves authentication of subscriber and optionally device credentials.

1   The functional blocks that are involved in the authentication procedure are presented below.

2   **Table 4-4 – Functional Blocks for Device/User Authentication**

Entity	Function
MS	Acts as the EAP peer.
NAS	Consists of the EAP authenticator and is the receiver of service authorization attributes. It resides in the ASN. For certificate-based device authentication terminating in the ASN, the NAS contains an EAP authentication server.
VAAA	The AAA proxy that resides in the VCSN.
HAAA	The AAA server resides in the HCSN. The EAP authentication server typically resides within this AAA server. The AAA server has access to the user profiles and is also involved in the authentication of the mobility operations.

3   Other AAA proxies such as those in broker networks are not considered. It is assumed that broker proxies are trusted
4   and act in a pass-through fashion and do not modify the RADIUS packets other than modifications made for routing
5   purposes.

6   After successful network access authentication, the HAAA delivers authorization attributes to the NAS. Since the
7   design goal is to reduce the number of AAA transactions, the HAAA delivers all possible attributes to the NAS. For
8   example, the HAAA will deliver attributes required for PMIP4 operations without knowing whether PMIP4 will be
9   invoked.

10   ### 4.4.1.1   Network Access Authentication Model

11   Network access authentication procedure consists of two parts: Optional NAP authentication, and mandatory HNSP
12   authentication.

13   The NAP MAY have a policy that requires authentication of the device credential. In that case, the NAP forces the
14   MS to perform Double EAP through SBC negotiation [2]. The first EAP authentication of Double EAP is used by
15   the NAP for device credential verification. Whether to perform the NAP authentication only during initial network
16   entry or also for all subsequent re-authentications is a matter of NAP policy.

17   The HNSP always performs authentication to verify the subscriber credential. While doing so, the HNSP MAY also
18   require verification of device credential. HNSP policy determines when to perform the latter (e.g., during initial
19   network entry, or also for each re-authentication, etc.) If the subscriber and device credentials are distinct and both
20   need to be authenticated, either a tunneling EAP method (e.g., EAP-TTLS) or credential combining (see section
21   4.4.1.4.1.3.2) is used.

22   When both the NAP and HNSP authentications need to be performed, Double EAP procedure is used. The first EAP
23   of Double EAP is used for the NAP authentication, and the second EAP for the HNSP authentication. When only
24   HNSP authentication is performed, Single EAP procedure is used.

25   Each EAP authentication involves executing an EAP method (e.g., EAP-TLS, EAP-TTLS, EAP-AKA, etc.). The
26   EAP method and the associated credential selection is a deployment decision. Mandatory to implement methods are
27   described in Section 4.4.1.2. The MS and the EAP authentication server uses [6] EAP method negotiation to
28   dynamically select a method during network access authentication..

29

30

31   ### 4.4.1.2   EAP Methods

32   For device authentication based on X.509 certificates, MS SHALL support EAP-TLS, as outlined in [17].

33   For user authentication, MS SHALL support at least one of EAP-AKA [18] or EAP-TTLS [19].

4.4.1.2.1 EAP-TLS

Whether performing device authentication using EAP-TLS is up to operator policy.

Username of the NAI presented in EAP-Response/Identity SHALL be the MAC Address of the device. It is expressed as six pairs of hexadecimal digits, e.g., "006021A50A23." The Alpha HEX characters (A-F) SHALL be expressed as uppercase letters.

MS and network SHALL support the fragementation function described in the section 3.3 of [17]. The MTU size of EAP-TLS fragementation SHALL be 1400 Bytes to avoid unnessary additional fragmentation over the path between the peer and the server.

Note that [17] does not specifically name the MSK and the EMSK (this is being addressed now by the IETF). The MSK and EMSK SHALL be derived as per the following formulas:

MSK(0,63)   = TLS-PRF-64(master secret, "client EAP encryption", random)

EMSK(0,63) = second 64 octets of: TLS-PRF-128(master secret, "client EAP encryption",random).

Where: random = client.random || server.random

4.4.1.2.2 EAP-AKA

When EAP-AKA is used for user authentication, MS SHALL support the full authentication procedure described in [18]. When EAP-AKA is used, the subscriber credential SHALL be used in generation of authentication vectors defined in [18]. Cryptographic functions used in EAP-AKA protocol are outside scope of this specification.

4.4.1.2.3 EAP-TTLS

When it is used, the MS and AAA SHALL support TTLS version 0 [19] and MS-CHAPv2 [20] as a tunneled authentication protocol. When EAP-TTLS is used, the subscriber credential SHALL be the identifier and password used for MSCHAPv2. Although support for the MSCHAPv2 is mandated, its use is not mandated and other inner methods are allowed.

The MS and the AAA SHALL support the fragmentation function described in the section 3.3 of [17]. The MTU size of EAP-TLS fragementation SHALL be 1400 Bytes to avoid unnessary additional fragmentation over the path between the peer and the server.

The MSK and the EMSK which are used in this document are generated by the formula described in the section 7 of [19][. Note that [19] does not specifically name the MSK and the EMSK (this is being addressed now by the IETF). The MSK and EMSK SHALL be derived as per the following formulas:

MSK(0,63)   = TLS-PRF-64(SecurityParameter.master secret, "ttls keying material", random)

EMSK(0,63) = second 64 octets of: TLS-PRF-128(SecurityParameter.master secret, "ttls keying material ",random).

Where: random = SecurityParameters.client_random || SecurityParameters.server_random

4.4.1.3   Network Access Identifier

The network access identifier used SHALL conform to [3]. In EAP there are two instances where the subscriber /device identity is to be specified. The first time identity is specified when the mobile responds to the EAP-Request Identity message. This identity is known as the outer-identity and as recommended by [7] and section 5.1 of [9], this identity SHOULD be used to primarily to route the packet and act as a hint helping the EAP authentication server select the appropriate EAP method. The outer-identity is used to populate the User-Name attribute of the RADIUS access-request message.

The EAP methods also provide an identity called the inner-identity. This inner identity SHOULD be used to identify the subscriber/device identity. EAP methods that provide identity hiding will transmit the inner-identity within an encrypted tunnel created by the EAP method.

In order to support identity hiding the real identity of the MS SHALL be carried in the EAP method itself (inner-identity).

4.4.1.3.1 Outer-Identity

In EAP the outer identity refers to the NAI delivered by the EAP-Peer in the EAP-Identity Response. The RADIUS User-Name attribute is set to this value in the Access-Request. The AAA infrastructure routes the AAA packets according to the information contained in this attribute.

This section describes the format of the outer identity used in WiMAX during access authentication. The section also describes how to map the NAI used in the outer identity to the NAI used by MIP.

The MS shall format the NAI used as an outer identity during EAP exchanges as follows:

[RoutingRealm1! RoutingRealm2!...!]{WiMAX-decoration}username@realm

Where:

RoutingRealm: Optionally used. The use of routing realm is described in [3].

{WiMAX decoration}: Optionally used to indicate various MS capability/intent. The WiMAX decoration is extensible. The WiMAX decoration consists of one or more attribute value pairs (avp) separated by the '|' enclosed within curly braces.

"{" avp1 "|" avp2 ...."}"

where an avp is formatted as: name"="value with no spaces before and immediately after the "=".

The character set used for name and value must be consistent with the character set specified by [3]. The name must be alphanumeric with no spaces.

Currently there is no specific avp defined in this specification. Future releases are expected to define appropriate avps within this framework.

Username: The user name is as defined by the EAP method with the following caveate. With the exception of NAP authentication,, it is a WiMAX requirement that the username SHALL uniquely identify the user in the home realm. In some cases, where the username in the outer identity is not required by the EAP method, the MS SHALL generate a pseudo-identity to be used as the username in the outer identity.

Realm: As specified by [3].

The MS requirements for generating pseudo-identities are as follows:

- If the MS is required to generate a pseudo-identity, then the MS SHALL generate a fresh pseudo-identity for each network entry.

- To reduce the probability of identity collisions, the pseudo-identity generated by the MS SHALL be at least 128-bit random number, expressed in ASCII-hex. For example: A234F6789B123456123456789C12345E.

HAAA procedure for processing pseudo-identity is as follows:

- Upon receiving an Access-Request as part of network entry, where the username is a pseudo-identity, the HAAA SHALL check to ensure that the pseudo-identity is not in use by an authenticated MS in the realm of the HCSN. If the pseudo-identity is used by another MS, then the HAAA SHALL fail the EAP authentication by sending an Access-Reject containing an EAP-failure indication.

As mentioned above, the MIP procedure requires the use of the NAI extension. The NAI used during the MIP SHALL be formatted as follows:

- Upon successful network entry, in order to initiate the MIP session, the MS SHALL formulate the NAI extension using the username and the realm of the HCSN, used during the HNSP authentication for network access.

- Similarly, in the case of PMIP, the PMIP4 client SHALL contruct the NAI extension as above by using the NAI received in the EAP-Response Identity during HNSP authentication.

- If the MS has an ongoing MIP session, then the MS SHALL continue to use the same NAI in the MIP NAI extension that it has been using.

1
2
- • In case of MIP6, the username and HCSN realm is carried in identifier option ([21]) or in IDi field in the IKE.

3 4.4.1.4   Detailed Impact on Functional Entities

4 4.4.1.4.1 MS Requirements

5 4.4.1.4.1.1   General Requirements

6 EAP messages SHALL be transported between the MS and the ASN using PKMv2.

7 If NAP authentication is required, ASN selects Double EAP during SBC negotiation. Otherwise, Single EAP is
8 selected. When NAP authentication is performed, it is performed as the first EAP of Double EAP followed by the
9 the HNSP authentication as the second EAP.

10 Network access authentication is started when the MS receives an EAP-Request Identity from the NAS.

11 If the EAP-Request Identity contains network selection attribute as per [46] the MS SHALL select the appropriate
12 VCSN. How this selection is performed is not in scope of this specification.

13 The MS assumes that the NAP authentication, when required, is for authenticating the device credential. On the
14 other hand, the HNSP authentication MAY be for authenticating only subscriber credential, or both subscriber and
15 device credentials.

16 The MS generates a pseudo-identity for this session as described in section 4.4.1.3.1. The pseudo-identity SHALL
17 be stored for the duration of this session and MAY be used as the NAI for CMIP and PMIP operations and any other
18 service that requires an NAI from the MS.

19 Based on the policy provisioned in the MS by the HNSP, the MS SHALL determine which realm SHALL perform
20 the authentication. The realm SHALL be omitted from the NAI for NAP authentication.

21 Given the above information, the MS SHALL construct an NAI as described in section 4.4.1.3.1 and use that NAI in
22 the EAP-Response Identity message. The length of this NAI MUST NOT exceed 253 octets.

23 NAP MAY have one of the various policies for detemining when to perform NAP authentication. It MAY choose to
24 not to do it at all, or do it only during the initial network entry, or do it each time MS authenticates. The MS figures
25 out the required action based on the SBC negotiation (Double EAP means NAP authentication required).

26 HNSP has the same flexibility with respect to when to authenticate the device credential. This policy is assumed to
27 be known to the MS. Details of how MS learns this policy is outside the scope of this specification.

28 After sending the EAP-Response Identity, the MS receives EAP-Request EAP-method suggesting the method to use
29 for performing the authentication. If the MS does not agree with the selected method then the MS SHALL respond
30 with a EAP-Response NAK suggesting its preferred EAP method to use for that authentication. Otherwise, the MS
31 starts executing the EAP-method.

32 In response to an EAP Success message, the MS is granted access to the network and SHALL proceed either with
33 PMIP or CMIP procedures. As well, the MS SHALL save a copy of its NAI.

34 4.4.1.4.1.2   NAP Authentication

35 In addition to the procedures specified in the section 4.4.1.4.1.1, this section specifically addresses the procedures to
36 follow for NAP authentication.

37 In response to EAP-Request Identity, the MS SHALL omit the realm part of the NAI during the NAP authentication.
38 The EAP authentication server typically resides in the ASN.

39 In response to EAP-Request EAP-method the MS SHALL either respond with an EAP-Response NAK if it does not
40 approve of the method selected by the ASN or it SHALL start executing the EAP method proposed by the ASN.

41 The EAP authentication SHALL proceed according to [6] and the specific EAP method used.

42 Upon successful EAP authentication, indicated by the reception of EAP-Success, the MS SHALL cache the MSK
43 and enter the HNSP authentication. The MS SHALL discard the EMSK.

1 If NAP authentication fails, the MS SHALL be denied network entry. If the EAP method is reset, the MS SHALL
2 abandon the authentication and re-enter the network.

3

4.4.1.4.1.3 HNSP Authentication

5 In addition to the procedures specified in section 4.4.1.4.1.1, this section specifically addresses the procedures to
6 follow for HNSP Authentication.

7 In response to EAP-Request Identity, the MS SHALL set the realm part of the NAI to be the FQDN of the HCSN.
8 This is where the EAP authentication server resides. If network routing is being utilized, the MS MUST ensure that
9 the route specified in the NAI terminates at the HCSN. The MS SHALL use the same username in the NAI as it
10 used during the NAP authentication.

11 In response to EAP Request EAP-method, the MS SHALL either respond with an EAP Response NAK if it does not
12 approve of the method selected by the HCSN or it SHALL start executing the EAP method proposed by the HCSN.

13 The EAP authentication SHALL proceed according to [6] and the specific EAP method used for HNSP
14 authentication.

15 If the EAP method is reset the MS SHALL abandon the authentication and re-enter the network. If the HNSP
16 authentication fails, the MS SHALL be denied network entry.

17 After successful completion of the HNSP authentication, the MS SHALL compute the keys required for PKMv2
18 using the MSK cached from the NAP authentication and the MSK derived during HNSP authentication. The MS
19 SHALL use the EMSK to compute other application keys (see section 4.3.1)

4.4.1.4.1.3.1 Authenticating Subscriber Credential

21 When the HNSP requires to authenticate the subscriber credential only, an appropriate EAP method that can use
22 subscriber credential SHALL be selected and executed between the MS and the HCSN. When the subscriber is
23 identified by the MAC address of the MS, device credential can be used as the subscriber credential.

4.4.1.4.1.3.2 Authenticating Subscriber and Device Credentials

25 A HNSP that requires to authenticate both the device and subscriber credential can do so by executing one EAP
26 method. Dual authentication by single EAP method is possible by using either combined credentials or tunneling
27 EAP methods (e.g., EAP-TTLS).

28

29 When the user and device credentials can be combined as outlined below and used with a single EAP method, two
30 separate authentications can be effectively executed at once. For combining PSK-based credentials the following
31 formula MUST be used.

32 $$Combined\_identifier = MAC\_address \mid \text{“-”} \mid user\_ID$$

33 $$Combined\_PSK = truncate(HMAC\text{-}SHA256(PSK\_device, PSK\_user), N)$$

34 MAC_address is the 48-bit IEEE 802.16 MAC address printed as 6 2-digit hexadecimals delineated by hyphens (“-“.
35 ASCII x2D). For example: “00-11-22-33-44-55”. User_ID is the identifier of the PSK_user. For example:
36 “joe@isp1.com”. The example combined identifier would be “00-11-22-33-44-55-joe@isp1.com”.

37 PSK_device and PSK_user are the pre-shared secret keys for device and user respectively. N is the length of the pre-
38 shared key used by the PSK-based authentication method. N is less than or equal to 256 bits.

39 Once generated, Combined_identifier and Combined_PSK can be used with a PSK-based authentication method
40 executed between the MS and the HCSN. Successful execution of the method indicates both the subscriber and the
41 device are authenticated.

42 Another way to achieve authentication of two entities using a single EAP method is to rely on tunneling methods
43 (e.g., EAP-TTLS). Tunneling method and tunneled method can achieve authentication of two separate entities (e.g.,
44 subscriber and device). While this specification does not prevent such schemes, further details are outside the scope
45 of this specification.

1 Some tunneled EAP methods (e.g., EAP-TTLSv0) are susceptible to man-in-the-middle attacks when one of the
2 end-point cannot verify that both the inner and the outer method are executed by the same entity. One way to
3 prevent such a threat is to cryptographically bind the inner and the outer authentication methods. Note this is not
4 supported by all tunneled methods (such as EAP-TTLSv0). Another is to ensure that both the MS and the HAAA
5 configurations are always in-synch with respect to when to engage tunneled EAP methods as opposed to using the
6 inner method only. Deployments SHOULD use one of these remedies or their equivalents when using at-risk EAP
7 methods

4.4.1.4.2 NAS Requirements

4.4.1.4.2.1   General Requirements

10 Network Access Authentication and Authorization starts when the NAS or more specifically the EAP-Authenticator
11 receives a signal to initiate EAP. Upon receiving this signal the EAP-Authenticator sends an EAP-Request Identity
12 to the MS (see section 4.5).

13 If the outer identity does not contain a realm part, the NAS invokes its EAP Authentication Server to commence
14 EAP authentication for the NAP. The resulting EMSK is discarded and MSK is used to protect the HNSP
15 authentication. If and only if the NAP authentication was successful, then the NAS SHALL trigger the HNSP
16 authentication by issuing another EAP-Request identity.

17 The NAS acts as an EAP pass-through ([6]) for any authentication that has a specific realm in the outer NAI (e.g.,
18 HNSP authentication). The NAS SHALL route the RADIUS messages according to routing information in the NAI,
19 if any. The NAS receives an MSK at the end of successful authentication.

20 Upon successful authentication (HNSP, or NAP and HNSP), the NAS SHALL bind the state for the MS to the R6
21 path identifier (for IP-CS) or the MAC address for (Ethernet-CS). This binding is used to verify that a particular
22 traffic flow is coming from a specific device.

4.4.1.4.2.1.1   NAP Authentication

24 When the NAS performs the NAP authentication it SHALL conform to [6] and the specific procedures as defined
25 for EAP method used to authenticate the device.

26 Regardless of whether the NAS is acting as the EAP authentication server or as a passthrough suthenticator, if NAP
27 authentication fails the NAS SHALL reject the MS request for network access. In this case the NAS MAY record
28 the failure using a RADIUS Accounting Request (Failure) packet.If the NAP authentication succeeds then the NAS
29 SHALL store the MSK (as computed locally or as received via RADIUS Access-Accept) and SHALL commence
30 the HNSP authentication.

31 If the NAS was acting as the EAP authentication aerver, the NAS SHALL discard the EMSK generated by the EAP
32 method.

4.4.1.4.2.1.2   HNSP Authentication

34 Whether NAP authentication was skipped or completed successfully,, the NAS SHALL trigger the HNSP
35 authentication phase by sending the MS an EAP-Request Identity.

36 HNSP authentication phase SHALL commence upon receiving an EAP-Response-Identity. The realm in the outer
37 identity SHALL NOT be null. Otherwise, the NAS SHALL reject the session and not allow the MS network access.

38 During the HNSP authentication phase, the NAS acts as an EAP pass-through authenticator in accordance to [6].
39 The NAS SHALL transport the EAP exchanges in accordance with [8].

40 The NAS SHALL include the Device Authentication Indicator in the RADIUS Access-Request indicating that the
41 NAP authentication was successful.

42 While acting as a pass-through authenticator, if the NAS receives an EAP-Request Identity in a RADIUS message
43 before receiving EAP-Success or EAP-Failure indication, the NAS SHALL terminate the authentication procedure
44 and send an EAP-Request Identity to the MS. The NAS SHALL erase the MSK generated/received during the NAP
45 authentication, if any.

1　Upon receiving an Access-Accept with EAP-Success indication, the NAS shall save the MSK and follow the
2　procedures as specified in section 4.3.4.

3　Upon receiving an Access-Accept with EAP-Failure indication, the NAS shall discard the previously saved MSK, if
4　any, and SHALL deny the MS network access.

5　**4.4.1.4.2.2　RADIUS Message Processing**

6　**4.4.1.4.2.2.1　Initial Access-Request**

7　The NAS SHALL send an Access-Request as triggered by the EAP process to initiate authentication. The attributes
8　for the Access-Request are listed in Stage 3 Annex – Prepaid Accounting and section 5.4.

9　The NAS SHALL set the EAP-Message attribute to the value received in the EAP-Response/Identity. The NAS
10　SHALL follow the procedures defined in [8] for processing the RADIUS messages carrying EAP data. This
11　includes setting the value of the Message-Authenticator attribute.

12　The NAS SHALL set the NAS-ID to the FQDN of the NAS.

13　The NAS SHALL include the MAC address in the Calling-Station-Id of the RADIUS Access Request message and
14　any other subsequent RADIUS Access-Request message or Accounting message.

15　The NAS SHALL set its WiMAX capability in the WiMAX Capability attribute for this user session.

16　If the device credential was successfully authenticated during NAP authentication, NAS SHALL set the Device-
17　Authentication-Indicator to 1 in the RADIUS Access-Request message of the HNSP authentication.

18　If the NAS supports CUI and it requires CUI to be delivered then the NAS SHALL include the CUI attribute in the
19　Access-Request packet and SHALL set its value to null.

20　The NAS SHOULD forward the Access-Request packet to the VAAA in the visited CSN using the routing
21　decoration of the NAI, if any.

22　**4.4.1.4.2.2.2　Responding to RADIUS Challenge**

23　During the execution of EAP method, the NAS receives RADIUS Access-Challenge packets, to which the NAS will
24　respond with RADIUS Access-Request packets. The contents of these packets are defined in Table 5-3.

25　If the NAS receives an EAP/Request Identity indication in the Access-Challenge packets then the NAS SHALL pass
26　the EAP-Request/Identity to the MS and if the NAS was performing Double EAP procedures, then the NAS SHALL
27　exit the authentication procedure as defined in section 4.4.

28　**4.4.1.4.2.2.3　NAS Receives Access-Accept from HAAA**

29　Upon successful HNSP authentication the NAS will receive an Access Accept packet as defined in Table 5-3.
30　Unless otherwise specified, any mandatory attributes that are missing from the Access-Accept, or if attributes not
31　allowed are present, then the NAS SHALL treat the Access-Accept packet as an Access-Reject packet and deny the
32　MS network access.

33　As per [8], the NAS SHALL validate the Message-Authenticator (80) attribute. The NAS SHALL silently discard
34　the Access Accept packet if the Message-Authenticator attribute is not present in the packet or if the computed
35　Message Authenticator does not match the value received in the packet.

36　The NAS SHALL store the MSK key. The MSK key is used for computing the AK used for securing the 802.16 air
37　interface.

38　The NAS receives a set of attributes for Mobile IP procedures which the NAS stores against the session context. See
39　PMIP and CMIP sections in 4.8.

40　The NAS SHALL store the CUI received. The CUI SHALL be sent in each RADIUS Accounting-Request message.

41　The NAS SHALL store the first Class attribute if received in the Access-Accept associated with the HNSP
42　authentication.

43　The NAS SHALL store the MAC address of the MS.

1 The NAS SHALL store the AAA-Session-Id attribute received in the Access-Accept. The AAA-Session-Id SHALL
2 be used in all subsequent Access-Request messages. The AAA-Session-Id is also used in the RADIUS Accounting
3 messages.

4 If the NAS receives Prepaid attributes it SHALL process them as per section 4.4.3 and Stage 3 Annex – Prepaid
5 Accounting.

6 If the NAS receives Filter and Tunneling attributes it SHALL process them as per section 4.4.3.5.

7 The NAS SHALL NOT send a RADIUS Accounting-Request (Start) packet until Mobile IP registration procedures
8 are completed.

9 **4.4.1.4.2.2.4   NAS Receives Final Access-Reject**

10 Upon unsuccessful authentication the NAS MAY receive an Access-Reject packet as defined in Table 5-3.

11 The NAS SHALL validate the Message-Authenticator (80) attribute as per [8]. The NAS SHALL silently discard
12 the Access-Reject packet if the Message-Authenticator attribute is not present or the computed Message
13 Authenticator does not match the value received in the Access-Reject packet.

14 **4.4.1.4.3 Visited CSN AAA Requirements**

15 The Visited CSN plays the role of a AAA proxy. To choose the target VCSN the VCSN can be statically configured
16 at the ASN. Alternatively, the Routing Realm used in the User-Name (NAI) attribute of the RADIUS message can
17 contain the FQDN of the selected VCSN. In either case the RADIUS messages are routed to this entity

18 **4.4.1.4.3.1   VCSN Acting as AAA Proxy**

19 During all AAA interaction the VCSN AAA server acts as a RADIUS proxy transporting RADIUS packets between
20 the ASN and the HCSN.

21 The VCSN AAA proxy is not passive and is allowed to modify, insert or remove attributes in the packet as specified
22 herein.

23 During proxy operation the AAA Proxy SHALL validate all RADIUS packets containing EAP messages as per [8].
24 If the packets received are invalid (Message Authenticator does not compute) the AAA proxy SHALL discard the
25 packet.

26 During routing operations the VCSN SHALL process the NAI found in the User-Name attribute as specified by [3]
27 and route the RADIUS packets accordingly.

28 **4.4.1.4.4 Home CSN AAA Requirements**

29 The Home AAA is involved in network access authentication and mobility service authentication. This section
30 describes the HAAA procedures for network access authentication.

31 The HAAA plays the role of the EAP authentication server. It is responsible for performing HNSP authentication.

32 Network access authentication starts when the HAAA receives an Access-Request message containing an EAP-
33 Message payload which is set to the MS EAP-Response/Identity. This message is sent from the NAS in the ASN to
34 the HAAA server in the HCSN via the AAA Proxy in the VCSN and perhaps one or more AAA brokers. The AAA
35 packets exchanged between the NAS and the HAAA are Access-Request, Access-Accept, Access-Reject and
36 Access-Challenge (see Table 5-3).   These messages comply with the RADIUS RFCs and the additional
37 requirements given in this specification.

38 The MSK and EMSK that result from HNSP authentication will be used to further derive other keys used in other
39 procedures. The MSK is transported to the NAS. The EMSK is used to derive application keys.

40 The HAAA also derives certain keys and information required for subsequent procedures. The information is
41 described below. Some of the data is transported to the NAS (and entities along the route) using the Access-Accept
42 message and some of the information is cached and used for subsequent procedures such as mobility authentication
43 procedures.

44 In all successful authentication cases the HAAA SHOULD cache the information described in section 4.4.1.4.4.1.

1 The HAAA SHALL delete any keys once they are not needed. Specifically, the HAAA SHALL delete the MSK
2 key after sending it in an Access-Accept message.

3 If Prepaid is active, that is if the user is a prepaid user, then refer to section 4.4.3.3 and Stage 3 Annex – Prepaid
4 Accounting for additional prepaid procedures.

5 If Hotlining is active, that is if the user sessions is to be hotlined then refer to section 4.4.3.5 for additional hot-lining
6 procedures.

7 **4.4.1.4.4.1   HAAA Caching Requirements**

8 The HAAA SHALL cache the following items that are used/generated during network access authentication:

Pseudo Identity	As received from the MS in the NAI in the EAP-Response/Identity. The HAAA is required to correlate this to the true identity of the user.
NAS-ID/NAS-IP address	One or both of these parameters are cached by the HAAA. This is required to locate the serving NAS.
Framed-IP Address or IPv6 address	The IP address allocated to the user session. This information is useful in identifying the session during AAA dynamic procedures.
MIP-RK, HA-RK,FA-RK, MN-HA	Mobility keys generated during network access authentication. These keys are cached and used by the network for mobility authentication.
HA-IP address	The IP address of the HA assigned to the MS.

9 **4.4.1.4.4.2   HAAA Packet Processing**

10 **4.4.1.4.4.2.1   Initial Access-Request**
11 The HAAA receives a RADIUS Access Request containing and EAP message attribute set to the NAI value
12 received in an EAP-Response Identity from the MS.

13 The HAAA plays the role of the EAP authentication server and based on the locally provisioned information,
14 suggests an EAP method by sending an Access-Challenge packet as defined in [8] containing an EAP message
15 attribute with the suggested EAP method.

16 The HAAA caches the pseudo-Identity and the NAS identifiers (NAS-ID, NAS-IP, NAS-IPv6).

17 If the MS rejects the EAP method proposed then it will send an EAP-NAK EAP method, carried in the next Access-
18 Request message proposing another EAP method. If the HAAA accepts the new method or has an alternate method
19 it will respond with an Access-Challenge message as specified in [8]. This continues until an EAP method is
20 selected, or until there are no more options in which case the HAAA SHALL respond with an Access-Reject.

21 Once the EAP method is agreed upon, the EAP method is executed by exchanges of Access-Request/Access-
22 Challenge packets.

23 Once the EAP method completes execution, the HAAA SHALL respond with a final Access-Accept packet or a
24 final Access-Reject packet.

25 The generation of the final Access-Accept is specified in section 4.4.1.4.4.2.2.

26 **4.4.1.4.4.2.2   Final Access-Accept**
27 Upon successful HNSP authentication the HAAA SHALL send an Access-Accept packet as defined in Table 5-3.

28 The HAAA SHALL compute the values of the mobility keys as described in sections 4.3.1 and 4.3.5:

29 The HAAA SHALL cache the attributes defined in section 4.4.1.4.4.1.

1 **4.4.1.4.4.2.3   Final Access-Reject**

2 Upon unsuccessful authentication the HAAA SHALL send an Access-Reject packet as defined in Table 5-3 and
3 specified in [8].

4 **4.4.1.5   Reauthentication**

5 This section describes the various aspects of MS-to-Network Reauthentication procedure. The processing of EAP
6 messages is not discussed and is similar to the one described in section 4.5.1.

7 **4.4.1.5.1   Reauthentication Triggers**

8 Reauthentication process MAY be instigated by MS or by Network (ASN GW) and it may result in the
9 Authenticator being relocated to the Serving ASN, when it is anchored away.

10 MS MAY instigate Reauthentication at any time. Note, it is Network/Authenticator that starts EAP Authentication
11 process and it is an Authenticator's decision whether to progress with EAP process when it receives a
12 reauthentication trigger from an MS.

13 MS SHOULD instigate EAP re-authentication some time before AK Context in the MS expires, - i.e. when one of
14 the following conditions is met:

15 • "AK Grace Time" is reached (the pre-configured time before PMK/ AK lifetime expiry);

16 • "CMAC_PN_* counter Grace Interval" is reached (CMAC_PN_U or CMAC_PN_D counter reaches some
17   pre-configured number before its maximum value, e.g., value bigger than $2^{32} - 10, 000$);

18 • "CMAC_KEY_COUNT Grace Interval" is reached (CMAC_KEY_COUNT counter reaches some pre-
19   configured number before its maximum value)

20 If Authenticator wants to maintain the session, it SHOULD initiate Reauthentication process when one of the
21 following conditions is met:

22 • "PMK Grace Time" is reached (the pre-configured time elapses before PMK lifetime expires);

23 • "CMAC_KEY_COUNT Grace Interval" is reached (CMAC_KEY_COUNT counter reaches some pre-
24   configured number before its maximum value);

25 If authenticator wants to maintain the session, it SHALL initiate Reauthentication process when one of the following
26 conditions is met:

27 • Authenticator receives a message from the Serving BS (*AR_EAP_Start* message with BS-originated trigger
28   TLV) informing it that MS' security context in the BS is going to expire (AK Context in a BS -
29   CMAC_PN_* counters, etc.);

30 • Authenticator receives *AR_EAP_Start* message from the Serving BS (in the case the MS instigates
31   reauthentication by sending protected PKMv2 EAP-Start message);

32 After R4 HO is completed, Authenticator MAY instigate Reauthentication start in Serving ASN – Reauthentication
33 with Authenticator relocation scenario (Authenticator relocation "push" mode).

34 Authenticator MAY ignore reauthentication request initiated via EAP Start from MS if the lifetime is going to expire

35 Authenticator SHOULD allow triggering of Reauthentication process by other ASN (e.g. after R4 HO, Serving ASN
36 MAY decide to start Reauthentication process and the "old" Authenticator SHOULD allow it). This requirement is
37 conditioned to the existence of trust relationships between the entity triggering Reauthentication process and the
38 "old" Authenticator.

39 Serving ASN SHOULD initiate Reauthentication process with Authenticator relocation (Authenticator relocation
40 "pull" mode) when one of the following conditions is met:

41 • When it receives *AR_EAP_Start* message from the Serving BS (e.g. MS instigates reauthentication by
42   sending protected PKMv2 EAP-Start message and the Serving BS forwards *AR_EAP_Start* to the "new"
43   Authenticator in the Serving ASN);

44 • Upon its own decision

1   Serving ASN SHOULD initiate Reauthentication (with Authenticator relocation) when it receives an explicit trigger
2   for Reauthentication from the "old" Authenticator.

3   Note, that the "old" Authenticator handles "reauthentication lock" state (as described below) to avoid simultaneous
4   EAP reauthentication process initializations from multiple network entities. When in this state, the "old"
5   Authenticator SHOULD prevent the new EAP reauthentication starts.

6   **4.4.1.5.2 Reauthentication Process**

7   Reauthentication process in the network may be presented as the following four consecutive phases:

8   **4.4.1.5.2.1   Reauthentication Initiation Phase:**

9   As mentioned in the previous chapter, Reauthentication process may be instigated by different entities – MS, "old"
10   Authenticator or Serving ASN.

11   Reauthentication initiation Phase includes the signaling required to trigger the EAP Phase and in the case of
12   Authenticator relocation, the communications between the "new" and the "old" Authenticators before the EAP
13   phase starts. These communications are intended to update the Anchor Authenticator that Reauthentication process
14   starts in the Serving ASN and transfer some relevant MS context.

15   The "old" Authenticator starting Reauthentication process or receiving *Relocation_Req* message from the Serving
16   ASN SHOULD enter "reauthentication lock" state. An Authenticator in "reauthentication lock" state SHALL avoid
17   any new Reauthentication process initiations (to prevent multiple EAP processes running in parallel from different
18   ASN entities). The "old" Authenticator terminates "reauthentication lock" state when it receives confirmation that
19   Reauthentication has been completed - either successfully or not. However, an Authenticator in "reauthentication
20   lock" state SHALL continue providing regular authenticator functions – e.g. such as delivery of AK Context to
21   support HO re-entry events.

22   The following subsections in this chapter present different Reauthentication initiation scenarios with or without
23   Authenticator relocation.

24   **4.4.1.5.2.2   EAP Phase**

25   EAP phase starts when an Authenticator sends EAP-Request/ Identity message over *AR_EAP_Transfer*. In the
26   single-EAP mode, EAP phase ends after the successful EAP method completion when security material (MSK) is
27   created in a supplicant and an authentication server, MSK key is delivered to an Authenticator in ASN and PKMv2
28   EAP-Transfer message with EAP-Success payload is sent to the MS.

29   In the double-EAP mode, EAP phase ends after the successful completion of the 2nd EAP round when security
30   material (MSK2) is created in a supplicant and an authentication server, MSK2 key is delivered to an Authenticator
31   in ASN and PKMv2 Authenticated-EAP-Transfer message with EAP-Success payload is sent to the MS.

32   When the new MSK/ security context is delivered to the Authenticator (in RADIUS Access-Accept message), it
33   creates the "next" MS security context in the ASN, starting the "security key overlapping period". This period is
34   defined as the time interval from the moment the "next" security key is delivered to ASN entity and up to the
35   moment ASN entity receives a signal that the "old" MS security context should be deleted (after the Serving BS
36   detects PKMv2 3WHS successful completion and the "next" security key enforcement). During this "overlapping
37   period", the ASN SHALL handle two security contexts for the MS - the "old" (currently active) and the "next" one.

38   Note, that Serving BS is not aware of EAP phase, it just relays EAP payload between PKMv2 EAP-related messages
39   (protected by CMAC based on the currently available AK) and AuthRelay protocol. EAP process is handled by
40   Supplicant function in MS, Authenticator function in ASN GW and Authentication Server function in AAA server
41   (except for the case when Authentication Server is located in ASN).

42   The Serving BS, however, handles the location of the MS' Authenticator (Authenticator ID). In the case of
43   Authenticator relocation scenario, the BS SHALL handle both IDs – the "old" Authenticator and the "new" one.

44   **4.4.1.5.2.3   PKMv2 3-way Handshake (3WHS) Phase**

45   PKMv.2 3-way Handshake (3WHS) process SHALL be performed after EAP phase completion to enforce the
46   "next" PMK context. The Authenticator triggers PKMv2 3WHS start in the Serving BS by sending

1 *Key_Change_Directive* message including the "next" security context. After the Serving BS detects the successful
2 completion of the PKMv2 3WHS and ensures that the MS uses the new security context over the air, the BS sends
3 *Key_Change_Cnf* message to the Authenticator including Key Change Indicator TLV, thus indicating the
4 completion of PKMv2 3WHS and the enforcement of the "next" security context.

5 At this moment, the Serving BS deletes the "old" MS' security context and, in the case of Authenticator relocation,
6 the Serving BS stops handling the "old" Authenticator ID and marks the "new" Authenticator as the active one.

7 [Note: Old MS security context SHALL not be deleted immediately after the new MS context is created]

8 This event also triggers the deletion of the "old" (currently active) security context in ASN, makes the "next"
9 security context active and terminates "security key overlapping period" in the Authenticator.

4.4.1.5.2.4   Reauthentication Completion Phase

11 This final stage of Reauthentication process is triggered by indication about reauthentication attempt completion
12 (either successful or unsuccessful). When no Authenticator relocation occurs, such a trigger may be
13 *Key_Change_Cnf* message with PKMv2 3WHS Result TLV indicating the results of PKMv2 3way handshake
14 between BS and MS. In the case Authenticator relocation is in progress, the "new" Authenticator SHALL indicate
15 its results to the "old" Authenticator using *Relocation_Cnf* message with Authentication Result TLV.

16 When "old" Authenticator receives a signal that reauthentication attempt has failed, it SHOULD terminate
17 "reauthentication lock" state, thus allowing new reauthentication attempts. "Old" Authenticator MAY also instigate
18 new reauthentication attempt by itself.

19 Note, that reauthentication attempt failure may be detected at any stage. This event should be reported back to the
20 "old" Authenticator, so that it will terminate "reauthentication lock" state and allow new reauthentication attempts.

21 If there was no Authenticator relocation, the Authenticator receiving *Key_Change_Cnf* message with PKMv2
22 3WHS Result indicating "success" should terminate "reauthentication lock" state and SHALL delete the old MS
23 security context (MSK/ PMK, AKs, CMAC_KEY_COUNT, etc.) assuming the successful completion of
24 Reauthentication process.

25 In the scenario with Authenticator relocation, the "new" Authenticator, detecting the successful reauthentication
26 completion, SHALL communicate this event with the "old" Authenticator (using *Relocation_Cnf* message with
27 Authentication Result TLV set to indicate "success"). The "old" Authenticator receiving this indication SHALL stop
28 acting as the Authenticator function for this MS.

29 The "new" Authenticator MAY also request some more MS context (e.g. MS Authorization Context, etc.) from the
30 "old" Authenticator using Context Purpose Indicator TLV included in *Relocation_Cnf* message.

31 If there was no *Context_Req* in *Relocation_Cnf* message, the "old" Authenticator SHALL send Authenticator
32 *Relocation_Cnf_Ack* message without any additional information and delete the MS' context. Otherwise, if
33 *Relocation_Cnf* contains *Context_Req*, the "old" Authenticator SHALL provide the requested context in
34 *Relocation_Cnf_Ack* message and wait for the acknowledgement from the "new" Authenticator (confirming that it
35 has received the requested MS context). When receiving this acknowledgement (ACK message), the "old"
36 Authenticator SHALL delete the MS' context.

37 In the case when the "new" Authenticator and the MS' Anchor GW are not collocated, the "new" Authenticator
38 SHALL also update the MS' Anchor GW (Anchor DP function) that Authenticator relocation has occurred (using
39 *Context_Rpt* message including the new Authenticator ID). This process may occur in parallel with update of the
40 "old" Authenticator.

4.4.1.5.3 Management of PMK SN During Reauthentication

42 In an MS, the PMK SN (in Double-EAP, PMK and PMK2 SN) usage in re-authentication will always follow the
43 rules defined in the section

44 At the network side, if re-authentication occurs on the Anchor Authenticator, since the Anchor Authenticator knows
45 PMK SN (in Double-EAP, PMK and PMK2 SN) from the previous successful authentication, the PMK SN (in
46 Double-EAP, PMK and PMK2 SN) usage in re-authentication can simply follow the rules defined in the section But
47 when re-authentication occurs on a new Authenticator (different to Anchor Authenticator), and if there is no record
48 for PMK SN (in Double-EAP, PMK and PMK2 SN) used in the last authentication in the new Authenticator, the

1   new Authenticator SHALL contact the "old" Anchor Authenticator to get the latest PMK SN (in Double-EAP, PMK
2   and PMK2 SN) which is transferred from the "old" Anchor Authenticator to the "new" Anchor Authenticator.

3   Authenticator SHALL know whether an authentication procedure is initial authentication or not, - when an initial
4   authentication occurs on an Authenticator, it SHALL initialize the PMK SN (in Double-EAP, PMK and PMK2 SN)
5   from Zero, but for re-authentication, it SHALL use PMK SN from the last successful authentication (copied from
6   the "old" Anchor Authenticator).

7   At the network side, current serving ASN can judge whether it is re-authentication or not as described in section
8   4.4.1.5.5.

9   When EAP reauthentication process is successfully completed, (in Single-EAP, when the new Authenticator
10   receives MSK from AAA server; in Double-EAP, when the new Authenticator receives the first and second MSK
11   from AAA server) the new Authenticator SHALL use the latest PMK SN (in Double-EAP, PMK and PMK2 SN).
12   Then, in the "new" Authenticator, AK SN can be derived from PMK SN (in Double-EAP, PMK and PMK2 SN).

13   **4.4.1.5.4 Reauthentication Process Without Authenticator Relocation**

14   EAP-based Reauthentication always starts from Authenticator/ ASN GW by sending EAP-Request/ Identity
15   message over *AR_EAP_Transfer* to Serving BS. MS instigates the start of Reauthentication in the Network by using
16   PKMv2 EAP-Start message protected with CMAC digest (using the currently active AK). Except for "EAP-Start"
17   steps, MS-initiated and Network-initiated Reauthentication procedures (without involving Authenticator relocation)
18   are the same. The Serving BS MAY instigate the start of Reauthentication (e.g. if it detects that MS security context
19   in BS is going to expire), by issuing *AR_EAP_Start* message to the Authenticator.

20   The MS Reauthentication process not involving Authenticator relocation is shown in Figure 4-12:
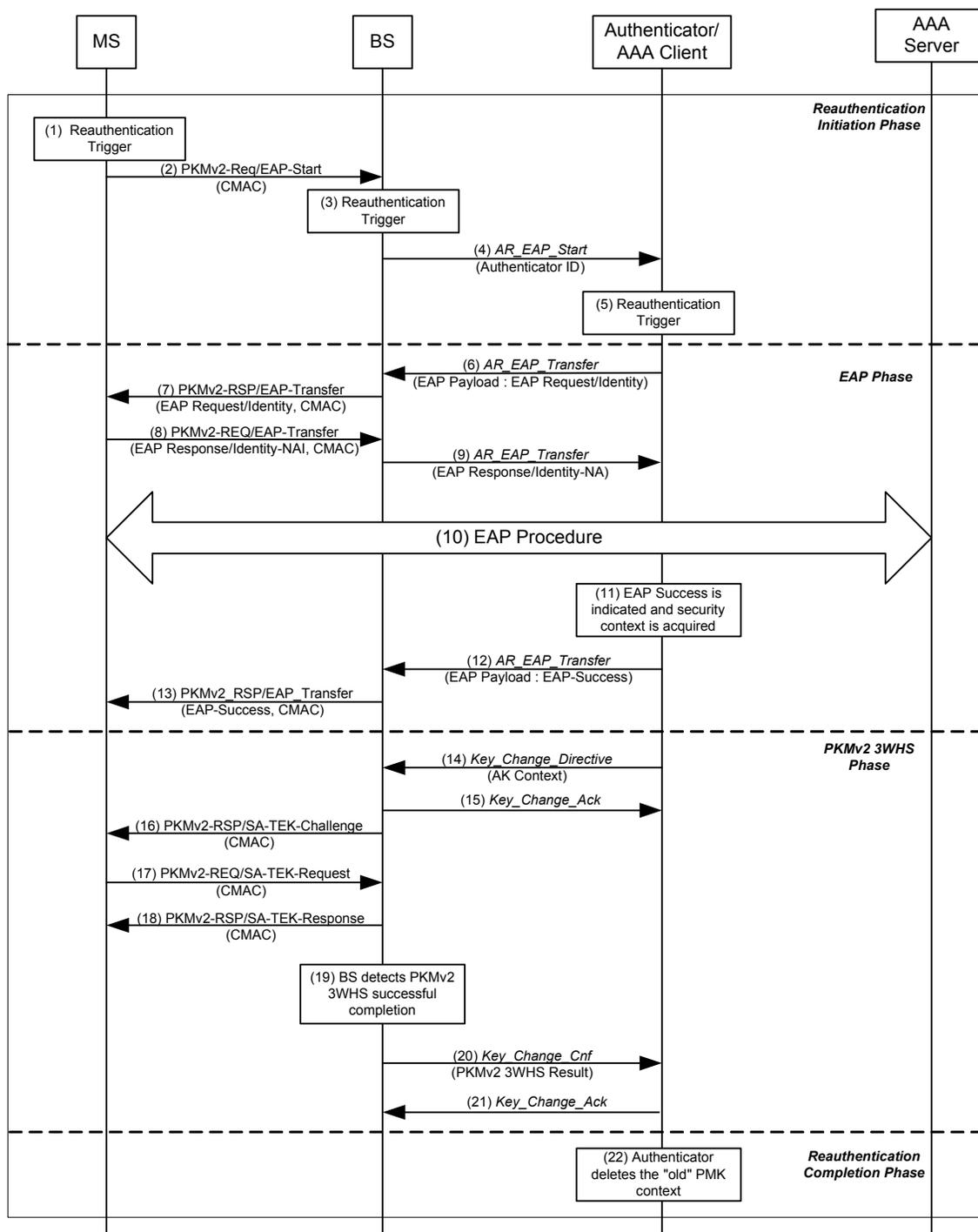
Figure 4-12 – Reauthentication Procedure (w/o Authenticator Relocation)

STEP 1

Reauthentication trigger occurs in MS. This step is relevant only for MS-instigated Reauthentication.

1 **STEP 2**

2 MS sends PKMv2-REQ EAP-Start message protected by CMAC digest (using the currently active AK context).
3 This step is relevant only for MS-instigated Reauthentication.

4 **STEP 3**

5 Reauthentication trigger occurs in the Serving BS, e.g., the BS detects that MS security context (AK lifetime,
6 CMAC_PN_* counters, etc) are going to expire. This step is relevant only when a BS instigates Reauthentication
7 process.

8 **STEP 4**

9 Serving BS verifies CMAC digest of the received PKMv2 EAP-Start message (using the currently active AK
10 context) and if this verification is successful, it sends *AR_EAP_Start* message to the Authenticator triggering
11 Reauthentication process initiation.

12 Note, that BS "relays" only protected and successfully verified PKMv2 EAP-Start messages. Unprotected (without
13 CMAC digest) or "fail to verify" messages (with wrong CMAC digest) SHALL be discarded by a BS.

14 In the case reauthentication trigger occurs in a BS, the BS MAY issue *AR_EAP_Start* message by itself (without
15 receiving PKMv2 EAP-Start from an MS). Such *AR_EAP_Start* SHALL include indication that it is BS-originated
16 message (BS-originated EAP-Start Flag).

17 Serving BS handles the location of the current MS' Anchor Authenticator. In the case the Serving BS and the MS'
18 Anchor Authenticator are located in the same ASN, the BS MAY choose to send *AR_EAP_Start* message directly to
19 the current MS' Anchor Authenticator (the "old" Authenticator). Otherwise, the BS sends *AR_EAP_Start* to its
20 "default" Authenticator (the "new" Authenticator), thus triggering Authenticator relocation. The logic of how a BS
21 decides whether to send *AR_EAP_Start* message to the "old" Authenticator or to its "default" Authenticator (when
22 the Serving BS and the "old" Authenticator are both located in the same ASN), is implementation-specific.

23 The discussed scenario assumes no Authenticator relocation - Serving BS sends *AR_EAP_Start* to the current MS'
24 Anchor Authenticator (or the current MS' Anchor Authenticator is collocated with BS' "default" Authenticator).

25 The composition of *AR_EAP_Start* message is presented in Table 4-5:

26   **Table 4-5 – AR_EAP_Start**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authenticator ID	5.3.2.19	O	Contains the ID of the current MS' Anchor Authenticator (the "old" Authenticator ID). This parameter may be omitted if the destination entity of the message is the current MS' Anchor Authenticator (the "old" Authenticator) – i.e. there is no Authenticator relocation.
>Authorization Policy	5.3.2.20	O	Indicates the authorization policy, supported by BS/ MS pair (single EAP vs. double EAP). It may be omitted if Serving BS assumes that Authenticator is aware of the BS/ MS capabilities.
>BS-originated EAP Start Flag	5.3.2.27	O	This flag is included when BS originates *AR_EAP_Start* message by itself (without receiving PKMv2 EAP-Start from an MS). This indicates BS-originated instigation of Reauthentication process (e.g. if MS security context in BS is going to expire).

IE	Reference	M/O	Notes
BS Info	5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	O	Serving BS ID

1   This step is relevant only for MS-instigated Reauthentication.

2   **STEP 5**

3   Reauthentication trigger occurs in the Authenticator.

4   **STEP 6**

5   The Authenticator initiates EAP-based reauthentication (EAP Phase) by sending *AR_EAP_Transfer* message with
6   EAP-Request/ Identity payload to the Serving BS. The composition of this message is presented in Table 4-6:

7   **Table 4-6 – AR_EAP_Transfer from Authenticator to BS (EAP Initiation)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
EAP Payload	5.3.2.62	M	EAP message. In this step it SHALL include EAP Identity Request message.

8   Note that *AR_EAP_Transfer* message composition remains the same through the EAP authentication process with
9   only difference in the content of the EAP Payload TLV (containing different EAP messages).

10   **STEP 7**

11   The Serving BS "relays" EAP-Request/ Identity payload to MS over PKMv2-RSP EAP-Transfer message protected
12   by CMAC digest (using the currently active AK context).

13   **STEP 8**

14   The MS verifies CMAC digest of the received PKMv2 EAP-Transfer message and if this verification is successful,
15   transfers EAP payload to its EAP Supplicant layer. In response, MS sends PKMv2-REQ EAP-Transfer message
16   with EAP-Response/ Identity payload (created by EAP Supplicant function in MS), protected by CMAC digest.

17   **STEP 9**

18   After the successful CMAC digest verification, Serving BS forwards EAP payload (EAP-Response/ Identity) of the
19   received PKMv2 EAP-Transfer message to the Authenticator using *AR_EAP_Transfer* message.

20   **STEP 10**

21   Authenticator analyzes the NAI provided in the EAP-Response/Identity message. Depending on the realm, EAP
22   payload MAY be forwarded to the MS' Home AAA server via the Visited AAA server (using the provided NAI for
23   resolving the Home-AAA server location). MS SHOULD use the same home and routing realms used in
24   reauthentication as the one used during initial authentication.

25   In order to deliver the EAP payload to the AAA server, the Authenticator forwards the EAP message via a
26   collocated AAA client using RADIUS Access-Request message (EAP payload is encapsulated into RADIUS "EAP
27   message" attribute(s)).

28   The EAP authentication process (tunneling EAP authentication method) is performed between the MS and the
29   Authentication server via the Authenticator in ASN GW in the same way as in the Initial Authentication. BS
30   provides "relay" of EAP payload from PKMv2 EAP-related messages to AuthRelay and vice versa. The

1   Authenticator in ASN GW acts in pass through mode (as described in [8]) and forwards the EAP messages received
2   as a payload from the BS in AuthRelay messages to the AAA server using RADIUS Access-Request messages and
3   vice versa – transferring EAP payload from RADIUS Access-Challenge messages to AuthRelay. The composition
4   of RADIUS messages is presented in section 5.4.1. Service-Type attribute (type 6, [27]) is set to the value
5   "Authenticate only" during reauthentication.

6   During reauthentication, NAS requests "Authentication only" to AAA, AAA doesn't send any authorization profiles
7   to NAS.

8   EAP peers (supplicant in MS and authentication server) negotiate the EAP method and perform it. At the successful
9   completion of EAP method, security keys (MSK and EMSK) are established at the EAP peers (supplicant in MS and
10   authentication server).

11   STEP 11

12   The Authenticator receives indication about the successful completion of EAP-based authentication and the required
13   security context (i.e. MSK key and its lifetime). MS authorization profile MAY be also delivered. The indication
14   about successful completion of EAP process is delivered using RADIUS Access-Accept message from AAA server
15   with EAP-Success message encapsulated in "EAP message" attribute.

16   From this moment, Authenticator SHALL hold two security contexts: the currently active one and the "next" context
17   created during re-authentication (Authenticator SHALL NOT override the currently active MSK key and its
18   lifetime). Authenticator continues to provide AK key (e.g. for re-entry) using the currently active security context
19   and uses the "next" security context only to derive AK Context for *Key_Change_Directive* (refer to the step 14).

20   In the case of EAP process failure, the Authenticator will receive RADIUS Access-Reject message with EAP-
21   Failure encapsulated in "EAP message" attribute. Note, that EAP failure in Reauthentication SHOULD NOT result
22   in service termination for the MS as long as the "currently active" MSK and security context are valid.

23   STEP 12

24   The Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to BS as EAP Payload TLV in
25   *AR_EAP_Transfer* message.

26   STEP 13

27   The BS relays EAP payload (received in AuthRelay message) to the MS in PKMv2 EAP-Transfer/ PKM-RSP
28   message protected by CMAC digest (using the currently active AK context). This message indicates the Supplicant
29   in the MS the results of EAP process. Note, that the BS does not relate to the content of EAP Payload – whether it is
30   EAP-Success or EAP-Failure message. The MS is also waiting for PKMv2 SA-TEK-Challenge message from BS to
31   proceed with PKMv2 3way handshake.

32   STEP 14

33   The Authenticator sends *Key_Change_Directive* message to the BS to provide it with the "next" security context
34   (AK Context) and trigger PKMv2 3WHS process between the BS and the MS (to enforce the "next" security
35   context). The composition of this message is presented in Table 4-7:

36   **Table 4-7 – Key_Change_Directive from Authenticator to BS**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>AK Context	5.3.2.6	M	This compound parameter includes AK context parameters (AK, AK SN, AK lifetime, etc.) for BS use.

37   In the case authentication failure signal is received from the AAA server (RADIUS Access-Reject with EAP-
38   Failure), the Authenticator may decide to restart EAP authentication process (by sending the new EAP Request
39   Identity)

1   **STEP 15**

2   BS receiving *Key_Change_Directive* message from Authenticator will acknowledge it by sending the *Key_Change_*
3   *Ack* message.

4   **STEP 16 - 18**

5   The BS initiates PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) with the MS to verify
6   the new AK. The "next" security context (the "new" AK context) SHALL be used to protect PKMv2 3way
7   handshake messages as specified in [2].

8   **STEP 19**

9   The BS detects the successful completion of PKMv2 3WHS process. The BS SHALL ensure that PKMv2 3way
10   handshake is indeed successfully completed and the new PMK/AK is enforced by the MS – i.e. the BS should
11   receive and verify a MAC management message from the MS signed by CMAC derived from the new AK. When
12   BS recognizes the completion of PKMv2 3-way handshake process (success or failure), it SHALL indicate this
13   event to Authenticator.

14   **STEP 20**

15   The BS indicates the completion of PKMv2 3WHS and enforcement of the "new" keys to the Authenticator by
16   sending *Key_Change_Cnf* message with PKMv2 3WHS Result indication.

17   **Table 4-8 – Key_Change_Cnf Message from BS to Authenticator (PKMv2 3WHS Completion)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
≥Key Change Indicator	5.3.2.86	M	Indicates the completion of PKMv2 3way handshake to Authenticator. In the case of successful PKMv2 3way handshake completion is detected, it shall indicate "success".

18   In the case, the BS detects a failure of PKMv2 3WHS process for any reason, it sends *Key_Change_Cnf* message
19   with PKMv2 3WHS Result set to indicate "failure".

20   **STEP 21**

21   The Authenticator receiving *Key_Change_Cnf* message from the BS, acknowledges it by sending the
22   *Key_Change_Ack* message.

23   **STEP 22**

24   The Authenticator recognizing that the "new" AK context has been successfully enforced over the air, SHALL
25   delete the "old" security context and change the status of the "new" security context from "next" to "active".

26   **4.4.1.5.5   Reauthentication with Authenticator Relocation or Authenticator and FA Relocation**

27   Authenticator relocation occurs when Reauthentication process is handled by an Authenticator entity, which is not
28   collocated with the MS' Anchor Authenticator. Optionally FA relocation can be done along with Authenticator
29   relocation. This may occur in the following scenarios:

30   •   In the case MS instigates Reauthentication process by PKMv2 EAP-Start message and the BS sends
31   *AR_EAP_Start* message to its "default" Authenticator entity, which is different from the "old"
32   Authenticator (the current MS' Anchor Authenticator).

33   •   In the case the Serving ASN (different from the Authenticator ASN) triggers Reauthentication process.

1 • In the case Reauthentication process is instigated by the "old" Authenticator (the current MS' Anchor
2 Authenticator), the Serving ASN MAY trigger FA relocation if FA is collocated with the Authenticator.(If
3 the FA is not collocated with the Authenticator, the FA relocation may be rejected. In this case to trigger
4 FA relocation, it should follow the procedure defined in section 4.8.2.3 or section 4.8.2.4.

5 The first two scenarios may be considered as Authenticator Relocation "pull" mode, while the last one may be
6 considered as a "push" mode.

7 The new Authenticator distinguishes the Reauthentication process start (vs. the Initial Authentication process) by
8 one of the following:

9 • Receiving *AR_EAP_Start* from a BS. This means that MS has sent a protected PKMv2 EAP-Start message
10 (signed by CMAC), BS has successfully verified it according to the currently active AK context and
11 "relayed" EAP-Start to the ASN GW (where the "new" Authenticator entity is located) using
12 *AR_EAP_Start* message.

13 • In the case the Serving ASN triggers Reauthentication by itself, it is aware whether MS is authenticated and
14 authorized.

15 • In the case the "old" Authenticator instigates Reauthentication process in the ASN GW (e.g. the Serving
16 ASN GW), R4 message informs this ASN GW that it is Reauthentication.

17 The "new" Authenticator learns the location of the "old" Authenticator during Reauthentication initiation phase. For
18 MS-instigated reauthentication, Authenticator ID is delivered to the "new" Authenticator in *AR_EAP_Start* message.
19 For network-initiated Reauthentication, it is delivered in the explicit R4 signal for "push" mode (e.g. from the "old"
20 Authenticator).

21 In the case of Authenticator relocation, until Reauthentication process is completed, the Serving BS handles the IDs
22 of both Authenticators – the "old" Authenticator and the "new" one.

4.4.1.5.5.1   Authenticator Relocation - "PULL" Mode

24 Authenticator relocation "pull" mode is considered when:

25 • MS or the Serving BS instigate Reauthentication process and the Serving BS sends *AR_EAP_Start* to the
26 "new" Authenticator entity in the Serving ASN, or

27 • Serving ASN triggers Reauthentication process and may trigger FA relocation process.

28 Figure 4-13 presents Authenticator relocation "pull" mode.

29 If reauthentication is triggered by MS or BS, BS forwards *AR_EAP_Start* to the "new" Authenticator. In this case,
30 BS SHALL include Old authenticator ID with *AR_EAP_Start* message.

31 Triggering of FA relocation is outlined in 4.4.1.5.5.
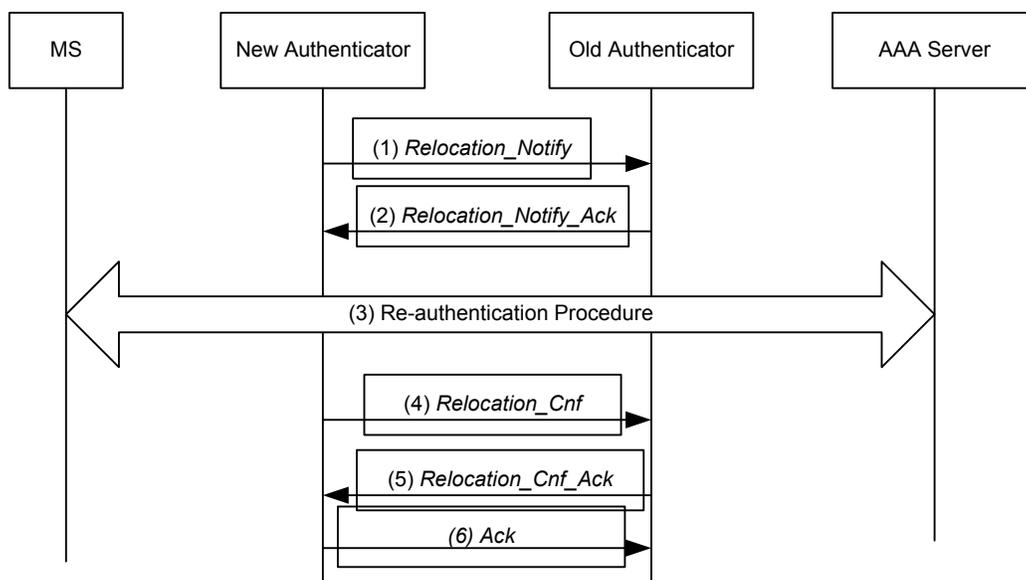
Figure 4-13 – Authenticator Relocation Procedure (PULL)

STEP 1

The "new" Authenticator sends *Relocation_Notify* message to the "old" Authenticator, thus informing it that Reauthentication process starts in the new ASN entity and requesting some relevant MS context (e.g. PMK SN). The composition of this message is presented in Table 4-9:

Table 4-9 – Relocation_Notify from "New" Authenticator to "Old" Authenticator

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authenticator ID	5.3.2.19	O	Indicates the ID of the "new" Authenticator
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context. MS Security History should be always requested in this step (to request PMK/ PMK2 SN, FA context may also be requested)

Authenticator ID TLV may be included to indicate the location of the "new" Authenticator. Otherwise, if Authenticator ID is not included, the "old" Authenticator may assume the ID of the "new" Authenticator by the source IP address of this message. The FA context may be requested to perform Authenticator and FA relocation together.

STEP 2

The "old" Authenticator receiving *Relocation_Notify* message should enter "reauthentication lock" state avoiding new Reauthentication process initiations until it receives some confirmation that Reauthentication process in the new ASN entity has been completed - either successfully or not. However, the "old" Authenticator SHALL continue providing AK Context based on the currently active security context to support HO re-entry events.

The "old" Authenticator responds to the "new" Authenticator with *Relocation_ Notify_Ack* message including the requested MS context. If FA is collocated with the "old" Authenticator, then "old" Authenticator may add the FA context in the response if requested by the serving ASN/ASN GW ("new" Authenticator).

1   **Table 4-10 – Relocation_Notify_Ack from "Old" Authenticator to "New" Authenticator**

IE	Reference	M/O	Notes
Accept/Reject Indicator	5.3.2.1	M	Indicates Accept/ reject of the corresponding request
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
> MS Security History	5.3.2.108	M	MS Security history – PMK/ PMK2 SN
> MS Authorization Context	**Error! Reference source not found.**	O	Contains Authorization context parameters of the specific MS
> MS Networking Context	5.3.2.106	O	Relevant MS Context
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS
> FA Context	5.3.2.101	O	Contains FA context for the MS. If the Anchor Authenticator is collocated with the FA, it may provide it in response to the serving ASN request (indicated by Context Purpose Indicator).

2   Old authenticator MAY reject *Relocation_Notify* only in the case that it is in re-authentication state.

3   **STEP 3**

4   In Step 3, the EAP phase and SA-TEK 3WHS procedures are performed in the same way as described in section
5   4.4.1.5.4.

6   When reauthenticaiton happens, the new authenticator SHOULD compare the realm and routing part of outer NAI
7   which was used in the old authenticator. If the realm and routing part of the NAI is different, the new Authenticator
8   SHALL discard the EAP-Response.

9   If double EAP hanppens during reauthentication, both round of EAP phases uses old AK, so the new authenticator
10   doesn't have to deliver EIK to the serving BS.

11   **STEP 4**

12   The "new" Authenticator informs the "old" Authenticator about the completion of EAP reauthentication process by
13   sending *Relocation_Cnf* message with Authentication Result TLV. This message may optionally include the request
14   for MS Context.

15   The composition of *Relocation_Cnf* message is presented in Table 4-11:

16   **Table 4-11 – Relocation_Cnf Message from "New" Authenticator to "Old" Authenticator**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authentication Result	5.3.2.18	M	Indicates the results of EAP authentication process. It shall be set to indicate "success" if Reauthentication has been successfully completed in the "new" Authenticator. Otherwise, it should indicate "failure".

IE	Reference	M/O	Notes
>FA Relocation Indication	5.3.2.71	O	Indicates the FA relocation process. It shall be set to indicate "Success" if FA relocation has been Successfully completed with authenticator relocation. otherwise it should indicate "Failure"
Context Purpose Indicator	5.3.2.36	O	Indicates the requested context. This TLV may be included only if Authentication Result indicates "success".

1 **STEP 5**

2 The "old" Authenticator, receiving *Relocation_Cnf* message with Authentication Result indicating "success",
3 terminates "reauthentication lock" state and deletes MS security keys.

4 The "old" Authenticator responds with *Relocation_ Cnf_Ack* message. If *Relocation_Cnf* message has contained the
5 request for some MS context, the "old" Authenticator responds with *Relocation_ Cnf_Ack* message containing the
6 requested MS context and waits for Ack (Optional Step6) from the "new" Authenticator. Otherwise, if *Relocation_*
7 *Cnf* didn't request any information, the "old" Authenticator may proceed with MS context deletion.

8 The composition of *Relocation_ Cnf_Ack* message is presented in Table 4-12:

9 **Table 4-12 – Relocation_Cnf_Ack Message**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>MS Networking Context	5.3.2.106	O	Relevant MS Context
>MS Authorization Context	**Error! Reference source not found.**	O	Contains Authorization context parameters of the specific MS
>REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS

10 **4.4.1.5.5.2   Authenticator Relocation -- "PUSH" mode**

11 This scenario presents "push mode" when the existing Authenticator (the "old" Authenticator) triggers
12 Reauthentication process start in Serving ASN. Authenticator relocation occurs upon successful completion of the
13 Reauthentication process.

14 Triggering of FA relocation is already available in section 4.8.2.3 or 4.8.3.3.

1
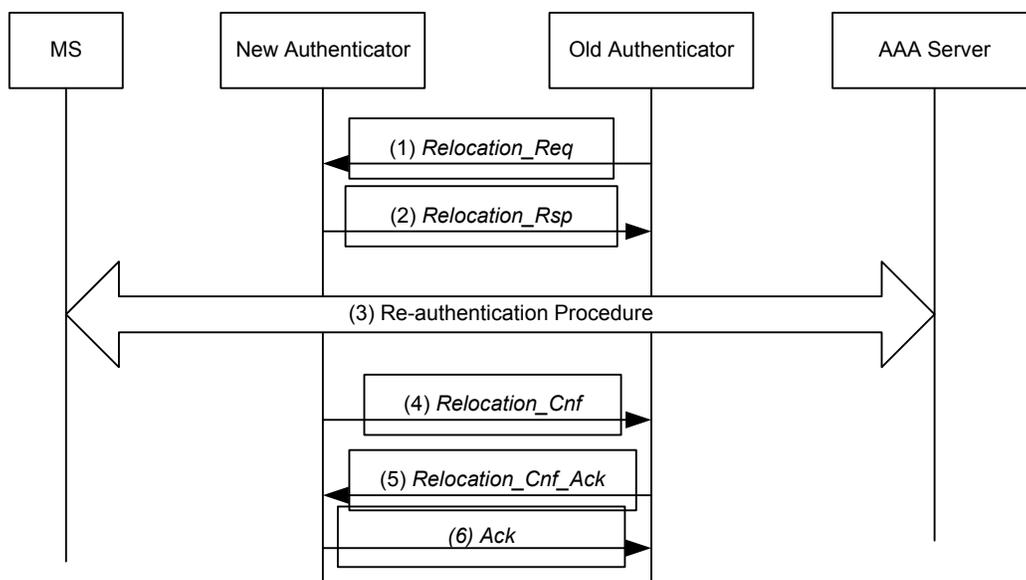
2 **Figure 4-14 – Authenticator Relocation (PUSH)**

3 **STEP 1**

4 The "old" Authenticator sends *Relocation_Req* message to an New Authenticator in order to request
5 reauthentication attempt start. The "old" Authenticator also enters "reauthentication lock" state preventing any new
6 reauthentication attempt start. The "old" Authenticator may include also some relevant MS context (e.g. PMK SN)
7 in this message. The "Old" Authenticator may add FA context in *Relocation_Req* message if FA is collocated.

8 The composition of *Relocation_Req* message is presented in Table 4-13:

9 **Table 4-13 – Relocation_Req from "Old" Authenticator to "New" Authenticator**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
> MS Security History	5.3.2.108	M	Provides MS Security history – PMK/ PMK2 SN
> MS Authorization Context	**Error! Reference source not found.**	O	Contains Authorization context parameters of the specific MS
> MS Networking Context	5.3.2.106	O	Relevant MS Context
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS
> Authenticator ID	5.3.2.19	O	Indicates the ID of the 'old' Authenticator GW.
> FA Context	5.3.2.101		Contains FA Context for the MS, If included it indicates the suggestion for FA relocation.
BS Info	5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	O	Serving BS ID

1 **STEP 2**

2 The "new" Authenticator entity responds to the "old" Authenticator with *Relocation_Rsp* message.

3 **Table 4-14 – Relocation_Rsp from "New" Authenticator to "Old" Authenticator**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Indicates Accept/ reject of the corresponding request.
>Failure Indication	5.3.2.69	O	Contains MS-related context in the nested IEs.
Accept/ Reject Indicator	5.3.2.1	M	Indicates the rejection/ error cause in the case of the negative response.

4 In the case, the Serving ASN responds with *Relocation_Rsp* message indicating a "reject" of Authenticator
5 relocation "push", the Anchor Authenticator MAY initiate MS Network Exit procedure.

6 **STEP 3 - 5**

7 The procedure is same as that of Authenticator Relocation procedure (PULL)

8 **4.4.1.5.5.3   Authenticator Update Notification Procedure**

9 After authenticator relocation procedure happens, new authenticator SHALL inform the Anchor DP of the change of
10 authenticator by sending *Context_Rpt* which includes the new authenticator ID.
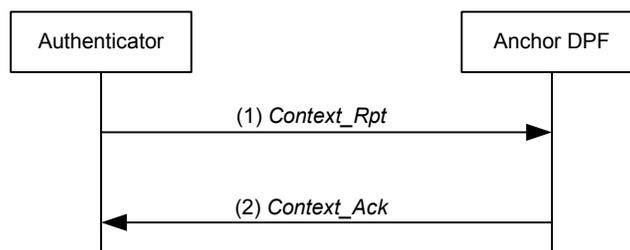
11

12 **Figure 4-15 – Authenticator Update Notification Procedure**

13 **STEP 1**

14 The "new" Authenticator updates the MS' Anchor DP with the "new" MS' Anchor Authenticator location using
15 *Context_Rpt* message. The composition of this *Context_Rpt* message is presented in Table 4-15:

16 **Table 4-15 – Context_Rpt from "New" Authenticator to Anchor DP**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authenticator ID	5.3.2.19	M	Indicates the ID of the "new" Authenticator
>Service Authorization Code		**O**	Indicates whether MS is authorized for service or not
Context Purpose Indicator	5.3.2.36	M	Identifies the purpose of the Context transaction. In this case it should be set to indicate – "MS Network Context" ,"Service Authorization Context" and may include "FA context" (bits #1, #3 and #6).
Failure Indication	5.3.2.69	O	Provide failure indication for this message

1   **STEP 2**

2   Anchor DP receiving *Context_Rpt* message, acknowledges it by *Context_Ack* message and overrides the
3   Authenticator ID value.

4   **4.4.1.5.6 Error Handling**

5   The failure of EAP Reauthentication process (EAP-Failure) should not cause any change in the MS state – MS
6   should be served until its PMK/ AK context expires (e.g. PMK/ AK lifetime expiry). Authenticator or MS may
7   restart EAP Reauthentication process when detecting EAP reauthentication failure.

8   **4.4.2 EAP over R6 Authentication Relay**

9   Authentication Relay protocol is a protocol among the suite of the WiMAX Protocols and follows R6 protocol
10   design. Authentication Relay protocol is used as an envelope to transfer EAP payload (EAP messages) between BS
11   (EAP Relay entity) and EAP Authenticator over the UDP/ IP infrastructure. AuthRelay protocol messages are
12   defined to correspond to PKMv2 EAP-related messages in IEEE 802.16e.

13   The following messages are defined in the scope of Authentication Relay protocol (see section 5.2 for details):

14   **Table 4-16 – List of Authentication Relay Protocol Messages**

AR_EAP_Start
AR_EAP_Transfer
AR_EAP_Complete
AR_Authenticated_EAP_Start
AR_Authenticated_EAP_Transfer

15   The Base Station acts as an EAP Relay entity. It transfers an EAP message received from the MS over R1 to the
16   Authenticator over R6 RP and vice versa. For each valid EAP message that the Base Station receives over PKMv2,
17   it sends a corresponding AuthRelay message to Authenticator (including the received EAP message as a payload).
18   The BS processes only valid PKMv2 EAP-related MAC messages on the air interface and discards non-valid
19   PKMv2 EAP-related messages (e.g. unprotected EAP-Start, unprotected EAP-Transfer during re-authentication,
20   protected PKMv2 messages which BS fails to validate, etc.).

21   The AuthRelay messages represented by different Message Types correspond one-to-one to the PKMv2 EAP-related
22   messages on 802.16e interface. The mapping between PKMv2 and AuthRelay messages is presented in Table 4-17.

23   **Table 4-17 – Authentication Relay Messages Mapping to PKMv2 and Vice Versa**

AuthRelay Message	PKMv2 message code	PKMv2 REQ/ RSP	Notes
AR_EAP_Start	EAP-Start	REQ	PKMv2 EAP-Start is sent by MS to initiate EAP reauthentication. *AR_EAP_Start* is sent by the BS to the Authenticator. If PKMv2 EAP-Start is not protected by CMAC, the BS drops this message and does not send an *AR_EAP_Start* to the Authenticator PKMv2: MS → BS AuthRelay: BS → Authenticator

AuthRelay Message	PKMv2 message code	PKMv2 REQ/ RSP	Notes
AR_EAP_Transfer	EAP-Transfer	REQ	This message is used to exchange EAP payload between peers. PKMv2: MS→ BS AuthRelay: BS → Authenticator
		RSP	AuthRelay: Authenticator → BS PKMv2: BS→ MS
AR-EAP-Complete	EAP-Complete	RSP	In the case of double EAP, this message is used to carry EAP-Success at the successful completion of the first EAP round. The Authenticator sends AR-EAP-Complete message to BS with EAP-Success payload. The BS sends PKMv2 EAP-Complete message with EAP-Success payload to the MS. PKMv2 message SHALL be protected by CMAC derived from the EIK of the 1st EAP round if initial NW entry or else by AK. AuthRelay: Authenticator → BS PKMv2: BS → MS
AR_Authenticated_EAP_Start	Authenticated-EAP-Start	REQ	This message is used only for initiation of the second EAP round in a double EAP procedure and is sent by the MS to the BS (PKMv2) and by the BS to the Authenticator PKMv2: MS→ BS AuthRelay: BS → Authenticator
AR_Authenticated_EAP_Transfer	Authenticated-EAP-Transfer	REQ	This message is used to exchange EAP payload between peers in the second round of EAP when double EAP is negotiated. PKMv2: MS→ BS AuthRelay: BS → Authenticator
		RSP	AuthRelay: Authenticator → BS PKMv2: BS→ MS

1   Note: AuthRelay messages are not formatted as PKMv2 messages – e.g. does not include CMAC TLV, PKMv2
2   header Identifier field, etc. that are created in BS.

3   WiMAX Authenticator is collocated with AAA client and acts in a pass-through mode with one exception: when
4   cert-based device authentication terminates in the ASN the Authenticator MAY act as the EAP Server.

5   The Authenticator issues EAP messages over AuthRelay and transfers EAP messages as a payload between
6   AuthRelay and RADIUS:

7   • Initiates EAP process by sending EAP identity request message over AuthRelay (using the appropriate
8   AuthRelay Message Type);

1   •   EAP message received on AuthRelay is transferred to the AAA server in EAP-Message attribute(s) of
2   RADIUS Access-Request message;

3   •   EAP message received in EAP-Message attribute(s) of RADIUS Access-Challenge, Access-Accept or
4   Access-Reject is transferred to the BS over AuthRelay (using the appropriate AuthRelay Message Type).

5   The Authenticator SHOULD manage EAP messages retransmissions (over AuthRelay) according to EAP
6   retransmission timers.

7   The AuthRelay protocol does not handle packet duplication nor "in sequence packet delivery". Both cases are to be
8   handled at the EAP level (using EAP Identifier field).

9   ### 4.4.3   Accounting

10   **4.4.3.1   Introduction**

11   Both offline (post-paid) and online (prepaid) accounting, and hot-lining protocols and procedures are described in
12   this section. The accounting will cover user billing while user is in home network or roaming.

13   **4.4.3.2   Accounting Modes and Terminology**

14   This section details the terminology and supported accounting modes used in WiMAX. Figure 4-16 shows the
15   different possible levels and related identities or identifiers. Two different modes with different granularity for
16   actual generation of accounting information are supported: IP-session accounting and PD-flow accounting.
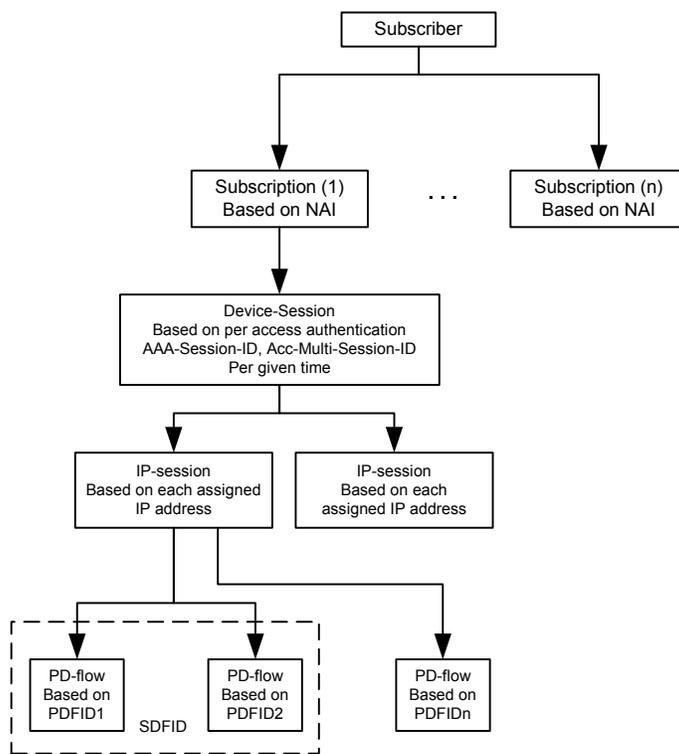
17

18   **Figure 4-16 – Accounting Modes and Terminology**

19   Accounting in WiMAX is based on a subscription that is identified through the subscription's NAI. A single
20   subscriber can have multiple subscriptions. However, methods for correlating accounting information across several
21   subscriptions of the same subscriber, is outside the scope of WiMAX.

1   **Table 4-18 – Relation of Subscriber and Subscription**

Identity	Description	ID
Subscriber	A subscriber owns one or more subscriptions with one or several (home) operators.	Not relevant for this specification. CUI may be used for correlating different subscriptions of a subscriber.
Subscription	A subscription may be used with different devices or may be bound to a specific device. At any given time a subscription can only be active in one device.	Username part of the NAI

2   Note: The term 'user', as for user authentication that is used throughout this specification, equals a subscription in
3   WiMAX accounting.

4   Accounting modes are defined in Table 4-19. Actual collection of accounting information happens either in IP-
5   session mode or in PD-flow mode, where ASN and CSN support for IP-session accounting is mandatory and support
6   for PD-flow accounting is optional.

7   **Table 4-19 – Accounting Modes**

Accounting Mode	Description	ID
IP-session	One or more IP-sessions map to the same device-session. IP-sessions are based on assigned IP addresses to an actual subscription/device pair. An example is an IP session for IPv4 and another session for IPv6.	IP address assigned to the MS
PD-flow	If packet data flow based accounting is used, there are one or more PD-flows mapping to the same IP session. A PD-flow can be mapped to one or more service data flows (see QoS section for detailed mapping). Several PD-flows can be grouped by a service data flow, identified by an SDFID.	PDFID, SDFID

8   The concept of a device-session is defined in addition to the above accounting modes, to group IP-sessions
9   belonging to the same subscription. This is not used as an actual mode to collect accounting information, however.
10 A device-session is defined by the authentication session started by initial network entry of an MS. Re-
11 Authentication does not terminate a Device-Session. Valid identifiers for identifying a device-session are the AAA-
12 Session-ID or the Acct-Multi-Session-ID.

13 ### 4.4.3.3   On-line Accounting (Prepaid Services)

14 On-line accounting also known as Prepaid Services is an optional to implement feature. On-line accounting
15 involves three entities: the Prepaid Client (PPC), the Prepaid Agent (PPA), and the Prepaid Server (PPS).

16 The PPS is assumed to be collocated with the HAAA in the HCSN. The PPC is located at the ASN in the NAS
17 and/or the HCSN or VCSN in the HA. The PPC performs metering when it is in the bearer path. When the PPC is
18 not on the bearer path, the PPA is responsible for metering the flows on behalf of the PPC and is located in the ASN
19 at the bearer path (ie., anchor DPF). The PPA communicates with the PPC over R4.

20 The normative Stage 3 Annex – Prepaid Accounting provides the specification for the operation of On-Line
21 Accounting. This section describes the WiMAX specifics operation as they pertain to On-line accounting. Section
22 5.4 specifies the On-line RADIUS attributes.

23 On-line accounting is set up by the exchange of RADIUS Access-Request and Access-Accept packets. The initial
24 Access-Request packet from the NAS and or the HA includes a prepaid accounting capability (PPAC) VSA to the
25 PPS indicating support for On-line accounting at the ASN and or the HA.. If the Subscription Session requires on-

1   line charging the PPS assigns a prepaid accounting quota (PPAQ) to the PPC using RADIUS access accept packets.
2   As the session continues, the PPC and the PPS replenish the quotas by exchanging RADIUS packets. A typical on-
3   line interaction is illustrated in Figure 4-17.

4   Off-line accounting SHALL also be used for subscribers that use Prepaid Services.
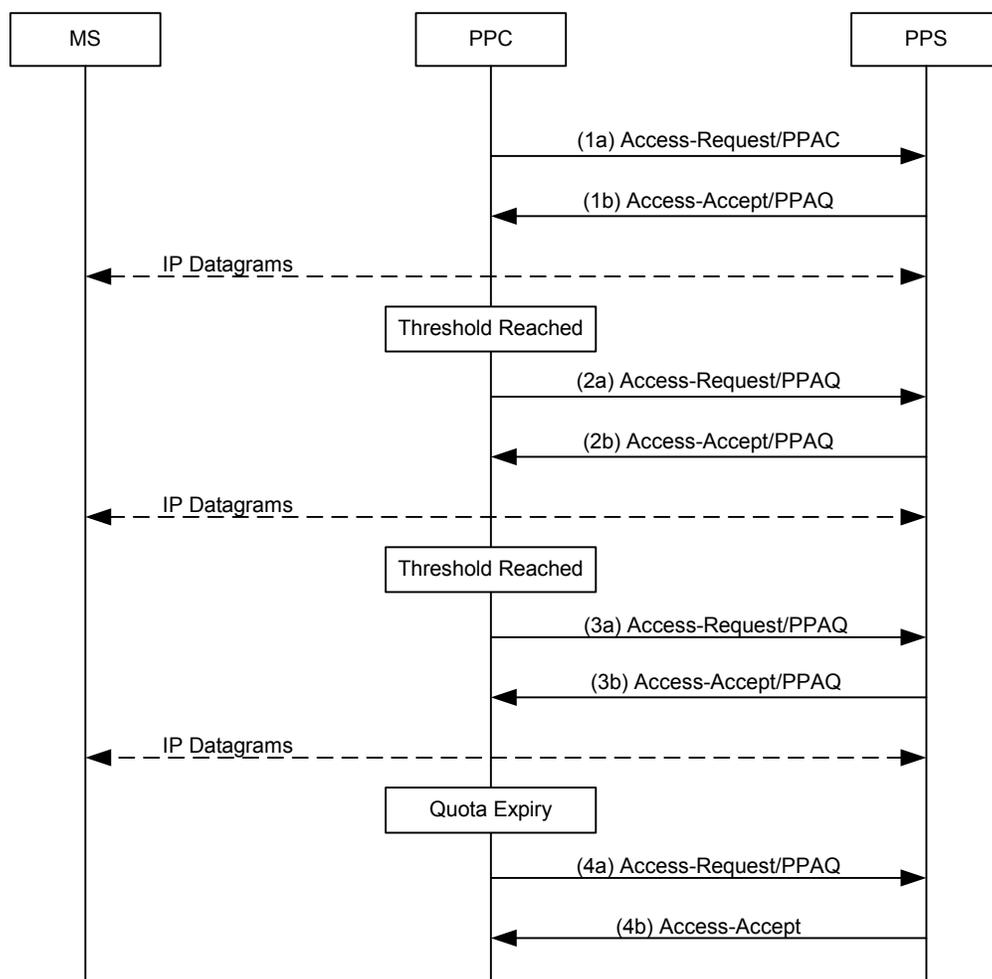
5

6   **Figure 4-17 – Online Accounting Procedures**

7   **STEP 1a**

8   During network entry a NAS sends an Access-Request packet to the HCSN. If the NAS supports a PPC then the
9   NAS includes the PPAC attributes indicating its Prepaid capabilities.

10 **STEP 1b**

11 If the Subscription Session is a prepaid session the HAAA (PPS) assigns the initial prepaid quota(s) by including
12 one or more PPAQ attributes in the Access-Accept packet.

13 **STEP 2a**

14 Once the threshold for the quota(s) is reached, the PPC requests additional quota by sending an Authorize-Only
15 Access-Request, containing one or more PPAQ indicating which quota(s) need to be replenished to the PPS.

STEP 2b

The PPS responds back with an Access-Accept packet containing one or more replenished quotas.

STEP 3a

Once again a threshold is reached for one or more of the quotas and the PPC requests more quotas by sending an Authorize-Only Access-Request to the PPS.

STEP 3b

The PPS responds back with the final quota in an Access-Accept. The final quota is indicated by the presence of the Terminate-Action subtype indicating the action for the PPC to take once quota is reached.

STEP 4a

The quota expires. The PPC sends an Authorize-Only Access-Request packet indicating that the quota has expired.

STEP 4b

The PPS responds back with an Access-Accept. If there were additional resources, the PPS could have allocated additional quotas at this time and the service could have continued.

On-line accounting can be IP-session based or Flow based. For IP-session based quotas are allocated to each IP-Session. The Service-ID in the PPAQ SHALL be set to the IP-Address corresponding to the IP-Session as specified in section 5.4.

For flow based accounting quotas are allocated to each packet data flow. The Service-ID attribute of the PPAQ SHALL identify the IP Session and the flow. The format of this attribute is specified in section 5.4.

4.4.3.3.1 Accounting Information Collection and UDR Structure

The accounting information collection points are at the accounting agents that may be located at:

a. The BS, which reports counts of all data packets and octet counts sent and received to/from the mobile over-the-air and other information that is available and metered at the base station. Accounting information collection at the BS is optional and is specified in Section 5.4. If the BS compresses the data over-the-air, it MAY report either uncompressed or compressed counts.

b. The Anchor/Serving DPF which reports signaling and user data packets and octet counts to/from the mobile. The Anchor/Serving DPF SHALL report counts for the user data. Report of control and signaling data is optional.

UDRs may also be collected by the AAA client at the CSN/HA. The UDR generated at the HA are sent over the AAA infrastructure to the home network (which is the accounting server in the CSN). The HA may generate all or a subset of accounting records that are generated at the Anchor/Serving DPF.

4.4.3.3.1.1 NAS/HA Requirements

If the NAS/HA support On-line accounting capabilities then they SHALL include the PPAC attribute in the RADIUS Access-Request packets.

In WiMAX, the HA and NAS SHALL support [28] and therefore the NAS and HA do not need to include the STC attribute as specified in the appendix.

4.4.3.3.1.2 HAAA Requirements

If the HAAA does not receive an PPAC attribute in the Access-Request packet from the NAS/HA, then the HAAA SHALL assume that device does not support On-line Accounting.

4.4.3.3.2 Tariff Switching

Tariff switching with both the volume and duration based prepaid services are initiated at the Home RADIUS/PPS.

4.4.3.3.3 Offline Switching Procedures

Offline Switching refers to the tariff switch from online accounting to offline accounting. When the prepaid account of user is depleted, the PPC will stop the online accounting service. If the user also has a postpaid account and is authorized to switch to offline accounting based on profile or rule, the ASN can notify the Accounting Client using the RADIUS Acct-Request (Start) message. The ASN will create the UDR and send an offline RADIUS accounting-request to AAA server. This switch ensures continued service.

4.4.3.4   Offline (Post-Paid) Accounting

4.4.3.4.1 Concept

This section describes the off-line (post-paid) accounting procedures. A user may connect to a network using more than one device. Each device maintains a device-session and one or more IP-sessions. Each IP-session may have a number of flows. This accounting model is illustrated in Figure 4-16.

According to this model, accounting can be done at two different levels. It can be IP-session based, or PD-flow based. In other words, accounting records can be collected per IP session or per PD flow, respectively. The AAA authorizes network access per device session. Since a subscriber can access multiple networks with multiple subscriptions simultaneously, subscriber or subscription based accounting can only be done after accounting records are consolidated at the AAA and correlated at the back office. Hence the specification of subscriber or subscription based accounting is out of scope of this document. IP session based accounting is mandatory to support by the ASN and CSN. PD flow based accounting is optional for both. If both accounting method are supported by the ASN, the CSN can select which accounting method is to be used for the session. See section 4.4.3.4.4.If the ASN supports PD flow based accounting and the CSN chooses IP session based accounting, the ASN may report IP session based accounting to the CSN by consolidating PD flow based accounting records per IP session.

PD flow based accounting has the flexibility to support IP-session based accounting by providing a mechanism to correlate PD-flow based accounting records per IP-session. The following description applies to both IP-session based accounting and PD-flow based accounting. However, if the vendor chooses to implement IP session based accounting in the ASN, then the description of PD-flow id or QoS profile id becomes irrelevant.

In the context of PD-flow based accounting, a flow represents a packet data flow that is identified by a packet data flow ID (PDFID). A PD flow is the flow for which an accounting client creates accounting records and reports them to the accounting server. A packet data flow is mapped to service flows that are identified by SFIDs. The mapping between the PDFID and the SFID is in the QoS specification in this document. The relationship between PDFIDs and Acct-Multi-session-Id is described in section 4.4.3.4.1. Note, the SFID is a layer 2 identifier and therefore not visible to the accounting function.

A service data flow provides a data service to a user. It consists of one or more PD flows to provide such a service. For example, a video conference data service is a service data flow that consists of audio PD flows, video PD flows, etc. In order to help accounting function to associate PD flows to a service data flow, a service data flow ID (SDFID) is available in the accounting record when flow based accounting is used and service data flow is created by the SFA.

Each PD-flow contains (see section 4.4.3.4.3 for details):

- a packet data flow identifier (PDFID)
- a service data flow identifier (SDFID)
- a QoS profile identifier
- a serving systems identifier (such as NAP ID)
- a device identifier (such as MSID)
- a session-id
- a user id (such as NAI or CUI)

Accounting information is kept in User Data Records (UDR) by the accounting client at the anchor authenticator or at the HA. The information includes the number of octets received or transmitted, and also the length of time the flow was active or reserved. Offline accounting information is generated by the accounting agent located at the anchor DPF or Serving DPF and/or the BS. The accounting agent in the Serving or Anchor DPFs counts the

1 uncompressed IP traffic to/from the mobile. When located at the BS, the accounting agent may report byte counts
2 for the dropped frame over the air.

3 As the MS moves around and changes the BS, the accounting client at the anchor authenticator continues to collect
4 and aggregate accounting information from the new accounting agent. As long as the anchor authenticator does not
5 change, the accounting session remains the same. While the accounting client is at the anchor aunthenticator, the
6 relationship between accounting client and accounting agent is illustrated in Figure 4-18.

7
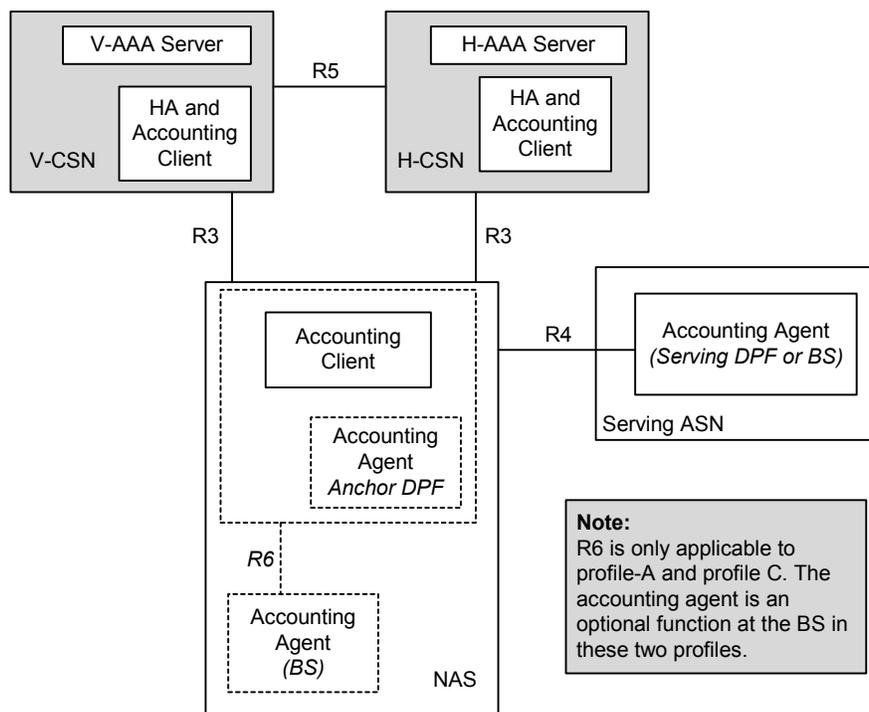
8 **Figure 4-18 – Accounting Client and Agent**

9 An accounting session is delineated by an Accounting-Request-Start and an Accounting-Request-Stop as per [27]
10 and is identified by the Acct-Session-Id. If PD-flow based accounting is used, an Accounting Session is established
11 at the creation of each PDFID. If IP-session-based accounting is used, an Accounting Session is established at the
12 time of IP address allocation. At the lifetime of a device-session, multiple Accounting Sessions as indicated by
13 Accounting-Starts and Stops may be generated.

14 Anchored Authenticator (NAS) movement triggers Accounting Segmentation. It generates one or more Accounting
15 Stop messages with the session continue attribute set to true at the old NAS, and one or more Accounting Start
16 messages with the beginning of session attribute set to false at the new NAS. For any other movements like DPF
17 relocation, Accounting Segmentation SHALL NOT occur.

18 Upon authenticator relocation, the same AAA-Session-ID is used for correlating old accounting session with the
19 new accounting session. AAA SHALL send the same AAA-Session-ID to the new serving authenticator if the
20 Service-Type is to "Authenticate only" in the RADIUS Access-Request message.

21 An Acct-Multi-Session-Id is used to correlate accounting records for multiple IP flows under a session. The Acct-
22 Multi-Session-Id is the AAA session id assigned at network access.

23 Accounting procedures per accounting session are illustrated in Figure 4-19.

1
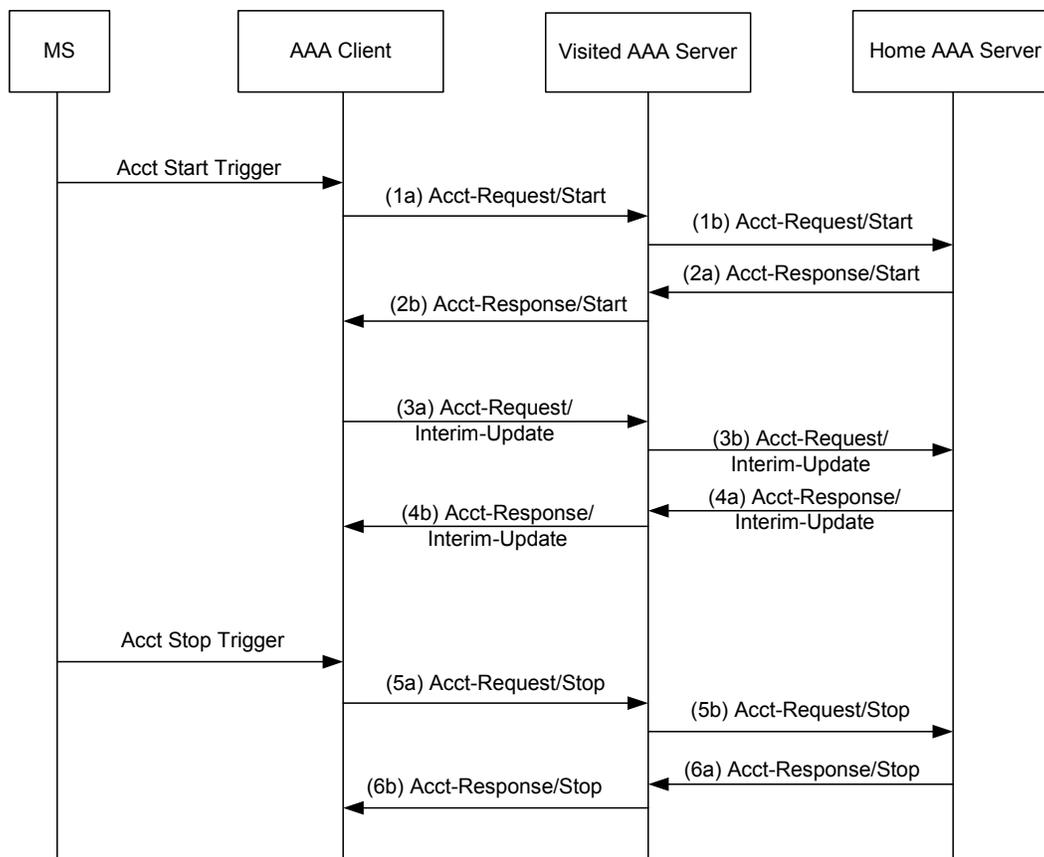
2 **Figure 4-19 – Offline Accounting Procedures**

3 In these procedures, the RADIUS Client creates independent accounting session for each Packet Data Flow, if PD-
4 flow accounting is supported. Packet Data Flow creation causes the ASN to take accounting action. When the
5 accounting client sends a RADIUS Accounting-Request message, it SHOULD include the packet data flow
6 information.

7 **4.4.3.4.2 Protocol**

8 WiMAX Release 1.0.0 is based on RADIUS Accounting as specified by [9] and [10]. This specification adds
9 additional requirements to accounting.

10 **4.4.3.4.2.1   Types of Accounting Packets**

11 There are three types of accounting packets:

12 • Accounting Request (Start)

13 • Accounting Request (Interim)

14 • Accounting Request (Stop)

15 Accounting-Request (Start) packets are mandatory to implement for the accounting client. It signals the beginning of
16 an IP-session or a PD-flow.

17 Accounting-Request (Interim) packets are optional to implement for the Accounting Clients. These packets are used
18 to periodically report accounting for the IP-session of the PD-flow. The purpose of Interim records is to mitigate
19 revenue loss due to a loss of a stop record. The HAAA controls the Accounting Interim rate by specifying the
20 number of seconds between Accounting Request (Interim) packets in the Acct-Interim-Interval(85) [9] which is sent
21 in Access-Accept packet. In the absence of this attribute, the interval between Accounting-Request (Interim) packets
22 is chosen by the accounting client.

1 Accounting-Request (Stop) packets are mandatory to implement for the accounting client. This information
2 represents the final count for the IP-session of the PD-flow.

3 Each Accounting Start/Stop packet delineates a complete IP session or a PD flow or a segment of an IP session. An
4 IP session or a PD flow may consist of several accounting segments. Accounting segmentation occurs due to:

5 • Accounting client relocation caused by anchored authenticator movement

6 • Change in Status such as hot-line state

7 The accounting attributes Beginning-of-Session, and Session-Continue help in the interpretation of the Accounting-
8 Request packets as shown in Table 4-20.

9 **Table 4-20 – Interpretation of Accounting- Request Packets**

Acct-Status-Type	Beginning-of-Session	Session-Continue	Description
Start	TRUE	N/A	Beginning of the first accounting segment for an IP session or a PD flow.
Start	FALSE (or missing)	N/A	Beginning of a subsequent accounting segment of an IP session or a PD flow
Stop	N/A	TRUE	The end of the accounting segment. Another accounting segment is starting expect an Accounting-Request (Start).
Stop	N/A	FALSE(or missing)	This is the end of the IP session or the PD flow.

10 **4.4.3.4.2.2   Transmission and Reception of Accounting Messages**

11 RADIUS supports two types of accounting record transmission. In the pass through style, the forwarding server
12 (RADIUS proxy) forwards accounting messages as soon as it receives the packet, or in batch style where it
13 acknowledges the reception of a accounting message and forwards it later.

14 WiMAX RADIUS proxies (between the accounting client and the Home CSN) SHALL act in a "pass through" style
15 as defined by [10].

16 As the UDRs are transported over the AAA infrastructure they may be routed through proxy servers in the Visited
17 CSN and in other broker networks. These entities may capture the accounting stream and use it to reconcile billing
18 with their partners and also for auditing purposes. The entities should not modify the accounting stream.

19 Unless otherwise specified, accounting messages do not have to follow the same path as the authentication
20 messages. The routing path of accounting packets is a matter of business agreement between ASN and CSN
21 providers.

22 **4.4.3.4.3 Accounting Information Collection and UDR Structure**

23 The accounting information collection points are at the accounting agents that may be located at:

24 • The BS, which reports counts of all data packets and octet counts sent and received to/from the mobile
25 over-the-air and other information that is available and metered at the base station. Accounting information
26 collection at the BS is optional and is specified in section 5.4.

27 • The Anchor/Serving DPF which reports signaling and user data packets and octet counts to/from the
28 mobile. The Anchor/Serving DPF reports separate counts for signaling, user data.

29 UDRs may also be collected by the AAA client at the CSN/HA. The UDR generated at the HA are sent over the
30 AAA infrastructure to the home network (which is the accounting server in the CSN). The HA may generate all or a
31 subset of accounting records that are generated at the Anchor/Serving DPF.

1 UDR records conform to the RADIUS packet structure as defined by [10] and [9]. The payload of the record is
2 defined by WiMAX and is divided into logical blocks as follows.

3 **Table 4-21 – UDR Record Structure**

Block Type	Description
Status and Type	The attributes of this section define the type of accounting record, convey the state of the user and describe why the record is generated.
Record Correlators	The attributes in this section help in correlating the records such as Start, Stop, Interim, or to a flow, or to an IP session.
User Identification	The attributes in this section identify the user.
Infrastructure Identifiers	The attributes in this section identify the serving network.
Time	The attributes in this section identity the time the accounting took place. The time zone is also conveyed.
L3 Counters	The attributes in this section report the various L3 counters.
OTA Counters	The attributes in this section report the various over-the-air counters.
Flowspec	The attributes in this section report the flow specification.
QoS	The attributes in this section report the QoS assigned to the flow.

4 Each section contains one or more attributes that are defined by RFCs, and attributes specific to WiMAX. WiMAX
5 vendors may add additional attributes as required by specific deployments.

6 Some of the attributes are required and some are conditionally required or they are optional. The attributes defined
7 by WiMAX are specified in section 5.4.

8 ### 4.4.3.4.4 Procedures

9 #### 4.4.3.4.4.1   Accounting Mode Selection

10 During Network Access Authentication and Authorization, the NAS SHALL indicate what type of accounting it
11 SHALL be able to support using the WiMAX Capability attribute that is sent in the RADIUS Access-Request. If
12 the NAS is able to support IP session based accounting it SHALL set the IP session-base-Accounting bit and if it
13 supports Flow-based accounting it SHALL set the Flow-base-Accounting bit. The NAS SHALL at least support IP
14 session based accounting.

15 The HAAA server SHALL indicate the mode of accounting to apply to the MS. The HAAA server selects IP
16 Session based accounting by setting the IP session-base-Accounting bit in the WiMAX Capability attribute sent
17 back in the RADIUS Access-Accept packet. The HAAA server selects PD flow-based accounting by setting the
18 Flow-base-Accounting bit in the WiMAX Capability attribute sent back in the RADIUS Access-Accept packet. The
19 HAAA SHALL select one and only one of the accounting modes for a given IP session or   PD flow.

20 If the NAS receives an Access-Accept in which the HAAA did not select an accounting mode, or in which the
21 HAAA selected an accounting mode that is not supported by the NAS (as indicated in the Access-Request), the
22 NAS SHALL treat the Access-Accept as an Access-Reject and it SHALL not provide any service to the MS.

23 #### 4.4.3.4.4.2   Accounting Record Correlation

24 The record correlators in the accounting record provide correlation identifiers that support accounting record
25 correlation at different levels in the correlation hierarchy. Figure 4-20 illustrates the correlation hierarchy and the
26 correlation identifiers associated with each level of correlation.

1
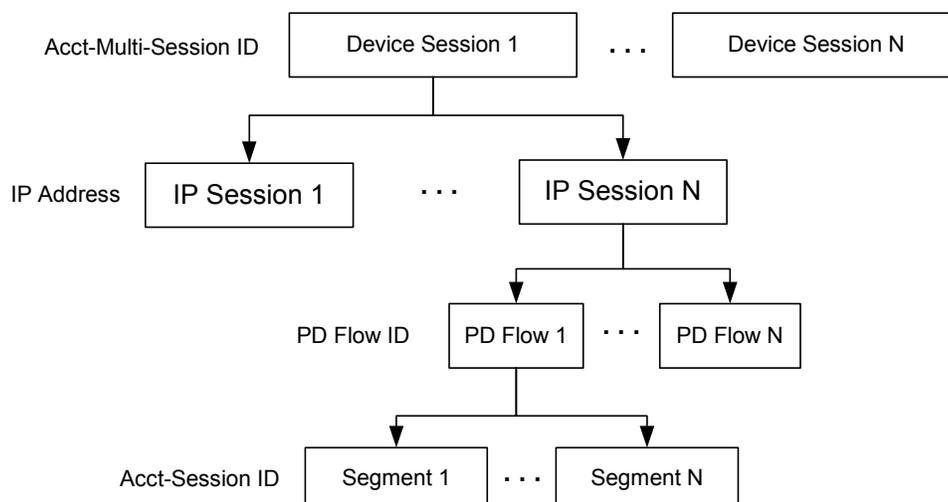
Figure 4-20 – Correlation Hierarchy

3 Different identifiers are used for correlation at different levels. The Acct-Multi-Session ID correlates accounting
4 records for a device session on a particular device for a given subscription. The IP address correlates accounting
5 records for an IP session on a given device session. PD Flow ID correlates accounting records for a PD flow. The
6 Acct-Session ID is used to match accounting Start/Interim/Stop messages for an accounting record on an accounting
7 segment. The Acc-Multi-Session ID is generated by AAA server. The IP address is the home address assigned to the
8 MS. The Packet Data Flow ID is also generated by the AAA server. Generation is described in the QoS section. And
9 finally, the Acct-Session ID is generated by the accounting client.

10 Note: The NAI is not used as a record correlator, as it may be a pseudonym that is only meaningful to the AAA
11 server and the MS. The AAA server, however, can use the (outer) NAI to correlate a device session to the
12 subscription and subscriber. This can also be used to relate different device sessions of the same subscription in the
13 AAA server. Also, the CUI can be used by the visited CSN to do record correlation.

14 ### 4.4.3.4.4.3   Idle Mode Notification

15 The anchor authenticator knows when an MS enters or exits the idle mode. (See Section "Idle Mode Entry" and
16 "Idle Mode Exit"). The accounting client collocated at the anchor authenticator may notify the accounting server at
17 the CSN of the idle mode transition using the accounting messages.

18 Idle mode notification can be negotiated at network access. During network access, the ASN SHALL indicate if it
19 supports idle mode notification using the Idle Mode Notification TLV in the WiMAX Capability attribute in the
20 RADIUS Access-Request. The HAAA SHALL indicate if it requires idle mode notification using the same TLV in
21 the Access-Accept.

22 If idle mode notification is supported at the ASN and is required by the CSN, the accounting client at the ASN
23 SHALL send an accounting interim update message with the Idle-Mode-Transition attribute when the MS enters or
24 exits the idle mode. The ASN SHALL only send an idle mode notification against the ISF and the message SHALL
25 not include counters.

26 ### 4.4.3.4.5 Tariff Switching

27 Tariff switching with both the volume and duration based prepaid services are initiated at the Home RADIUS/PPS.

28 In order to avoid a flood of messages over R6 from BS to ASN-GW at the Tariff Switch Time of Day (ToD) and
29 another flood of messages over R3 from ASN-GW to AAA for all of the RADIUS messages trigger by the Tariff
30 Switch, optional Tariff Switch attributes have been added the TLVs and messages described below.

31 • The Accounting Agent saves off the volume counts for a subscriber at the ToD time. When the next
32 accounting event/trigger happens for the subscriber those volume counts at ToD are sent to the Accounting
33 Client along with the regular volume counts. The Accounting Client then generates a RADIUS Stop
34 message to capture the accounting information before the ToD and a RADIUS Start message to indicate the

1   start of accounting after the ToD. Then the regular RADIUS message(s) are sent based on event/trigger
2   mentioned above. The RADIUS messages that include the volume counts at ToD are backdated to the
3   actual time of the ToD for accurate billing.

4   **4.4.3.5   Hot-lining**

5   As indicated in NWG Stage-2 document, the Hot-lining feature provides a WiMAX operator with the capability to
6   efficiently address issues with the users that would otherwise be unauthorized to access packet data services. The
7   hot-lining device (HLD) can be an FA located at the ASN, or a HA located at the CSN. As discussed in NWG
8   Stage-2 document, there are two methods defined by which the HAAA indicates that a user is to be hot-lined

9   •   Profile based Hot-lining: For the profile based Hot-lining, Hot-line profile(s) with all Hot-lining rules are
10   pre-provisioned at the HAAA. The HAAA sends a hot-line profile identifier in the RADIUS message
11   (Access-Accept and Change of Authorization) when the Hot-lining is activated.

12   •   Rule based Hot-lining: Hot-lining rules (filter rules, IP or HTTP redirection rules) are sent in the RADIUS
13   message (Access Accept and Change of Authorization) by the HAAA when the Hot-lining is activated.

14   Based on the status of the user's session, there are two ways users can be hot-lined,

15   •   Active Session Hot-lining: The user starts normal packet data session and in the middle of the session, the
16   HAAA receives trigger for Hot-lining from the Hot-lining Application (HLA).

17   •   New Session Hot Lining: The trigger from the HLA arrives prior to the user access authentication.

18   Once the hot-lining is resolved, the packet data session is returned to normal. Both these approaches are discussed in
19   the following sub-sections.

20   Only IP session based Hot-Lining procedures are defined in this document. PD flow based Hot-Lining may be
21   defined in the future version of this document.

22   **4.4.3.5.1 Active Session Hot-lining**

23   The active IP session hot-lining is invoked when the user is currently engaged in a packet data session and the
24   HAAA receives hot lining trigger from the HLA. Figure 4-21 depicts the call flow between the HLD, HAAA and
25   HLA.
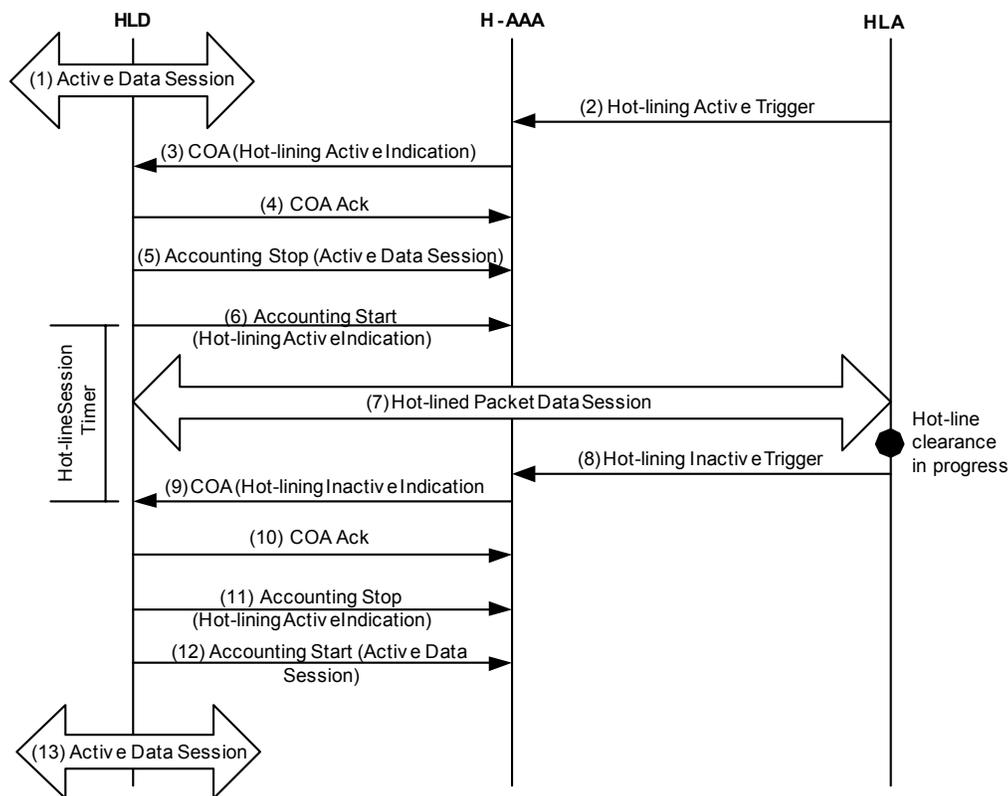
Figure 4-21 – Active IP Session Hot-lining

STEP 1

User is in an active IP session which is not Hot-lined.

STEP 2

The HLA detects that the user needs to be hot-lined. This is indicated to the HAAA by sending "Hot-lining Active Trigger". The details of these triggers are out of scope for Release 1.0.0.

STEP 3

Upon receiving the notification from the Hot-Line Application, the Home-AAA server records the Hot-Lining state against the user record in the database. The Home-AAA server will determine if the user has an ongoing packet data session. If the user has an ongoing packet data session, the Home-AAA server initiates the Active-Session Hot-Lining procedure. The Home-AAA server uses the contents of the Hot-Line Capability VSA and other local policies to determine which access device will be the Hot-Lining Device for the session, by sending RADIUS CoA-Request to the HLD with either Profile based Hot-lining or Rule based Hot-lining. See the table of attributes for hot-lining in section 5.4.1.4.

STEP 4

Upon receipt of the RADIUS COA:

- If the HLD can honor the request then it responds with a RADIUS COA Ack to the HAAA.

- If the HLD cannot honor the request then it SHALL respond with a COA NAK message. Based on the local policy, HAAA may either retry sending the Hot-Lining request to the HLD or it may send a RADIUS Disconnect Message (DM) to the HLD for terminating the session.

1 **STEP 5**

2 The HLD sends a RADIUS Accounting Request (Stop) indication for the active data session.

3 **STEP 6**

4 The HLD sends RADIUS Accounting Request (Start) for the hot-lined session. If Session-Timeout attribute was
5 included in step 3, the HLD initiates session teardown (i.e. tear down of the service flows associated with the IP
6 session) when the duration specified in the Session-Timeout attribute has elapsed and the user's session is still hot-
7 lined. . After tearing down the service flow(s), the HLD sends an Accounting Request (Stop) to the HAAA to inform
8 that the user's IP session has ended.

9 **STEP 7**

10 Since the user's data session is hot-lined in mid session, user's data traffic is affected. Based on the Hot-lining rules
11 set at the HAAA and indicated by it in the RADIUS COA earlier, the uplink and/or downlink data traffic of the user
12 is either dropped/disconnected, or blocked, and redirected to the HLA by the HLD.

13 **STEP 8**

14 Once the Hot-line status is applied to the user status, the HLA notifies the user of his/her hot-lined status and tries to
15 resolve the issue. The method of notification to the user is undefined in this document.

16 • If the condition which triggered the hot-lining session does not get cleared, the HLA may terminate the
17   session. In this case, the HAAA is notified by the HLA. Upon receipt of this notification, the HAAA
18   SHALL send a RADIUS Disconnect Message to the HLD where the accounting records are stopped and
19   the session termination is initiated. This may also happen automatically at the HLD, if the user's Hot-Lined
20   status does not change within the duration of the Session-Timeout value.

21 • Otherwise, if the condition that triggered Hot-lining session gets cleared (via an undefined procedure), the
22   HLA detects this and indicates to the HAAA to clear the Hot-lined status of the user by sending the Hot-
23   lining Inactive Trigger to the HAAA.

24 **STEP 9**

25 Upon receipt of the Hot-lining Inactive Trigger, the HAAA sends a RADIUS COA message to the HLD with
26 appropriate attributes. Note that this may not be the same HLD that initially handled the activation of the Hot-lining.
27 This may occur due to events like handoff.

28 **STEP 10**

29 Upon receipt of the RADIUS COA:

30 • If the HLD can honor the request then it will respond with a RADIUS COA Ack to the HAAA and Hot-line
31   Session-Timeout timer is turned off.

32 • If the HLD cannot honor the request then it SHALL respond with a COA NAK message. Based on the
33   local policy, the HAAA may either retry sending the Hot-Lining signal to the HLD or it may send a
34   RADIUS Disconnect Message to the HLD for terminating the session. In this case, the HLD sends a
35   RADIUS Accounting Request (Stop) message to the HAAA indicating the end of the IP session for the user
36   after it successfully processed the Disconnect Message and tears down the service flow(s) associated with
37   the IP session.

38 **STEP 11**

39 The HLD generates RADIUS Accounting Request (Stop) message for the hot-lined packet data session.

40 **STEP 12**

41 The RADIUS Accounting Request (Stop) message SHALL be followed by a RADIUS Accounting Request (Start)
42 message indicating the start of the normal packet data session.

1   **STEP 13**

2   User continues the packet data session and the traffic is routed normally.

3   During the Hot-Lined active status in the HLD (FA or the HA), the byte and packet counts for user's hot-lined IP
4   session SHALL not be counted towards the overall byte and packet counts. In this document, the byte/packet counts
5   during Hot-Line active status are not reported to the accounting server by the accounting client.

6   **4.4.3.5.2 New IP Session Hot-lining**

7   New IP session Hot-lining is invoked when the user starts a new IP session and the HAAA already has Hot-lining
8   status set for that IP session for that user. Figure 4-22 depicts the call flow between the HLD, HAAA and HLA.
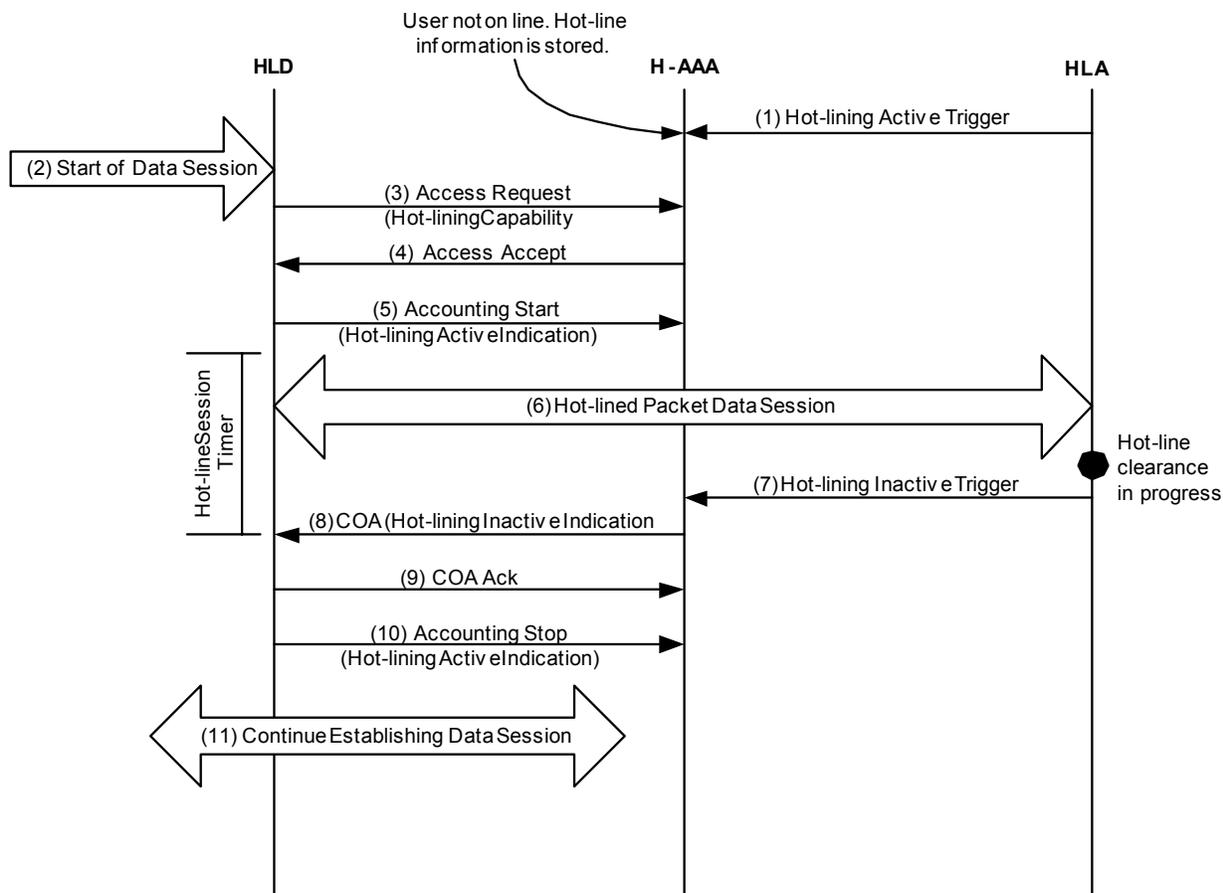
10   **Figure 4-22 – New IP Session Hot-lining**

11   **STEP 1**

12   The HLA hot-lines the user and indicates that to the HAAA by "Hot-lining Active Trigger". Hot-lining takes in
13   effect when the user attempts to initiate a packet data session (The details of events that cause the HLA to send the
14   Hot-Line Active trigger to the HAAA are not within the scope of this document).

15   **STEP 2**

16   User attempts to initiate an IP session. This is detected in the ASN as activation of one or more service flow(s).

1 **STEP 3**

2 Upon detection of new service flow(s) for the user, the HLD sends a RADIUS Access-Request to the HAAA to
3 authorize the user to establish the service flow(s). The HLD includes it Hot-Line capability in the Hot-Line
4 capability VSA in the Access-Request.

5 **STEP 4**

6 At the HAAA, the local Policy and received Hot-Line Capability in the RADIUS Access Request is used to
7 determine which HLD will be used to hot-line the session. This is because more than one HLD may send this
8 session setup indication with Hot-Line capability to the HAAA. In case of the HA acting as the HLD, the trigger for
9 detecting a new IP session is the reception of an Mobile IP RRQ or BU from the user. Depending on the type of
10 method (either profile based hot-ling or Rule based Hot-lining) selected at the HAAA, it sends a RADIUS Access
11 Accept to the HLD with the appropriate attributes.

12 **STEP 5**

13 The HLD sends RADIUS Accounting Request (Start) for the hot-lined session. If Session-Timeout attribute was
14 included in step 3, the HLD initiates session teardown (i.e. tear down of the service flows associated with the IP
15 session) when the duration specified in the Session-Timeout attribute has elapsed and the user's session is still hot-
16 lined. . After tearing down the service flow(s), the HLD sends an Accounting Request (Stop) to the HAAA to inform
17 that the user's IP session has ended.

18 **STEP 6**

19 Based on the Hot-lining rules set at the HAAA and indicated by it in the RADIUS Access-Accept earlier, the uplink
20 and/or downlink data traffic of the user is either dropped/disconnected, or blocked, or blocked and redirected to the
21 HLA by the HLD.

22 **STEP 7**

23 Once the Hot-line status is applied to the user status, the HLA notifies the user of his/her Hot-lined status and try to
24 clear the Hot-line status. The method of notification to the user is undefined in this document.

25 • If the condition that triggered Hot-lining session does not get cleared, the HLA may terminate the session.
26 In this case, the HAAA is notified by the HLA. Upon receipt of this notification, the HAAA SHALL send a
27 RADIUS Disconnect Message to the HLD where the accounting records are stopped and the session
28 termination is initiated. This may also happen automatically at the HLD, if the user's Hot-Lined status does
29 not change within the duration of the Session-Timeout value.

30 • Otherwise, if the condition that triggered Hot-lining session gets cleared (via an undefined procedure), the
31 HLA detects this and indicates to the HAAA to clear the Hot-line status of the user by sending the Hot-
32 lining Inactive Trigger to the HAAA.

33 **STEP 8**

34 Upon receipt of the Hot-lining Inactive Trigger, the HAAA sends a RADIUS COA message to the HLD with
35 appropriate attributes. Note that this may not be the same HLD that initially handled the activation of the Hot-lining.

36 **STEP 9**

37 Upon receipt of the RADIUS COA,

38 • If the HLD can honor the request then it will respond with a RADIUS COA Ack to the HAAA and Hot-line
39 Session-Timeout timer is turned off.

40 • If the HLD cannot honor the request then it SHALL respond with a COA NAK message. Based on the
41 local policy, the HAAA may either retry sending the Hot-Lining signal to the HLD or it may send a
42 RADIUS Disconnect Message to the HLD for terminating the IP session.

1 **STEP 10**

2 The HLD sends a RADIUS Accounting Request (Stop) to the HAAA.

3 **STEP 11**

4 User continues establishing the IP session.

5 **4.4.3.6   Accounting Messages**

6 **4.4.3.6.1   R6 Reference Point**

7 **4.4.3.6.1.1   RR_Req (Create) / HO_Req / Context_Rpt / IM_Exit_State_Change_Rsp**

8 The Accounting Extensions TLV is sent in *RR_Req* (Create) during Service Flow Creation, in *HO_Req* during
9 Controlled HO, in *Context_Rpt* during Uncontrolled HO and *IM_Exit_State_Change_Rsp* during Idle Mode Exit.
10 The TLV is included only once even if multiple flows are included in the message.

11 **Table 4-22 – RR_Req (Create) / HO_Req / Context_Rpt / IM_Exit_State_Change_Rsp Message**
12 **Structure**

IE	Description	M/O	Notes
…			
Accounting Mode Provisioning	Accounting Mode Provisioning	O	This accounting extension is sent by the accounting client at the ASN-GW to the accounting agent during service flow creation, HO, and exiting idle mode.

13 **4.4.3.6.1.2   RR_Rsp (Modify and Delete)**

14 *RR_Rsp* (Modify and Delete) contains the Accounting Session/Flow Volume Counts TLV for Service Flow
15 Modification and Deletion. If per service flow accounting information is reported by the accounting agent,
16 accounting information associated with one or more service flows are included in the *RR_Rsp* (Modify and Delete)
17 then a separate Accounting Session/Flow Volume Counts TLV should be included for each flow.

18 **Table 4-23 – RR_Rsp (Modify and Delete) Message Structure**

IE	Description	M/O	Notes
…			
Accounting Session Flow Volume Counts	Accounting counts info for a subscription which is either per IP session or per service flow	O	This accounting extension is sent by the accounting agent to the accounting client at the ASN-GW during service flow modification and deletion.

19 **4.4.3.6.1.3   Bulk Interim Update**

20 The Bulk Interim Update contains volume counts for several subscribers in one message. It is only used for volume-
21 based accounting. This message is sent by the BS to the ASN-GW. The Ack message does not contain any TLVs, it
22 is just a confirmation to the BS that the ASN-GW received the Bulk Interim Update. The accounting client at the
23 ASN-GW will unbundle the bulk counts and construct the UDRs separately for each MS based on the corresponding
24 MSID and the accounting granularity.

1
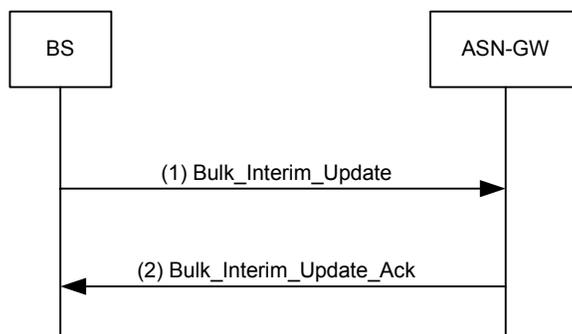
2   **Figure 4-23 – Bulk Interim Update**

3   **Table 4-24 – Bulk Interim Update Message Structure**

IE	Description	M/O	Notes
Accounting Bulk Session/Flow Volume Counts	The volume count information for one or more subscribers.	M	The information in this TLV is repeated per subscription served by a particular accounting agent at either the IP-session level or service flow level granularity

4   **4.4.3.6.1.4   R6 Path Deregistration Request/ R6 IM_Entry_State_Change_Req**

5   R6 *Path_Dereg_Req* and R6 *IM_Entry_State_Change_Req* contain the Accounting Bulk Session/Flow Volume
6   Counts Info TLV for Idle Mode Entry and de-registration from the network.

7   **Table 4-25 – R6 Path_Dereg_Req / R6 IM_Entry_State_Change_Req Primitive Structure**

IE	Description	M/O	Notes
…			
Accounting Bulk Session/Flow Volume Counts	The volume count information for this subscriber.	O	This accounting extension is exchanged between accounting agent at the BS and the accounting client at the ASN-GW for Idle Mode Entry and de-registration from the network

8   **4.4.3.6.2 R4 Reference Point**

9   **4.4.3.6.2.1   RR_Req (Create) / HO_Req / Context_Rpt / IM_Exit_State_Change_Rsp**

10 The Accounting Extensions TLV is sent in the RR_Req (Create) during Service Flow Creation, in *HO_Req* during
11 Controlled HO, and in *Context_Rpt* and *IM_Exit_State_Change_Rsp* during Idle Mode Exit. The TLV is included
12 only once even if multiple flows are included in the message.

13   **Table 4-26 – RR_Req (Create) / HO_Req / Context_Rpt / IM_Exit_State_Change_Rsp Message**
14   **Structure**

IE	Description	M/O	Notes
…			
Accounting Mode Provisioning	Accounting Mode Provisioning	O	This accounting extension is exchanged between ASNs during service flow creation, Controlled HO and Idle Mode Exit.

1   **4.4.3.6.2.2   RR_Rsp (Modify and Delete)**

2   The *RR_Rsp* (Modify and Delete) contains the Accounting Session/Flow Volume Counts TLV for Service Flow
3   Modification and Deletion. If the ASN receives the Accounting Session/Service Flow Volume Counts TLV in the
4   *RR_Rsp*, this TLV is relayed in the *RR_Rsp* message to the ASN where the Accounting Client is resided. If per
5   service flow accounting information is reported by the accounting agent, separate Accounting Session/Flow Volume
6   Counts TLV should be included for each flow.

7   **Table 4-27 – RR_Rsp (Modify and Delete) Message Structure**

IE	Description	M/O	Notes
…			
Accounting Session Flow Volume Counts	Accounting counts info for a subscription which is either per IP session or per service flow	O	This accounting extension is exchanged between ASNs during service flow modification and deletion.

8   **4.4.3.6.2.3   Bulk Interim Update**

9   The Bulk Interim Update contains volume counts for several subscribers in one message. It is only used for volume-
10   based accounting. This message is sent over the R4 interface upon receipt of the Bulk Interim Update message over
11   the R6 interface. Note that the response message does not contain any TLVs.

12   **Table 4-28 – Bulk Interim Update Message Structure**

IE	Description	M/O	Notes
Accounting Bulk Session/Flow Volume Counts	The volume count information for one or more subscribers.	M	The information in this TLV is repeated per subscription served by a particular accounting agent at either the IP-session level or service flow level granularity

13   **4.4.3.6.2.4   R4 Path_Dereg_Req / R4 IM_Entry_State_Change_Req**

14   R4 Path_Dereg_Req and R4 IM_Entry_State_Change_Req contain the Accounting Bulk Session/Flow Volume
15   Counts TLV for Idle Mode Entry and de-registration from the network.

16   **Table 4-29 – R4 Path_Dereg_Req / R4 IM_Entry_State_Change_Req Message Structure**

IE	Description	M/O	Notes
…			
Accounting Bulk Session/Flow Volume Counts	The volume count information for this subscriber.	O	This accounting extension is exchanged between ASNs for Idle Mode Entry and de-registration from the network.

17

18   **4.4.3.7   Accounting Events in the ASN**

19   The accounting events control the generation of Accounting-Request Start, Stop and Interim messages at the
20   Accounting Client in the ASN.

21   The accounting client collocated in the Authenticator ASN SHALL generate the Accounting-Start or Accounting-
22   Stop messages based on some events as described below and based on the accounting type indicator received from
23   the HAAA in the Access-Accept message at the time of Authentication.

24   The Accounting-Request Start message is sent when one of the following events occurs at the Accounting Client:

1   a.   When an IP address is assigned to the MS.

2   b.   At a specific time of the day

3   c.   At the onset of Hot-Lining of an ongoing IP session.

4   d.   At the reset of Hot-Lining of an ongoing IP session.

5   e.   In case of PD flow based accounting, at the time when a PDFID is allocated to a service flow..

6   The Accounting-Request Stop message is sent when one of the following events occurs at the Accounting Client:

7   a.   When an IP address is de-allocated for the MS. This is normally the indication of an IP session termination.

8   b.   At a specific time of the day

9   c.   At the onset of Hot-Lining of an ongoing IP session.

10   d.   At the reset of Hot-Lining of an ongoing IP session.

11   e.   In case of PD flow based accounting, at the time when service flow terminated for the PDFID.

12   f.   Due to overflow of any of the counters.

13   4.4.3.8   Accounting Events in the CSN

14
15   The accounting client in the Home Agent in the CSN SHALL generate Accounting-Request Start message based on the following events:

16   a.   Upon successful creation of a mobility binding for a MS.

17
18   b.   Upon successful modification of an ongoing mobility binding for a MS (subsequent to an Accounting-Request Stop for the ongoing mobility binding).

19   c.   At a specific time of the day

20   d.   At the onset of Hot-Lining of an ongoing IP session.

21   e.   At the reset of Hot-Lining of an ongoing IP session.

22
23   The accounting client in the Home Agent in the CSN SHALL generate Accounting-Request Stop message based on the following events:

24   a.   Upon successful deletion of a mobility binding for a MS.

25
26   b.   Upon successful modification of an ongoing mobility binding for a MS (prior to an Accounting-Request Start for the ongoing mobility binding).

27   c.   At a specific time of the day.

28   d.   At the onset of Hot-Lining of an ongoing IP session.

29   e.   At the reset of Hot-Lining of an ongoing IP session.

30   f.   Due to overflow of any of the counters.

31   Illustrations of the Accounting Start Events in the ASN

32   The purpose of the figures in this section is to contextualize the accounting triggers. The figures are informative.
33   For further details refer to the specific sections in this document.
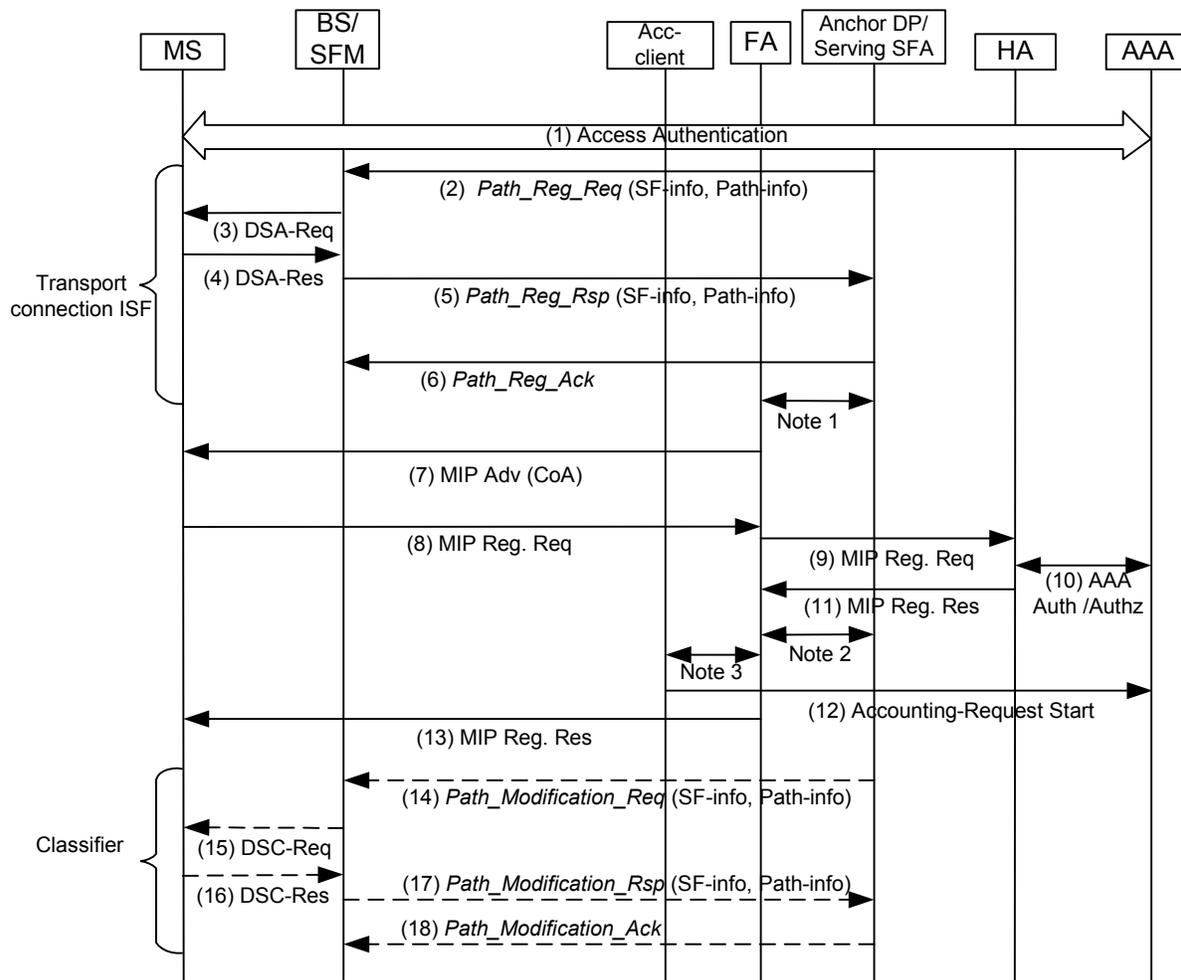
Note 1: Serving SFA triggers FA to initiate MIP registration (out of scope of spec)
Note 2: FA triggers the Anchor DP/Serving SFA to update the SF classifier. (out of scope of spec)
Note 3: FA triggers the Acc client to generate Accounting-Request Start (out of scope of spec)

1

2   **Figure 4-24 – In Case of CMIP4**
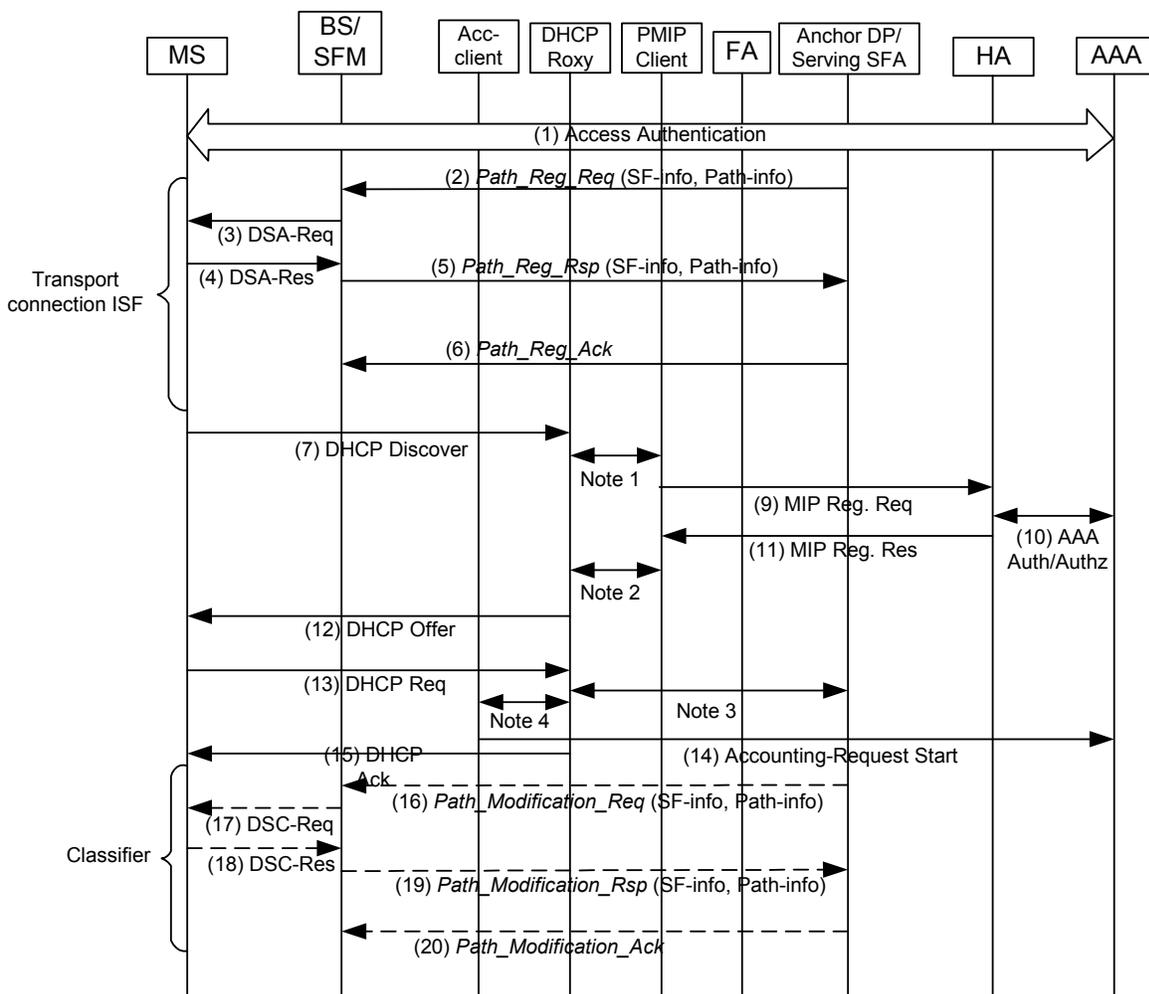
Note 1: DHCP Proxy trigger PMIP client to initiate MIP registration (out of scope of this section)
Note 2: PMIP client trigger the DHCP proxy and passes MIP registration response information. (out of scope of this section)
Note 3: DHCP proxy triggers the Anchor DP/Serving SFA to update the SF classifier. (out of scope of this section)
Note 4: DHCP proxy triggers the Acc Client to generate Accounting-Request Start (out of scope of this section)

1

2 **Figure 4-25 – In Case of PMIP4**
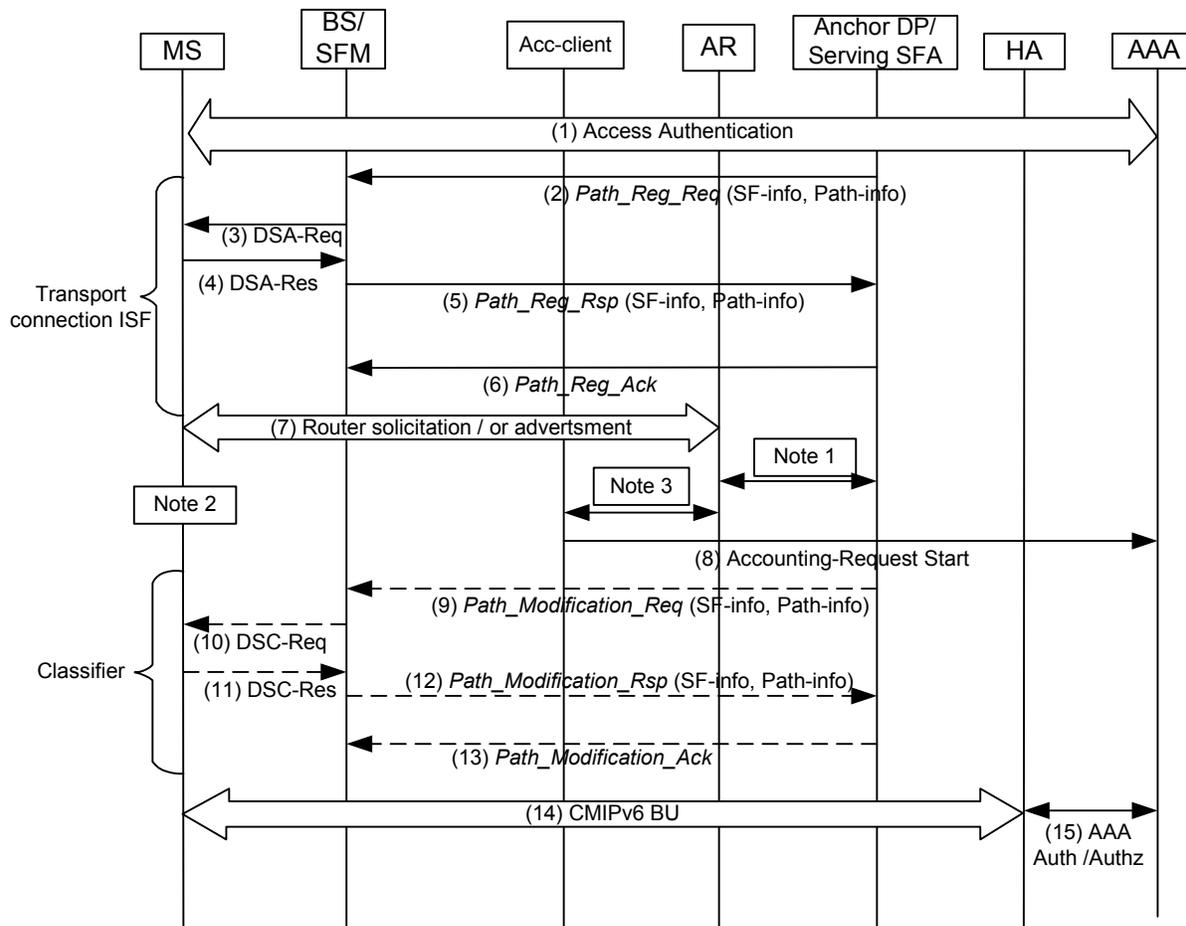
Note 1: AR in the ASN triggers the Anchor DP / Serving SFA to update the SF classifier, with IPv6 Prefix (64 bits)
Note 2: Address Auto-configure and DAD occurs after the router solicitation, advertisement, and DAD.
Note 3: AR triggers the Acc Client to generate Accounting-Request Start (out of scope)

1

2 **Figure 4-26 – In Case of Simple IPv6 and CMIP6 (note CMIP6 has no accounting event in ASN)**

3 **Illustrations of the Accounting Start Events in the CSN**

4 The purpose of the figures in this section is to contextualize the accounting triggers. The figures are informative.
5 For further details refer to the specific sections in this document.
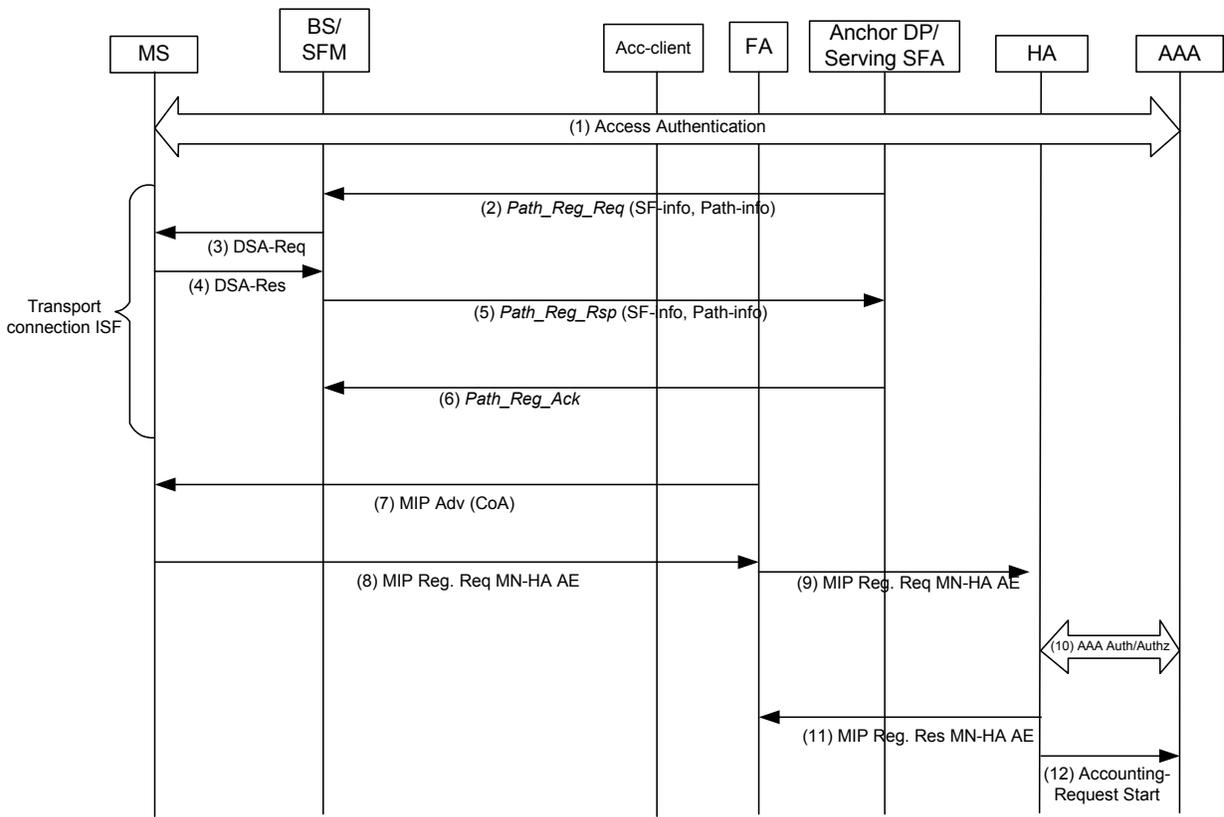
1

2
Figure 4-27 – In Case of CMIP4
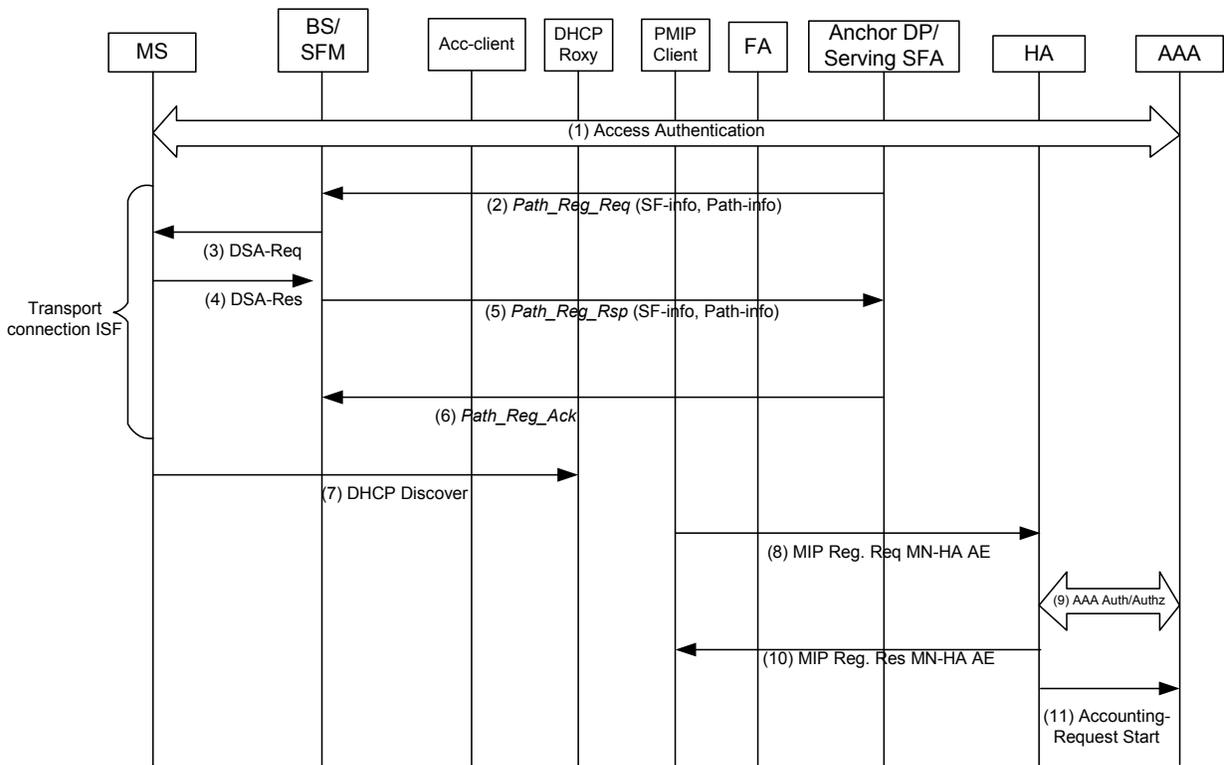
1

2 **Figure 4-28 – In Case of PMIP4**
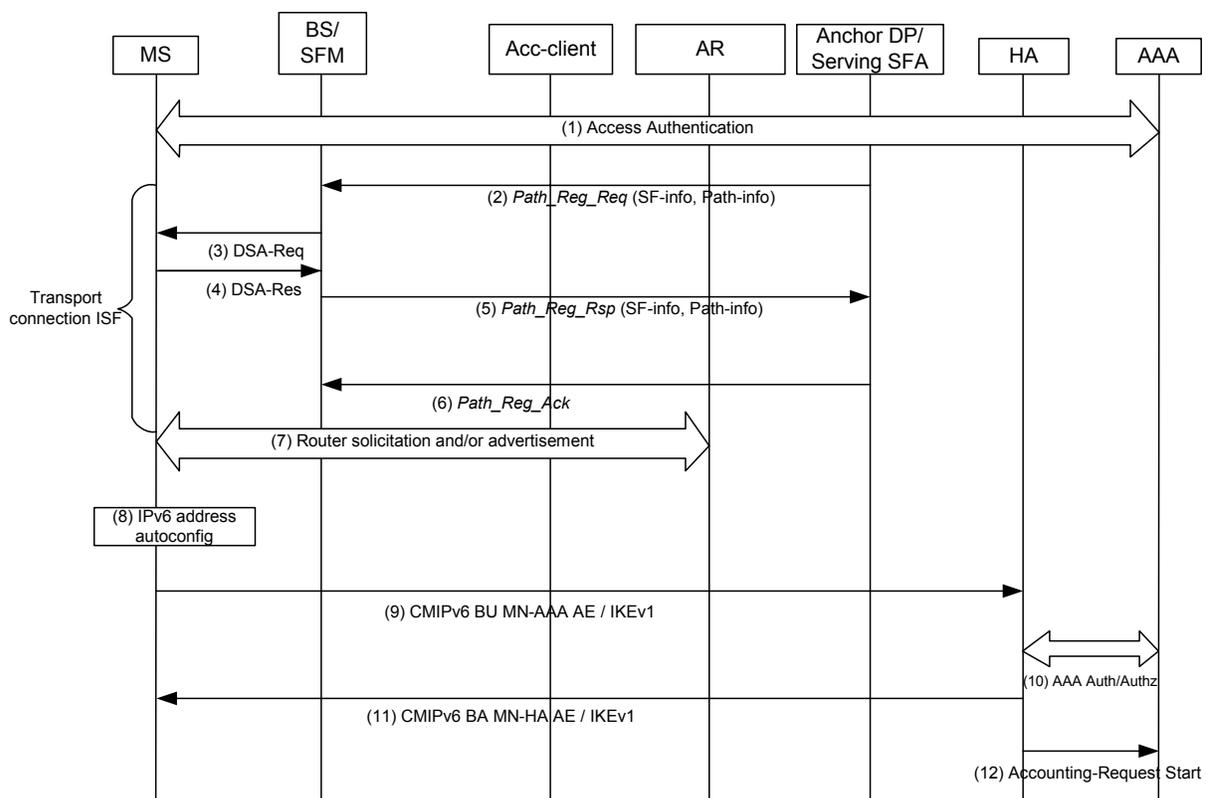
1

2 **Figure 4-29 – In Case of CMIP6**

3 ## 4.5 Network Entry and Exit

4 ### 4.5.1 MS-to-Network Initial Authentication Flow

5 #### 4.5.1.1 Single EAP

6 Figure 4-30 describes normative procedures for an initial MS network entry focusing on MS-to-Network EAP
7 authentication process (single EAP) and MS 802.16e registration.
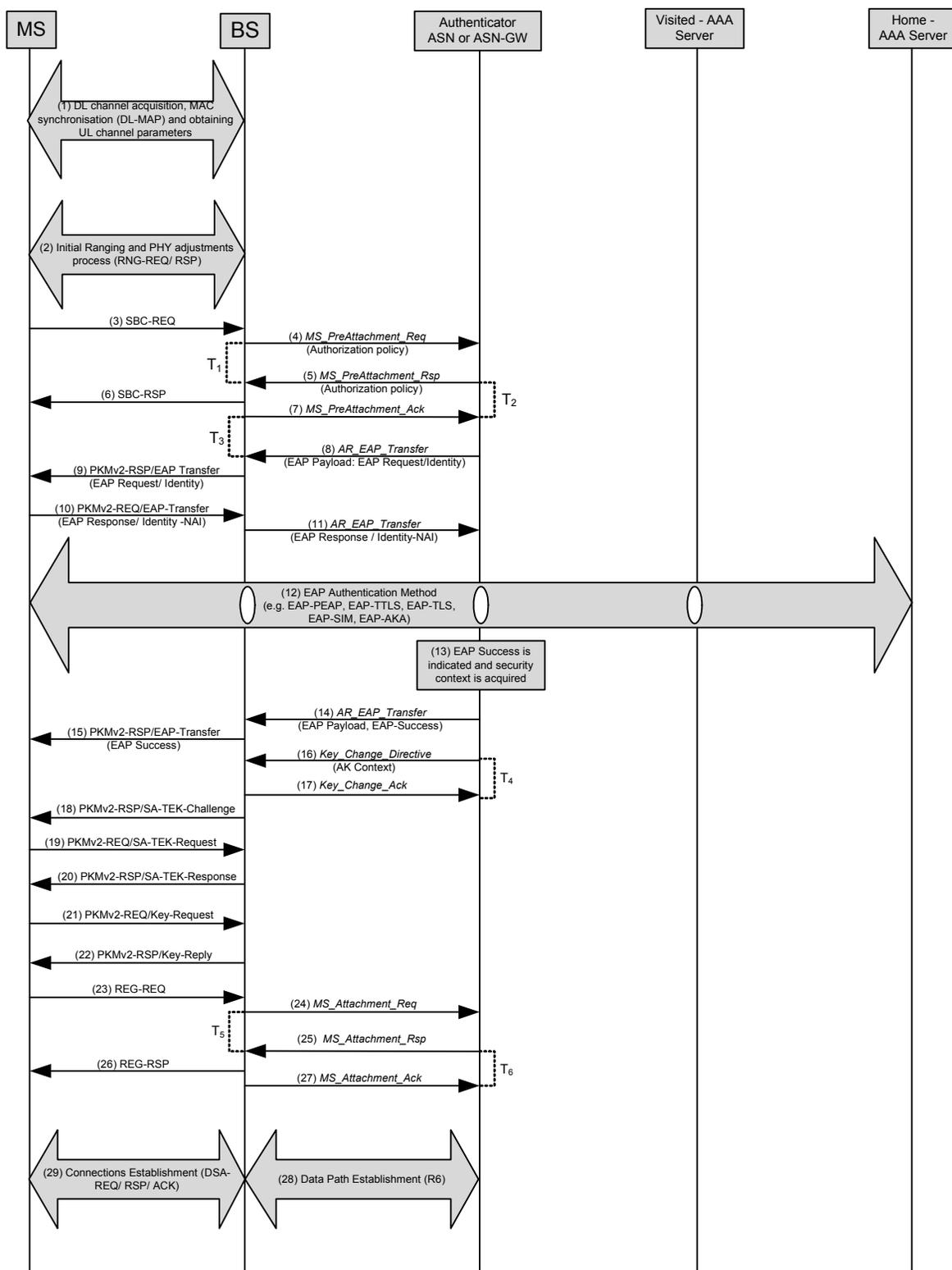
Figure 4-30 – MS Initial Network Entry (Single EAP)

802.16e MS Network Entry starts:

1 **STEP 1**

2 DL channel acquisition, MAC synchronization and obtaining UL channel parameters.

3 **STEP 2**

4 Initial Ranging round trips – RNG-REQ/ RNG-RSP message exchange. The MS performing initial network entry
5 will perform CDMA ranging and after that will send RNG-REQ message without Serving BSID parameter thus
6 indicating that it performs initial entry and not HO (as specified in [2] section 6.3.2.3.5).

7 **STEP 3**

8 MS sends SBC-REQ message starting Basic Capabilities negotiation where MS and BS among other parameters
9 negotiate the PKM protocol version, Authorization Policy and Message Authentication Code mode.

10 **STEP 4**

11 The BS SHALL send *MS_PreAttachment_Req* message to its "default" Authenticator in order to inform it about the
12 new MS entering the network

13 The composition of this *MS_PreAttachment_Req* message is presented in Table 4-30:

14 **Table 4-30 – MS_PreAttachment_Req from BS to Authenticator**

IE	Reference	M/O	Notes
MS Info	Section 5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authorization Policy	Section 5.3.2.20	M	Identifies the MS authorization policy (such as single EAP, double EAP)
BS Info	Section 5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.
> BS ID	Section 5.3.2.25	O	Serving BS ID

15 PKM protocol version and MAC mode are related to BS capabilities and SHOULD be enforced by BS as per
16 network policy (there is no need to transfer these parameters to Authenticator).

17 **STEP 5**

18 Authenticator in the ASN/ASN-GW receiving *MS_PreAttachment_Req* creates a new context block related to this
19 MSID and responds to BS with *MS_PreAttachment_Rsp* message. The composition of this message is presented in
20 Table 4-31:

21 **Table 4-31 – MS_PreAttachment_Rsp from Authenticator to BS**

IE	Reference	M/O	Notes
MS Info	Section 5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authorization Policy	Section 5.3.2.20	M	Identifies the authorization policy. In the case of Single EAP mode, this parameter should indicate "single EAP".
BS Info	Section 5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.
> BS ID	Section 5.3.2.25	O	Serving BS ID

22 **STEP 6**

23 BS receiving SBC-REQ sends SBC-RSP message to MS enforcing the authentication framework policy (PKMv.2,
24 single EAP, CMAC mode).

1 The point in time when SBC-RSP is sent is an implementation decision of the BS: that is, it may be sent before or
2 after performing the MS Pre-Attachment exchange with the Authenticator in the ASN/ASN-GW.

3 In the case MS does not receive SBC-RSP, it will retransmit SBC-REQ.

STEP 7

4

5 BS sends *MS_PreAttachment_Ack* message to the Authenticator (in ASN/ASN-GW) to confirm that SBC-RSP has
6 been sent to MS. Note that this does not confirm that MS has successfully received SBC-RSP. This message does
7 not carry any additional TLVs.

STEP 8

8

9 The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with MS. The trigger for it - is the
10 successful end of the MS Pre-Attachment transaction.

11 The Authenticator sends EAP Request/ Identity message over Authentication Relay protocol (*AR_EAP_Transfer*) to
12 BS.

13 The composition of this message is presented in Table 4-32:

Table 4-32 – AR_EAP_Transfer from Authenticator to BS (EAP initiation)

IE	Reference	M/O	Notes
EAP Payload	Section 5.3.2.62	M	EAP message. In this step it shall include EAP Identity Request message.

15 Note that *AR_EAP_Transfer* message composition remains the same through the EAP authentication process with
16 only difference in the content of the EAP Payload TLV (containing different EAP messages).

STEP 9

17

18 The BS relays the EAP Request/ Identity payload (received in *AR_EAP_Transfer* message) in the PKMv2-
19 RSP/EAP-Transfer message to the MS.

STEP 10

20

21 MS responds with EAP Response/ Identity message providing NAI. This message is transferred to BS over PKMv2-
22 REQ/EAP-Transfer message.

STEP 11

23

24 BS relays EAP payload received in PKMv2 EAP-Transfer to the Authenticator over Authentication Relay protocol
25 (*AR_EAP_Transfer* message).

STEP 12

26

27 The Authenticator analyses the NAI provided by the MS Depending on the realm, EAP payload MAY be forwarded
28 to the MS' Home AAA server via the Visited AAA server (using the provided NAI for resolving the Home-AAA
29 server location). In order to deliver the EAP payload to the AAA server, the Authenticator forwards the EAP
30 message via a collocated AAA client using RADIUS Access-Request message (EAP payload is encapsulated into
31 RADIUS "EAP message" attribute(s)).

32 The EAP authentication process (tunneling EAP authentication method) is performed between the MS and the
33 Authentication server via the Authenticator in ASN/ASNASN-GW. BS provides "relay" of EAP payload from
34 PKMv2 EAP-Transfer messages to *AR_EAP_Transfer* and vice versa. The Authenticator in ASN/ASN-GW acts in
35 pass through mode (as described in [8]) and forwards the EAP messages received as a payload from the BS in
36 *AR_EAP_Transfer* messages to the AAA server using RADIUS Access-Request messages and vice versa –
37 transferring EAP payload from RADIUS Access-Challenge messages to *AR_EAP_Transfer*. There can be multiple
38 EAP message exchanges between the MS and AAA server.

1   The composition of RADIUS messages is presented in the section 5.4.1.

2   EAP peers (supplicant in MS and authentication server) negotiate the EAP method and perform it. At the successful
3   completion of EAP method, security keys (MSK and EMSK) are established at the EAP peers (supplicant in MS and
4   authentication server).

5   **STEP 13**

6   The Authenticator receives indication about the successful completion of EAP-based authentication, the MS
7   authorization profile and the required security context (i.e. MSK key and its lifetime). It is done using RADIUS
8   Access-Accept message from AAA server with EAP-Success message encapsulated in "EAP message" attribute. In
9   the case of EAP process failure, the Authenticator will receive RADIUS Access-Reject message with EAP-Failure
10   encapsulated in "EAP message" attribute.

11   The composition of RADIUS Access-Accept and Access-Reject messages is presented in the section 5.4.1.

12   **STEP 14**

13   The Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to BS as EAP Payload TLV in
14   *AR_EAP_Transfer* message.

15   **STEP 15**

16   The BS relays EAP payload (received in *AR_EAP_Transfer* message) to the MS in PKMv2 EAP-Transfer/ PKM-
17   RSP message (not protected by CMAC according to [2]). This message indicates the results of EAP authentication
18   round to the Supplicant in the MS. Note that the BS does not relate to the content of EAP Payload – whether it is
19   EAP-Success or EAP-Failure message. The BS continues waiting for the explicit indication of EAP authentication
20   completion from the Authenticator. MS is also waiting for PKMv2 SA-TEK-Challenge message from BS to proceed
21   with PKMv2 3way handshake.

22   **STEP 16**

23   The Authenticator in ASN/ASN-GW sends *Key_Change_Directive* message to the BS to indicate completion of the
24   EAP authentication process. The composition of this message is presented in Table 4-33:

25   **Table 4-33 – Key_Change_Directive from Authenticator to BS**

IE	Reference	M/O	Notes
MS Info	Section 5.3.2.103	M	Contains MS-related context in the nested IEs.
>AK Context	Section 5.3.2.6	M	This compound parameter includes AK context parameters (AK, AK SN, AK lifetime, etc.) for BS use.

26   This message informs the BS that it SHOULD proceed with PKMv2 3-way handshake (start the new key
27   enforcement and Security Associations creation process).

28   *Key_Change_Directive* message SHOULD include AK Context parameter including the appropriate keying material
29   – AK, key's context, etc.

30   Release 1.0.0 specification does not define MS security properties (the number of SAs and their attributes) delivery
31   from a Home AAA server to ASN and from an Authenticator to a BS. Instead, the single "default" SA (Primary SA)
32   SHOULD be configured in a BS. (All the preprovisioned service flows should be associated with this "default" SA
33   during service flow establishment process).

34   In the case authentication failure signal is received from the AAA server (RADIUS Access-Reject with EAP-
35   Failure), the Authenticator may decide to restart EAP authentication process (by sending the new EAP Request
36   Identity) or bring down the user. In the latter case, the Authenticator proceeds with MS Network Exit procedure.

1 **STEP 17**

2 BS receiving *Key_Change_Directive* from Authenticator will acknowledge it by *Key_Change_Ack* message.

3 **STEP 18, 19, 20**

4 PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) is conducted between BS and MS to
5 verify the AK to be used and to establish the Security Association(s) pre-provisioned for the MS (WiMAX Rel.1
6 assumes the "default" SA-Descriptor identifying the primary SA to be provisioned in a BS).

7 The BS SHALL ensure that PKMv2 3way handshake is indeed successfully completed and the new PMK/AK is
8 enforced by the MS – i.e. the BS should receive and verify a MAC management message from the MS signed by
9 CMAC derived from the new AK. Said MAC management message may be the one described in step 21 (Key
10 Request/Reply) or the one in step 23 (REG-REQ/RSP)

11 When BS recognizes the completion of PKMv2 3way handshake process (success or failure), it SHALL indicate this
12 event to Authenticator. This indication is described in the step 24.

13 **STEP 21, 22**

14 MS acquires the valid TEK keys using PKMv2 Key-Request/ Reply exchange between MS and BS for each SA
15 (This step is repeated for each SA).

16 **STEP 23**

17 When PKMv2 3-way handshake is completed, MS proceeds with 802.16e Registration procedure by sending REG-
18 REQ message as specified in 6.3.2.3.7 of IEEE 802.16e-2005. This message will carry the MS supported
19 capabilities (such as CS capabilities, Mobility parameters and Handover support, etc.).

20 **STEP 24**

21 The BS forwards to the Authenticator in the ASN/ASN-GW the result of the PKMv2 3-way handshake, and when
22 successful also the MS REG Context parameters in *MS_Attachment_Req* message. The composition of this message
23 is presented in Table 4-34:

24 **Table 4-34 – MS_Attachment_Req from BS to Authenticator**

IE	Reference	M/O	Notes
MS Info	Section 5.3.2.103	M	Contains MS-related context in the nested IEs.
> REG Context	Section 5.3.2.144	O	Identifies the MS REG Context parameters as received from MS in REG-REQ and as supported by the BS.
> Key Change Indicator	Section 5.3.2.86	M	Indicates the completion of PKMv2 3way handshake to Authenticator
BS Info	Section 5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.
> BS ID	Section 5.3.2.25	O	Serving BS ID

25 The Key Change Indicator TLV indicates to the ASN-GW if the 3-way handshake was successful or not.

26 In case the 3-way handshake failed, the NW entry process may be aborted or a new EAP authentication may be
27 triggered. In case it's successful, the REG Context TLV conveys to the ASN/ASN-GW information provided by the
28 MS in REG-REQ.

29 **STEP 25**

30 ASN /ASN GW Authenticator receiving *MS_Attachment_Req* message, responds to BS with *MS_Attachment_Rsp*
31 message. The composition of this message is presented in Table 4-35:

1 **Table 4-35 – MS_Attachment_Rsp from Authenticator to BS**

IE	Reference	M/O	Notes
MS Info	Section 5.3.2.103	O	Contains MS-related context in the nested IEs.
> REG Context	Section 5.3.2.144	O	Identifies the MS REG Context parameters as enforced by the Authenticator.

2 **STEP 26**

3 The BS sends REG-RSP message to MS as specified in 6.3.2.3.8 of IEEE 802.16e-2005 formatting the appropriate
4 parameters (from BS policy and/or ASN/ASN GW Authenticator response).

5 The point in time when REG-RSP is sent is an implementation decision of the BS: that is, it may be sent before or
6 after performing the *MS_Attachment_Req* and *MS_Attachment_Rsp* exchange with the ASN/ASN GW
7 Authenticator.

8 In case the MS does not receive REG-RSP, it will retransmit REG-REQ.

9 **STEP 27**

10 The BS sends *MS_Attachment_Ack* message to the Authenticator in the ASN/ASN-GW indicating that
11 *MS_Attachment_Rsp* message from the ASN/ASN GW Authenticator has been received and REG-RSP message has
12 been sent to MS. This message serves as a trigger to the ASN/ASN GW Authenticator to instigate the process of
13 pre-provisioned service flows establishment.

14 **STEP 28, 29**

15 ASN/ASN-GW triggers SFA to create the Initial service flow (ISF) and optionally other pre-provisioned service
16 flows.

17 **4.5.1.2   Double EAP**

18 MS initial network entry with double EAP authentication process is presented in Figure 4-31:
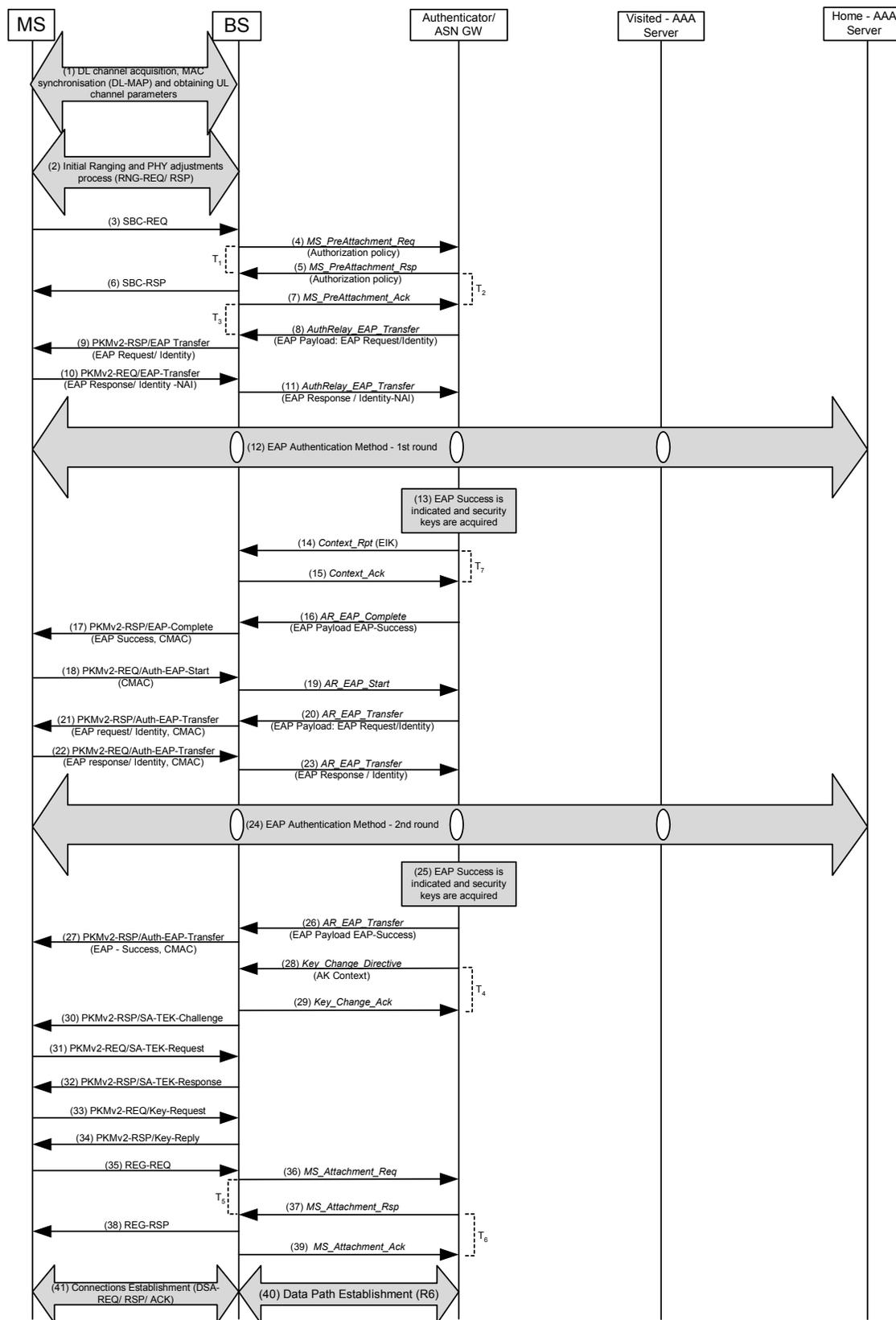
Figure 4-31 – MS Initial Network Entry (Double EAP)

1   The differences in the presented message flow for double EAP are highlighted below:

STEP 1-7

3   These steps are generally the same as in the case of Initial Network Entry with single EAP authentication procedure.
4   The only difference is that Authorization Policy TLV in *MS_PreAttachment_Rsp* message (Step 5) SHALL indicate
5   the double EAP authentication mode. BS should set parameters of SBC-RSP message (Step 6) accordingly.

STEP 8-13

7   These steps are generally the same as in the case of Initial Network Entry with single EAP authentication procedure.
8   Note, that MS authorization profile parameters are not included in the RADIUS Access-Accept message of the 1st
9   EAP round.

STEP 14

11   In the case the successful completion of the 1st EAP round was indicated in Step 13 (RADIUS Access-Accept
12   message with EAP-Success is received), Authenticator/ ASN GW sends *Context_Rpt* message to BS to provide it
13   with EIK key derived from the MSK1/ PMK1 key of the 1st EAP round. The Context Purpose Indicator TLV should
14   be set to indicate "Security Context delivery".

15   Otherwise, if EAP-Failure was indicated in Step 13, Steps 14 and 15 are skipped.

16   The composition of this message is shown in Table 4-36:

17   **Table 4-36 – Context_Rpt from Authenticator to BS (EIK delivery)**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Identifies the purpose of the *Context_Rpt* transaction. In this case it should be set to indicate – Security Context delivery.
MS Info	5.3.2.103	M	
> EIK	5.3.2.63	M	Contains EIK key
Failure Indication	**5.3.2.69**	**O**	Provide failure indication for this message

STEP 15

19   BS receiving *Context_Rpt* message from Authenticator will acknowledge it by *Context_Rpt_Ack* message. The
20   composition of this message is shown in Table 4-37:

21   **Table 4-37 – Context_Rpt_Ack from BS to Authenticator (EIK delivery)**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Identifies the purpose of the *Context_Rpt* transaction. In this case it should be set to indicate – Security Context delivery.

22   The BS also acquires the EIK key delivered in the *Context_Rpt* message. From this point in time, the BS SHALL
23   use this EIK for CMAC generation (on DL) or CMAC verification (on UL) in PKMv2 EAP-Complete and
24   Authenticated EAP messages (Authenticated-EAP-Start and Authenticated-EAP-Transfer). The BS keeps this EIK
25   key until it receives the explicit indication from the Authenticator to start 3-way handshake or until it receives
26   another *Context_Rpt* message with a new EIK key (e.g. if the 1st EAP round has been restarted).

1 **STEP 16**

2 Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to the BS as EAP Payload TLV in
3 AuthRelay message. EAP-Success SHALL be forwarded to the BS using *AuthRelay-EAP-Complete* message. EAP-
4 Failure SHALL be forwarded to the BS using *AR_EAP_Transfer* message.

5 The composition of AuthRelay-EAP-Complete message (with EAP-Success) is shown in Table 4-38:

6 **Table 4-38 – AuthRelay_EAP_Complete from Authenticator to BS**

IE	Reference	M/O	Notes
EAP Payload	5.3.2.62	M	EAP message. For AuthRelay-EAP-Complete, it shall include EAP-Success message.

7 **STEP 17**

8 If the BS receives AuthRelay-EAP-Complete message from the Authenticator, it forwards EAP-Success payload
9 over PKMv2 EAP-Complete message (PKM-RSP) protected by CMAC (based on the recently acquired EIK key) to
10 the MS indicating that the 1st EAP authentication round has been successfully completed. Otherwise, if BS receives
11 *AR_EAP_Transfer* message from the Authenticator, it forwards EAP payload (EAP-Failure in this case) over
12 PKMv2 EAP Transfer message not protected by CMAC.

13 **STEP 18**

14 The MS validates the CMAC in the EAP-Complete message and if validation is successful, it instigates the 2nd EAP
15 round by sending PKMv2 Authenticated-EAP-Start message (PKM-REQ) protected by CMAC (based on the EIK
16 key derived from the MSK of the 1st EAP round).

17 **STEP 19**

18 The BS validates the CMAC in Authenticated-EAP-Start message and if validation successful, it sends
19 *AR_Authenticated_EAP_Start* message to the Authenticator.

20 **STEP 20**

21 The Authenticator starts the 2nd EAP round by sending EAP-Request/ Identity message over
22 *AR_Authenticated_EAP_Transfer* to BS.

23 **STEP 21**

24 The BS forwards the received EAP payload in the PKMv2 Authenticated-EAP-Transfer message to the MS. The BS
25 applies CMAC parameter (based on EIK) for this PKMv2 message

26 **STEP 22, 23, 24**

27 The 2nd EAP round is processed. EAP messages are sent using protected PKMv2 Authenticated-EAP-Transfer
28 messages over the air (between the MS and the BS) and using *AR_Authenticated_EAP_Transfer* messages over R6
29 (between the BS and the Authenticator).

30 **STEP 25**

31 The Authenticator receives indication about the successful completion of EAP-based authentication (the 2nd EAP
32 round), the MS authorization profile and the required security context (i.e. MSK2 key and its lifetime). It is done
33 using RADIUS Access-Accept message with EAP-Success message encapsulated in "EAP message" attribute. In
34 the case of EAP process failure, the Authenticator will receive RADIUS Access-Reject message with EAP-Failure
35 encapsulated in "EAP message" attribute.

36 The composition of RADIUS Access-Accept or Access-Reject is presented in the section 5.4.1.

1 **STEP 26**

2 The Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to the BS as EAP Payload TLV in
3 *AR_Authenticated_EAP_Transfer* message.

4 **STEP 27**

5 The BS relays EAP Payload over PKMv2 Authenticated-EAP-Transfer message protected by CMAC (based on EIK
6 from the 1st EAP round) to the MS. This message indicates the Supplicant in the MS the results of the 2nd EAP
7 authentication round. Note that the BS does not relate to the content of EAP Payload – whether it is EAP-Success or
8 EAP-Failure message. The BS continues waiting for the explicit indication of EAP authentication completion and
9 trigger for PKMv2 3WHS from the Authenticator (in *Key_Change_Directive* message). The MS is also waiting for
10 PKMv2 SA-TEK-Challenge message from the BS to proceed with PKMv2 3-way handshake.

11 **STEP 28-41**

12 These steps are generally the same as in the case of Initial Network Entry with single EAP authentication procedure.

13 **4.5.1.3   Error Handling During Initial Network Entry**

14 **4.5.1.3.1 Timers and Timing Considerations**

15 This section identifies the timer that the entities participating in the Initial Network Entry procedure SHALL use.
16 The Initial Network Entry procedure utilizes seven timers:

17 • T_1: is started by an BS upon sending an *MS_PreAttachment_Req* (Authorization Policy). It is stopped upon
18 receiving a corresponding *MS_PreAttachment_Rsp*.

19 • T_2: is started when an Authenticator sends an *MS_PreAttachment_Rsp* and is stopped upon receiving a
20 corresponding *MS_PreAttachment_Ack*.

21 • T_3: is started by the BS when *MS_PreAttachment_Ack* is sent and the negotiated Authorization Policy
22 indicates Single or Double EAP. It is stopped upon receiving *AR_EAP_Transfer*.

23 • T_4: is started by the Authenticator when it sends a *Key_Change_Directive* message and is stopped upon
24 receiving the *Key_Change_Ack*.

25 • T_5: is started by a BS upon sending an *MS_Attachment_Req*. It is stopped upon receiving a corresponding
26 *MS_Attachment_Rsp*.

27 • T_6: is started when an Authenticator sends an *MS_Attachment_Rsp* and is stopped upon receiving a
28 corresponding *MS_Attachment_Ack*.

29 • T_7: is started when an Authenticator sends *Context_Rpt* message (EIK delivery) and is stopped upon
30 receiving the corresponding Context_Report_Ack message.

31 Table 4-39 shows the default value of timers and also indicates the range of the recommended duration of these
32 timers.

33 **Table 4-39 – Timer Values for Initial Network Entry Procedure**

Timer	Default Values (msec)	Criteria	Maximum Timer Value (msec)
T_1	TBD		TBD
T_2	TBD		TBD
T_3	TBD		TBD
T_4	TBD		TBD
T_5	TBD		TBD

Timer	Default Values (msec)	Criteria	Maximum Timer Value (msec)
T_6	TBD		TBD
T_7	TBD		TBD

1 **4.5.1.3.2 Handling Error Conditions**

2 Table 4-40 lists the behavior for various error conditions during Initial Network Entry:

3 **Table 4-40 – Initial Network Entry – Handling Error Conditions**

	Failure Case	Action
1	Auth failure at the Authenticator.	Authenticator shall either start another EAP attempt (by sending EAP-Request/ Identity message) or initiate MS Network Exit (as described in the section 4.5.2).
2	*MS_PreAttachment_Req* or *MS_Attachment_Req* messages not understood by the Authenticator (decode error, corrupted packet etc).	Send *MS_PreAttachment_Rsp* (or *MS_Attachment_Rsp* correspondingly) with Failure Indication TLV.
3	*MS_PreAttachment_Rsp* or *MS_PreAttachment_Ack* messages are not understood by the Authenticator or BS (decode error, corrupted packet etc).	Discard the message, no response generated.
4	Internal error at the Authenticator or BS – need to abort the call	Initiate MS Network Exit (as described in the section 4.5.2).
5	MS dropped call at the BS during call setup	Initiate to the peer entity using procedure described in the MS Network Exit section 4.5.2.
6	Unexpected message received (for a given state).	Discard the message, no response generated.
7	If R6 data path was already established in any of the above cases.	Terminate Data Path with *Path_Dereg_Req*.
8	*Path_Dereg_Req* received for a MS or Data Path that does not exist.	Respond with *Path_Dereg_Rsp* with Success so that the peer does not retry.
9	BS receives SBC-REQ message retransmission from the MS (SBC-REQ retransmission as a result of timer expiry in the MS or SBC-RSP message loss).	BS resends *MS_PreAttachment_Req* message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with *MS_PreAttachment_Rsp* and reset T_2 timer.
10	BS receives REG-REQ message retransmission from the MS (REG-REQ retransmission as a result of timer expiry in the MS or REG-RSP message loss).	BS resends *MS_Attachment_Req* message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with *MS_Attachment_Rsp* and reset T_6 timer.
11	BS detects PKMv2 3way handshake failure for any reason.	BS sends *Key_Change_Cnf* message with Key Change Indicator TLV set to indicate "failure".

Failure Case	Action
	Authenticator responds with *Key_Change_Ack* message and initiates MS Network Exit (as described in the section 4.5.2).

4.5.1.3.3 Timer Expiry

Table 4-41 shows the details of the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-41.

Table 4-41 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T_1	BS	Initiate MS Network Exit (as described in section 4.5.2).
T_2	Authenticator	Initiate MS Network Exit (as described in section 4.5.2).
T_3	BS	Initiate MS Network Exit (as described in section 4.5.2).
T_4	Authenticator	Initiate MS Network Exit (as described in section 4.5.2).
T_5	BS	Initiate MS Network Exit (as described in section 4.5.2).
T_6	Authenticator	Initiate MS Network Exit (as described in section 4.5.2).
T_7	Authenticator	Initiate MS Network Exit (as described in section 4.5.2).

4.5.2 Network Exiting

MS De-registration is a common scenario caused by graceful shutdown or some failure situation where MS is deregistered from network service and its context is deleted.

The following entities may start MS Deregistration process:

- MS, when initiates graceful shutdown;
- ASN, based on either graceful shutdown trigger or failure situation in network;
- Home AAA server located in CSN also is able to trigger MS Deregistration.

The MS De-registration procedure covers different scenarios:

- MS De-registration as a result of MS Graceful Shutdown;
- MS De-registration from the current BS (and probably re-initialization in other BS/ Network);
- Enforcing MS to halt any transmissions (including MAC management messaging);
- Enforcing MS to halt traffic transmissions;
- Erasing MS context in the ASN entities when radio link with the MS has been lost.

Deregistration signaling over R1 Reference Point (over the air) is done using IEEE 802.16e defined messages with the specific Action/ De-registration_Request_Code parameters:

- DREG-CMD – message used by BS to signal deregistration command to MS. It may be unsolicited or in response to MS-initiated DREG-REQ. DREG-CMD message should include Action Code parameter indicating the requested deregistration action;
- DREG-REQ – MS sends this message to BS to request deregistration. This message should include De-registration_Request_Code parameter indicating the reason of deregistration request.

Above the procedure, it should consider the difference when the MS is Simple IP mode, PMIP4 mode, CMIP mode.

1   **4.5.2.1   Normal Mode**

2   In the normal mode, considering MS exiting network entry, the related network entities will release the related data
3   paths, resources and delete the MS contexts.

4   The scenarios mainly include MS powering down, resource blocking, fault, or changing service strategy of network
5   side.

6   **4.5.2.1.1 MS Triggered Network Exit**
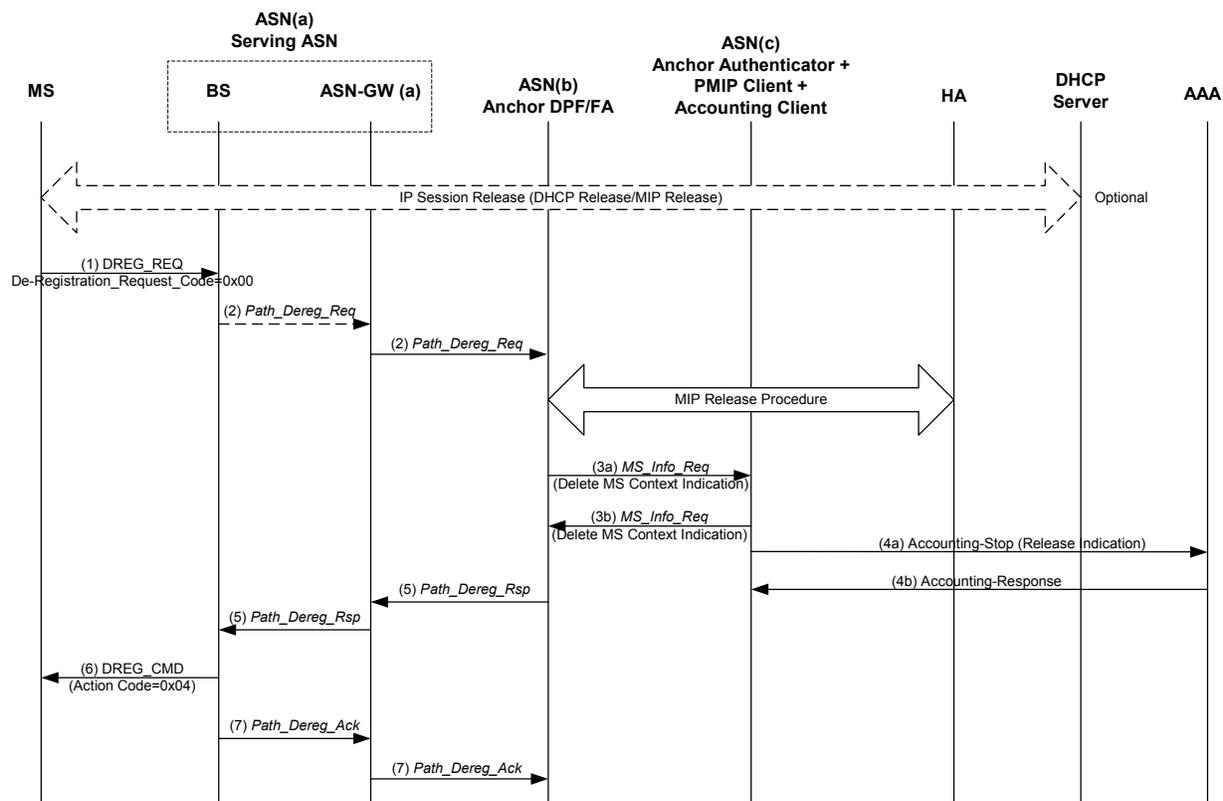
7

8   **Figure 4-32 – MS Triggered Network Exit (Normal Mode)**

9   **STEP 1**

10   While the MS has an active session the MS exits the network by sending an DREG_REQ message to BS in serving
11   ASN, including De-Registration_Request Code=0x00.

12   Before this step, optionally, MS performs initiating DHCP Release Procedure; And for CMIP terminal, MS may
13   perform MIP tunnel releasing (MIP De-registration) procedure; For PMIP, DHCP Release may trigger PMIP Client
14   to intiate a MIP tunnel releasing procedure.

15   There may not be DHCP release procedure, i.e. IP is stateless auto-configuration in IPv6, and then PMIP client will
16   not initiate MIP tunnel release at this step.

17   **STEP 2**

18   BS sends R6 *Path_Dereg_Req* message to the ASN-GW (a) which in turn will send a R4 *Path_Dereg_Req* message
19   to Anchor ASN(b) which contains the Anchor DPF/FA.

1 **STEP 3**

2 Anchor ASN(b) associated with FA, sends R4 *MS_Info_Req* message to notify ASN(c) (which contains Accounting
3 Client, Anchor Authenticator and PMIP Client) to delete MS contexts.

4 During this step, ASN(b) can initiate MIP tunnel release procedure as follows:

5 For CMIP, if MS did not perform MIP De-registration procedure in the step1, the ASN(b) can perform MIP
6 Revocation procedure based on [26]

7 For PMIP, if MS did not perform DHCP Release procedure in the step 1, the ASN(b) can trigger PMIP Client to
8 perform MIP De-Registration procedure upon receipt of a R4 *MS_Info_Req* message.

9 The details regarding MIP session termination are as described in 4.8.

10 **STEP 4**

11 ASN(c) containing the Accounting Client sends Accounting Stop message including a Release Indication of MS De-
12 registration to AAA (visited-AAA/Home-AAA) for indicating MS de-registration; AAA server releasing the related
13 MS contexts.

14 **STEP 5**

15 ASN(b) replies with the R4 *Path_Dereg_Rsp* to the Serving ASN(a) which in turns sends a R6 *Path_Dereg_Ack*
16 message to the BS.

17 **STEP 6**

18 BS sends DREG_CMD message to the MS including Action Code =0x04;

19 **STEP 7**

20 BS sends R6 *Path_Dereg_Ack* to the ASN-GW(a) which in turn will send a R4 *Path_Dereg_Ack* message to
21 ASN(b). During this procedure, the related entities will release the retained MS context and the assigned data path
22 resource for the MS.

1   **4.5.2.1.2 Network Trigger**
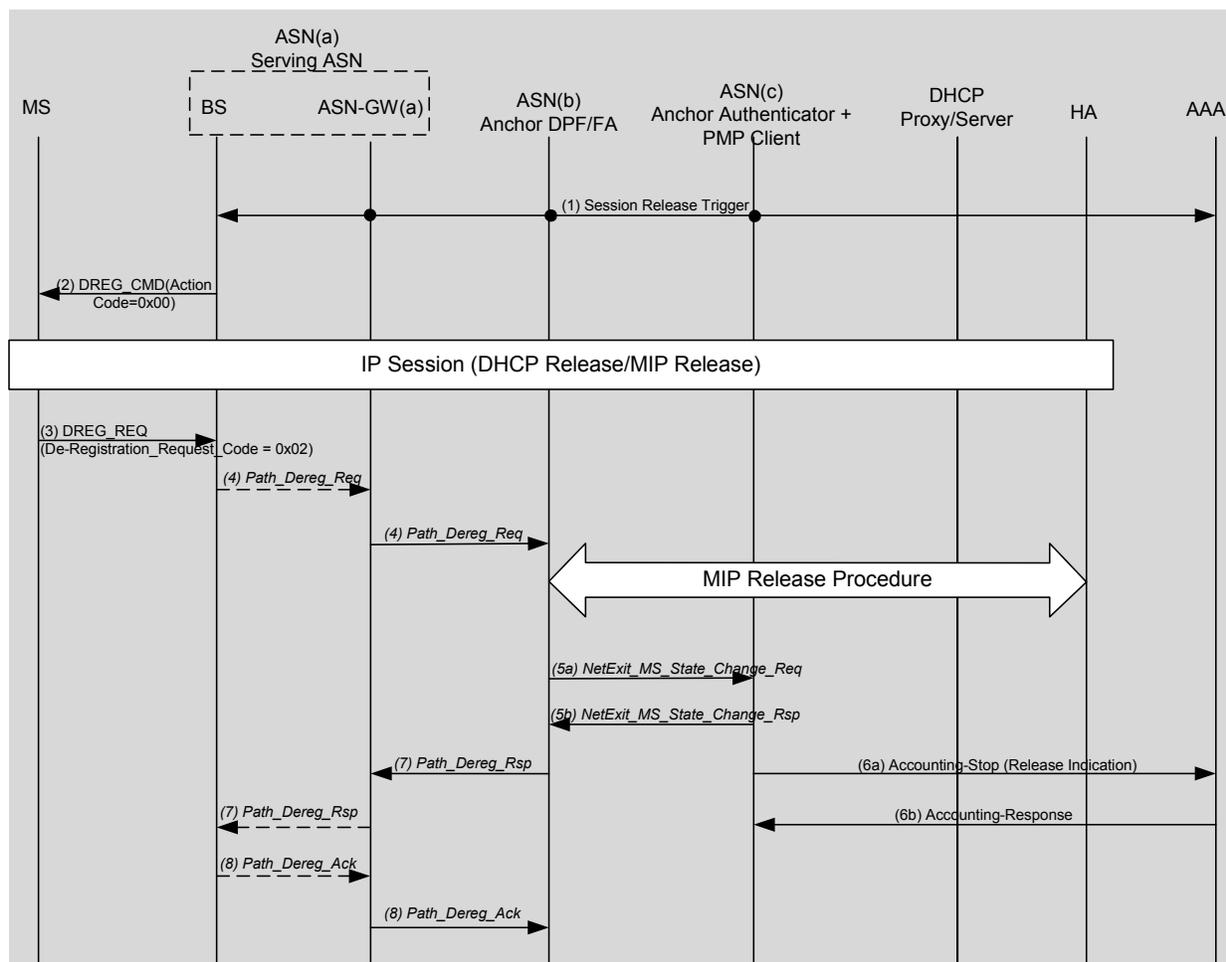
2

3   **Figure 4-33 – Network Trigger (Normal Mode)**

4   **STEP 1**

5   During Normal Mode, the related network entities trigger MS exiting network, such as AAA Server, HA, FA etc.;
6   And the final decision need be notified to the Serving BS;

7   **Case 1 - AAA Server Trigger:**

8   Home-AAA server in Home CSN takes a decision for MS Deregistration based on changing service strategy
9   including user's arrearage, report loss of mobile phone by user etc.

10   H-AAA sends RADIUS Disconnect-Request message to ASN(c) hosting the Anchor Authenticator (NAS). The
11   message composition is presented in 5.4.1.7.

12   Anchored Authenticator (NAS) acknowledges Disconnect-Request message by Disconnect-ACK. The message
13   composition is presented in the Table xxx. ASN(c) proceeds with the MS deregistration process by sending a R3
14   *Session_Release_Req* to ASN(b), which in turn relays the message to the serving ASN(a). ASN-GW(a) sends a R6
15   *Session_Release_Req* message to the BS. Upon receipt of the R6 *Session_Release_Req* message, the BS send a
16   DREG_CMD to the MS (see step 2) and sends a R6 *Session_Release_Rsp* to the ASN-GW(a). Upon receipt of this
17   message ASN(a) sends a R3 *Session_Release_Rsp* to ASN(b) which in turn relays the message to the ASN(c).
18   ASN(c) completes the deregistration by sending a R3 *Session_Release_Cnf* to ASN(b), which in turn relays the
19   message to the serving ASN(a).

1 If NAS can not proceed with MS deregistration, it should respond with RADIUS Disconnect-NACK message as
2 presented in 5.4.1.7.1.

Case 2 - Anchor DPF/FA Trigger:

4 This trigger may be caused by some failure situation where MS re-initialization is needed, or as a result of failure
5 report from HA, Serving ASN or the ASN associated with Anchor Authenticator. ASN(b) proceeds with the MS
6 deregistration process by sending a R3 *Session_Release_Req* to the serving ASN(a). ASN-GW(a) sends a R6
7 *Session_Release_Req* message to the BS. Upon receipt of the R6 *Session_Release_Req* message, the BS send a
8 DREG_CMD to the MS (see step 2) and sends a R6 *Session_Release_Rsp* to the ASN-GW(a). Upon receipt of this
9 message, ASN(a) sends a R3 *Session_Release_Rsp* to ASN(b). ASN(b) completes the deregistration by sending a R3
10 *Session_Release_Cnf* to ASN(a).

Case 3 - Anchor Authenticator Trigger:

12 There is a trigger occurs in Anchored Authenticator entity to initiate MS Deregistration process. This trigger may be
13 caused by graceful shutdown (e.g. PMK lifetime expiry) or some failure situation where MS re-initialization is
14 needed. ASN(c) proceeds with the MS deregistration process by sending a R3 *Session_Release_Req* to ASN(b)
15 which in turn relays the message to the serving ASN(a). ASN-GW(a) sends a R6 *Session_Release_Req* message to
16 the BS. Upon receipt of the R6 *Session_Release_Req* message, the BS sends a DREG_CMD to the MS (see step 2),
17 and sends a R6 *Session_Release_Rsp* to the ASN-GW(a). Upon receipt of this message, ASN(a) send a R3
18 *Session_Release_Rsp* to ASN(b) which in turn relays the message to the ASN(c). ASN(c) completes the
19 deregistration by sending a R3 *Session_Release_Cnf* to ASN(b) which in turn relays the message to the serving
20 ASN(a).

Case 4 - Serving BS/Serving ASN Trigger:

22 Generally, BS/ Serving ASN should not be an initiator of MS Deregistration. In the case of failure, it should report
23 the problem to Anchor ASN/ Authenticator and wait for command from ASN entity. If, in this state, failure occurs
24 in communications with ASN entities or there is no command during some timeout, BS/ Serving ASN may start MS
25 Deregistration process by sending the DREG_CMD to the MS (see step 2).

STEP 2

27 BS sends DREG_CMD message to MS including Action Code =0x00 to indicate MS exiting network.

STEP 3

29 MS replies DREG_REQ message to BS including Action Code = 0x02. Before this step, for CMIP terminal, MS
30 may perform MIP tunnel release procedure. At the same time, optionally, MS may perform DHCP release
31 procedure.

32 For PMIP, DHCP Release may trigger PMIP4 client initiates MIP tunnel releasing procedure.

33 There may be not DHCP release procedure, i.e. IP is stateless auto-configuration in IPv6, and then PMIP4 client will
34 not initiates MIP tunnel release at this step.

35 Note: Based on implementation, this step can be optional. And BS can still perform step 4 based on the timer
36   expires.

STEP 4

38 BS sends *Path_Dereg_Req* message to the ASNb with Anchor DPF/FA, including Power Down Indication. In case
39 the BS cannot send the message directly to the ASNb, it SHALL send the message to the Serving ASNa. Then the
40 Serving ASNa forwards this message to the ASNb which contains Anchor DPF.

STEP 5

42 Further, ASNb with FA, notifies ASNc which contains Anchor Accounting Client, Anchor Authenticator and
43 PMIP4 client to delete MS contexts.

1 For CMIP, in the step3, if MS did not perform MIP De-registration procedure, here the ASNc associated with FA
2 can perform MIP Revocation procedure based on [26].

3 For PMIP, the ASNb which contain Anchor DPF/FA can trigger PMIP4 client to perform MIP De-Registration
4 procedure.

5 The detail of MIP session termination is covered in section 4.8.

6 **STEP 6**

7 The ASNc associated with Anchor Accounting Client sends Accounting Stop message including a Release
8 Indication of MS De-registration to AAA (visited-AAA/Home-AAA) for indicating MS de-registration network.
9 AAA server releases the related MS contexts. This step can start anytime after the MIP Release Procedure.

10 **STEP 7**

11 ASNb which contains Anchor DPF replies *Path_Dereg_Rsp* to the BS. In case the ASNb cannot send the message
12 directly to the BS, it SHALL send the message to the Serving ASNa, then the Serving ASNa forwards this message
13 to the BS.

14 **STEP 8**

15 BS sends *Path_Dereg_Ack* to the ASNb which contains anchord DPF. In case the BS cannot send the message
16 directly to theASNb, it SHALL send the message to the Serving ASNa. Then the Serving ASNa forwards this
17 message to the ASNb. During this procedure, the related entities will release the retained MS context, and the
18 assigned data path resource for the MS.

19 **4.5.2.2   Idle Mode**

20 In the Idle mode, considering MS exiting network entry, Anchor PC will conduct MS de-registration procedure, and
21 the related network entities will release the resources and delete the MS contexts.

22 The scenario mainly includes MS power down, resource blocking, fault, or changing service strategy of network
23 side.

24 **4.5.2.2.1 MS Triggered Network Exit (Idle Mode)**

25 There are two options for a MS to trigger network exit while it is in idle mode:

26 • MS exits idle mode and conducts graceful termination while in active mode. For the network exit
27   procedure, it is covered by Idle exit and Network exit in active mode text.

28 • Per IEEE 802.16e-2005, MS sends RNG_REQ with power down indication without exiting the idle mode.
29   The following call procedure is for this network exit method.
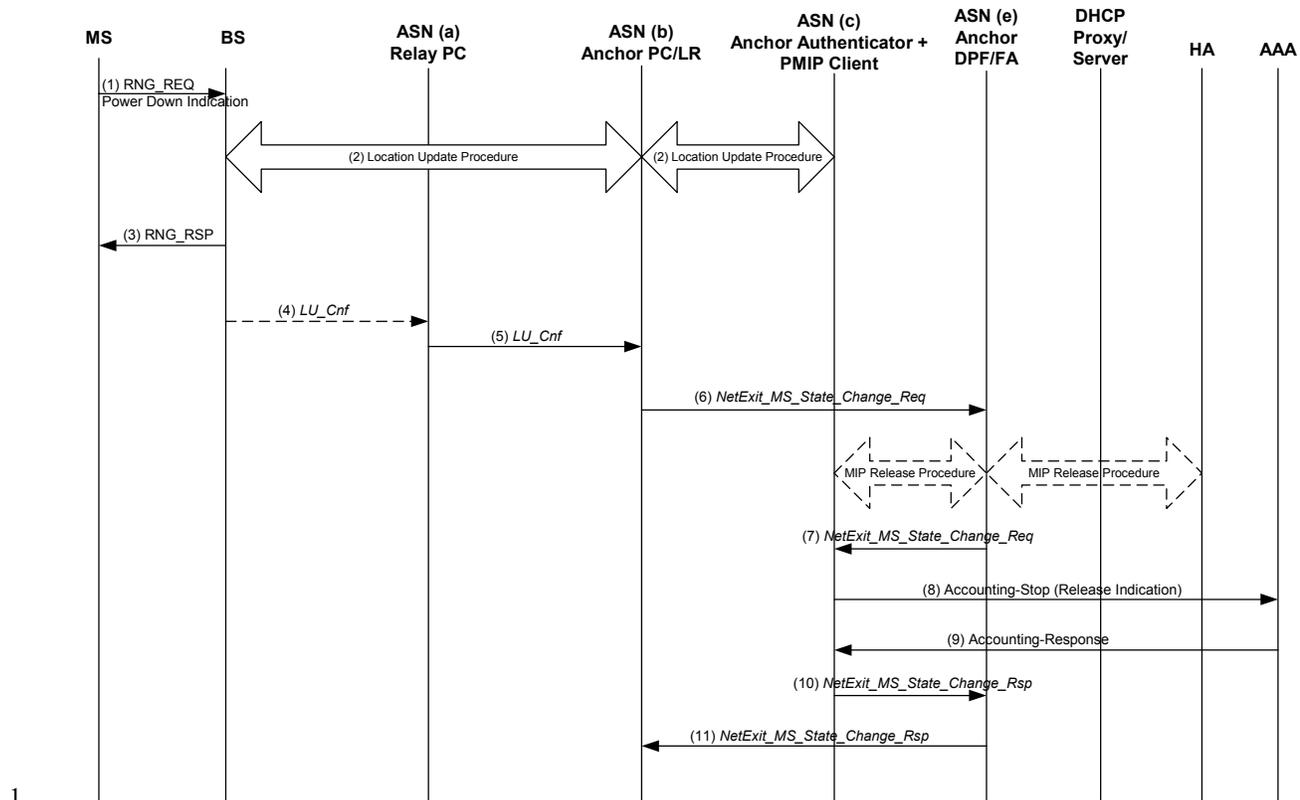
Figure 4-34 – MS Triggered Network Exit (Idle Mode)

STEP 1

During the Idle Mode, MS decide to power down, MS sends RNG_REQ message including Power down Indication
and Anchor PC ID to initiate the location update of De-registration.

STEP 2

After BS/PA is verified successfully RNG_REQ message based on MS's AK and AK Context, BS/PA and ASNb
with Anchor PC will perform location update procedure normally.

STEP 3, 4, 5

BS replies RNG_RSP to MS, and sends LU_Cnf message to ASNb with Anchor PC including successful indication.
Later ASNb with Anchor PC/LR will conduct MS De-registration procedure, the related network entities will
release the the assigned resource for this MS and delete the MS context.

STEP 6

ASNb with Anchor PC sends NetExit MS State Change Request message including Power Down Indication to
ASNe associated with Anchor DPF/ FA.

STEP 7, 10

ASNe with Anchor DPF/FA sends NetExit MS State Change Req including deleting MS context indication to
Anchor ASNc with Anchor Authenticator.

For PMIP and CMIP terminal, before this step, ASNe with FA will initiate the MIP De-Registration procedure. For
PMIP, ASNc with Anchor PMIP Client, ASNe with FA, HA can complete MIP De-Registration procedure based on
the normal MIP De-registration procedure; for CMIP, FA can perform MIP Revocation procedure based on [26].

1 Additionally the associated entities will release the related MS context and resource retained by these entities. See
2 section 4.8 for details for MIP session termination.

3 **STEP 8, 9**

4 The ASNc with Anchor Accounting Client sends Accounting Stop message including a Release Indication of MS
5 De-registration to AAA (visited-AAA/Home-AAA) for location update and indicating MS de-registration network
6 AAA server releasing the related MS contexts.

7 **STEP 11**

8 After releasing the MS context retained by the related entity, Anchor DPF/FA reply NetExit MS State Change
9 Response to ASNa with Anchor PC. Anchor PC releases the retained MS context.

10 **4.5.2.2.2 Network Trigger**
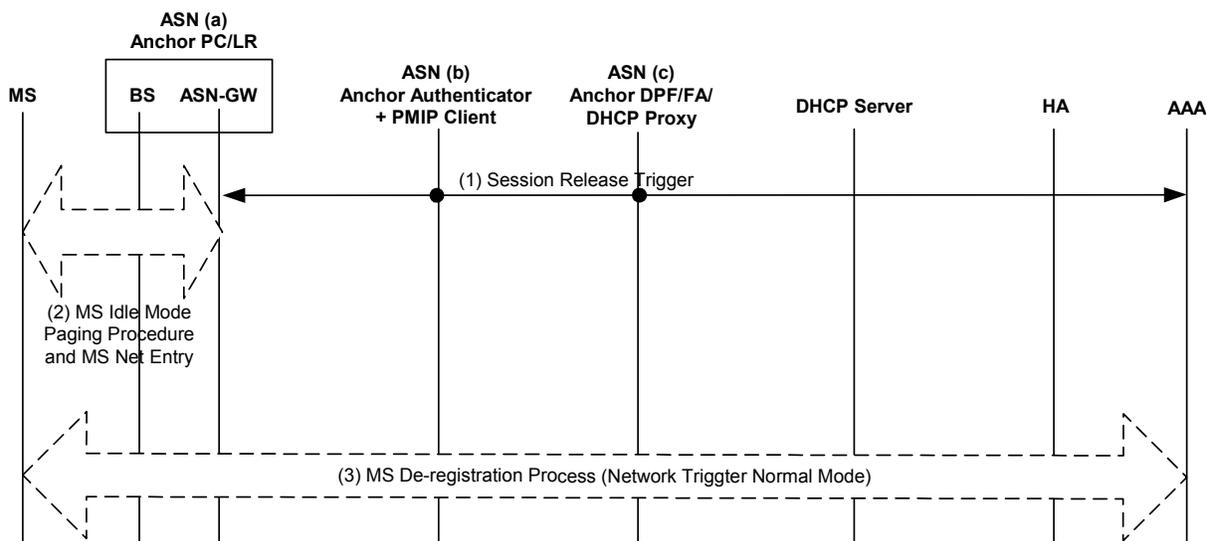
11

12 **Figure 4-35 – Network Trigger (Idle Mode)**

13 **STEP 1**

14 During Idle Mode, the related network entities, such as AAA server, Anchor PC, FA etc. may trigger MS exiting
15 network; And the final decision SHALL be made by the Anchor PC; If decision has been made to exit the MS while
16 it is in Idle mode, the Anchor PC initiates the paging procedure for this MS.

17 **Case 1 - AAA Server Trigger**

18 See AAA Server Trigger conditions as specified in Network Trigger (Normal Mode) section 4.5.2.1.2.

19 **Case 2 - Anchor DPF/FA Trigger**

20 See Anchor DPF/FA Trigger conditions as specified in Network Trigger (Normal Mode) section 4.5.2.1.2.

21 **Case 3 - Anchor Authenticator Trigger**

22 See Anchor Authenticator Trigger conditions as specified in Network Trigger (Normal Mode) section 4.5.2.1.2.

23 **Case 4 – Anchor PC Trigger**

24 ASN(a) hosting the Anchor PC may trigger the MS deregistration process because of any error conditions with
25 respect to the MS's Idle state, such as the Idle Mode System Timer expires, absence of response to paging messages
26 to *LU_Req* etc.

1 **STEP 2**

2 Network initiates the Idle Mode Paging procedure for the MS, and MS enters the network as described in section
3 4.5.1.

4 **STEP 3**

5 When the MS enters network from Idle mode, it is Active and normal. Hence to deregister the MS from the network,
6 network triggered exit (normal mode) procedure described in section 4.5.2.1.1 are followed.

7 **4.5.2.3   Message Composition**

8 **4.5.2.3.1   R4/ R6 Data Path Control Messages**

9 MS Network Exit may be indicated using Path De-Registration message exchange.

10 The *Path_Dereg_Req* message composition is shown in Table 4-42:

11 **Table 4-42 – Path_Dereg_Req Message in MS Network Exit Procedure**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
BS Info	5.3.2.26	O	
MS Info	5.3.2.103	M	Compound TLV including information about MS.
>MSID	5.3.2.102	O	MS MAC address
>Anchor GW ID	5.3.2.10	O	Unique Identifier of the Anchor GW (Anchor DP entity).
>Authenticator ID	5.3.2.19	O	Unique Identifier of the Anchor Authenticator entity
>Action Code	5.3.2.3	O	Included only when the message is directed to a Serving BS and if it carries the instruction for MS Network Exit. Deregistration instruction for the MS
>Network Exit Indicator	5.3.2.109	O	Included only when the message is sent from DPF in Serving BS to Relay DPF and from Relay DPF to Anchor DPF. If present, indicates the reason of MS Network Exit (e.g. MS Power Down indication, radio link with MS is lost, etc.).
>SF Info	5.3.2.185	O	Compound TLV comprising the information related to Service Flow (either UL or DL). Multiple SF Info may be included in the message. This compound TLV will include accounting information relevant for the flow reported by the accounting agent.

12 **4.5.2.3.2   R4/R6 MS Stage Change Messages**

13 Delete MS Context Directive message is used to indicate or command MS Network Exit. The message composition
14 is presented in Table 4-43:

1 **Table 4-43 – Delete MS Context Directive Message Composition**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	O	Compound TLV including information about BS.
>BS ID	5.3.2.25	O	Unique BS Identifier.
MS Info	5.3.2.103	M	Compound TLV including information about MS.
>MSID	5.3.2.102	O	MS MAC address
>Anchor GW ID	5.3.2.10	O	Unique Identifier of the Anchor GW (Anchor DP entity).
>Authenticator ID	5.3.2.19	O	Unique Identifier of the Anchor Authenticator entity
>Action Code	5.3.2.3	O	Deregistration instruction for the MS Included only when the message is directed to a Serving BS and if it carries the instruction for MS Network Exit.
>Network Exit Indicator	5.3.2.109	O	If present, indicates the reason of MS Network Exit (e.g. MS Power Down indication, radio link with MS is lost, etc.).

2 ### 4.5.2.3.3 R3 RADIUS Messages

3 Home-AAA server MAY trigger MS Network Exit process using RADIUS procedure:

4 • Disconnect-Request message is sent by AAA to NAS to initiate MS Network Exit;

5 • Disconnect-ACK message is sent by NAS to AAA as a positive response to Disconnect-Request;

6 • Disconnect-NACK message is sent by NAS to AAA as a negative response to Disconnect-Request (e.g.
7 MS context is not found).

8 The message composition is presented 5.4.1.7:

9 .

10 ## 4.6   QoS and SFID Management

11 ### 4.6.1   Introduction

12 This section describes the control protocol and messaging to realize the QoS-related functions described in section
13 7.6 of the NWG Stage 2 specification [11]. The control protocol is based on RADIUS and transported over the ASN
14 transport protocol specified in section 4.

15 This specification defines the following procedures:

16   a. Pre-provisioned service flow creation, modification, and deletion.

17   b. Initial Service Flow creation, modification and deletion

18   c. Static QoS policy provisioning between AAA and SFA.

19   d. Service Flow ID management

20 As the scope of Release 1.0.0 is limited to pre-provisioned service flows, PF-SFA interactions are not addressed in
21 this release.

22 ### 4.6.2   Functional Model

23 The QoS functional model is illustrated in Figure 7-33 "QoS Functional Elements" of [11]. This model indicates
24 three functional entities, the PF (out of scope of Release 1.0.0), the Anchor-SFA, Serving-SFA and the SFM, and
25 peering relationships between the PF and the SFA, and the SFA and the SFM. In addition, there is a peering
26 relationship between the SFM and the MS, but this interaction is covered by the IEEE 802.16 specifications. At the

network entry of a MS, the Anchor SFA and the Serving-SFA SHALL be the same entity. The SFA may be split between Anchor SFA and Serving SFA after a handover. The Anchor-SFA should be collocated with the AAA-client where the Authenticator ID SHALL be used to address the Anchor-SFA. The Serving-SFA should be collocated with the FA / AR where the Anchor GW ID SHALL be used to address the entity. The FA/AR should be collocated with the Serving-SFA as the Serving-SFA SHALL trigger the Anchor-DP function in case of SF creation, modification or deletion.

The interaction between PF and SFA is out of the scope of this specification.

4.6.2.1   Policy Framework

The policy framework consists of:

- Subscriber QoS profile information accessible to the SFA function,
- Local policy information accessible to the SFA function and
- Admission control policies accessible to the SFM function.

The mechanism for provisioning the policies and QoS profile into a Policy Information Base is not within the scope of this specification. The mechanism for provisioning the pre-provisioned QoS policies and the subscriber QoS profile into the SFA is described in this specification.

4.6.3   Subscriber QoS Profile

The Subscriber QoS profile is defined on a per-subscriber basis. The subscriber is identified by the network access identifier (NAI) that is included by the NAS in RADIUS messages to the HAAA. For each subscriber, the QoS profile includes the permissible number and schedule type of WiMAX service flows and permissible range of values for associated QoS parameters. For instance, a subscriber may be limited to two concurrent real-time service flows.

The HAAA should provide the QoS profile and associated policy rules to the Anchor SFA at the time of user authentication, dependent on the local CSN configuration and the ASN version information provided in the Access-Request.

4.6.4   Service Flow Management

QoS-related messages as defined in section 5.2.1 are used to create, modify and delete service flows over the air. NWG stage-2 specification [11] (section 7.6.3) defines following:

- Pre-provisioned service flow creation, modification and deletion
- Initial Service Flow creation and deletion
- Service Flow management to support MS mobility

Dynamic service creation procedures are deferred to a future Release.

4.6.4.1   Pre-Provisioned Service Flows

Pre-provisioned service flows are defined as service flows which SHALL be activated at network entry after successful MS access authentication. Figure 4-39 describes protocol actions allowing pre-provisioned service flow setup. If any of the pre-provisioned service flows other than the initial service flow (see later section for more details on the initial service flow) is failed to be activated by the local ASN, and if the "Combined Resources Required" flag for the associated MS is set, the MS shall be denied of the service by the local ASN.

4.6.4.1.1 Create Service Flow

During Initial Network Entry procedure (section 4.5), the authenticator receives indication about the successful completion of authentication via Access-Accept message from AAA server. The AAA server SHALL include the QoS profile in the Access-Accept message (section 5.4) sent to AAA-client. This information is provided to the Anchor-SFA. The first serving SFA detects the completion of registration through means of Initial Network Entry procedures (see section 4.5). The creation of the Service Flow SHALL take place after a successful Initial Network Entry procedures as described in section 4.5, steps 27/28.

In this release, this is the only time when creation of service flows takes place.

1 ### 4.6.4.1.2 Delete Service Flow

2 Deletion of service flows may only take place as part of the network exit procedure (as described in section 4.5) or
3 in case of error handling. Explicit triggers to delete service flows are not supported.

4 ### 4.6.4.1.3 Modify Service Flow

5 There is no modification supported in Release 1.0.0.

6 ### 4.6.4.2 Initial Service Flow

7 The Initial Service Flow is a special kind of a Pre-Provisioned Service Flow as described at the previous section.
8 Among the set of pre-provisioned unicast service flows, the very first pair of service flows (i.e. for uplink and
9 downlink) that are initiated by the SFA are called the Initial Service Flows (ISF).

10 The purpose of the ISF is that it is used by the MS and the ASN to transfer delay tolerant control traffic such as
11 standards-based IP configuration management and IP client application signaling (e.g. DHCP DISCOVERY, FA
12 Advertisement, Mobile IP Registration, Router Advertisment, SIP signaling etc.) in case of IP-CS as well as
13 configuration management signaling required for Ethernet in case of Eth-CS.

14 If any of the initial service flow is failed to be activated by the local ASN, and if the "Combined Resources
15 Required" flag for the associated MS is set, the MS shall be denied of the service by the local ASN. Otherwise, if the
16 "Combined Resources Required" flag is not set, and at least one of the initial service flows of the MS is operational,
17 the ASN shall continue the support the MS operation at the local ASN.

18 ### 4.6.4.2.1 IP-CS Related Issues

19 Since the ISF is established prior to the IP address assignment to the MS, the ASN cannot rely on the IP header
20 information initially to determine the proper routing decision to forward any downlink traffic destined to the MS.
21 Therefore, a special context binding, which contains the MSID and/or MS's NAI information, is required to be
22 installed at the ASN to associate with the peer SFIDs of the ISF (i.e. the two uni-directional SFIDs for uplink and
23 downlink) for the given MS to process the uplink and downlink IP packets. In the case when multiple pre-
24 provisioning service flows including the ISF are established before the IP address assignment to the MS, for the IP
25 CS based ISF, the special context binding may have to be done at the service flow level in order to allow the
26 downlink IP client application signaling packet to be directed to the appropriate ISF transport over R6. During the
27 time of initial creation of ISF to IP address acquisition is complete, all other pre-provision service flows SHALL not
28 transport any IP traffic. The existence of the ISF does not preclude the MS to send IP configuration and IP client
29 application signaling over another service flow that has been created by the MS once the MS has been assigned with
30 an IP address with the support of ISF. Except from the time of creation, an ISF is treated like any other pre-
31 provisioned service flow (like from the parameters settings as well as from the accounting perspective. Once the
32 ASN is aware of the assigned IP address for the MS, ASN MAY perform the following steps:

33 1) Update the classifier and QoS policy of the ISF, and any existing pre-provisioned service flow, which are
34   created during the ISF

35 2) In the case where ISF was created and pre-provisioned flow was not created, ASN SHALL initiate the service
36   flow creation request and apply the QoS policy to the pre-provisioned service flow.

37 Section 4.8, CSN Mobility Management supports three different IP address assignment mechanisms for the MS.
38 Figure 4-36, Figure 4-37 and Figure 4-38 show trigger and steps for updating the ISF and any existing pre-provision
39 service flow.
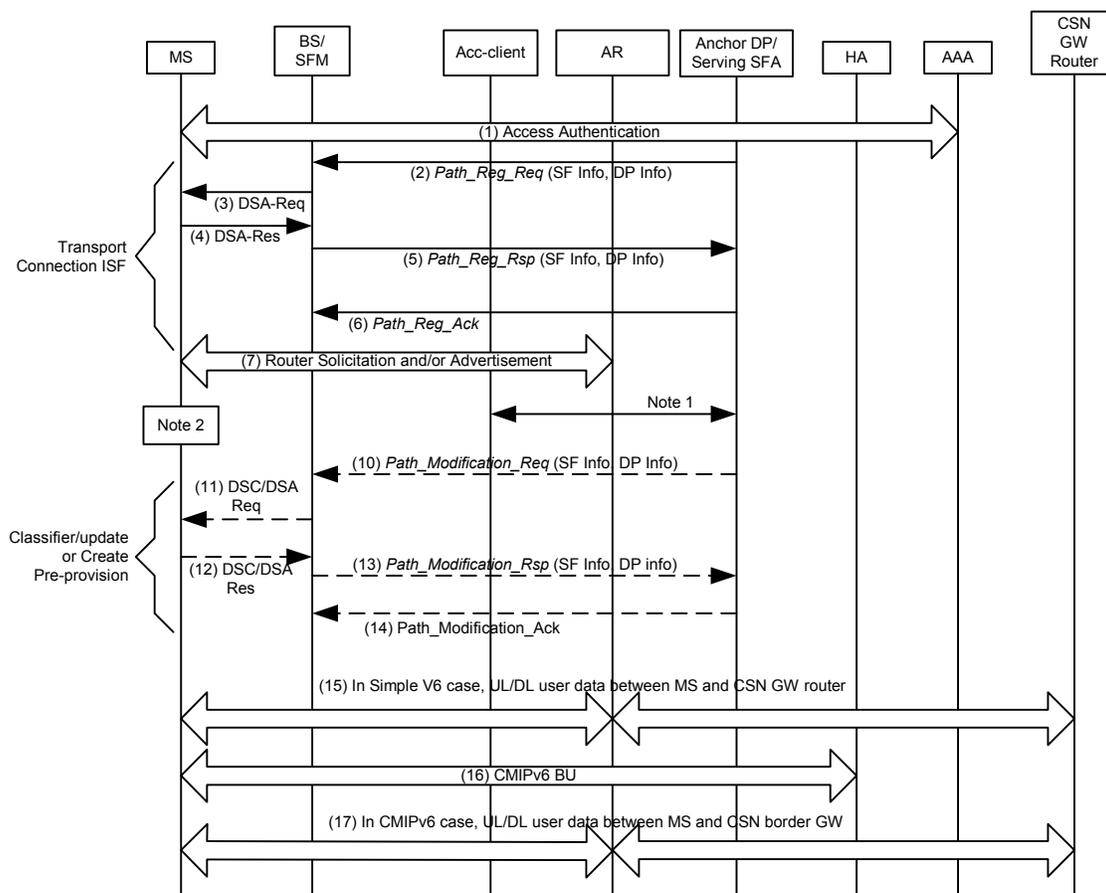
Note 1: AR in the ASN MAY trigger the Anchor DP/Serving SFA to update the SF classifier, with IPv6 Prefix (64bits).
At the same time, AR triggers ACC-Client to start Accounting-Start.
Note 2: Address Auto-configure and DAD occurs after the router solicitation, advertisement and DAD.

1

2 **Figure 4-36 – ISF Classifier Update for IPv6**

3 'The purpoe of the figure in this section is to contextualize the ISF data path setup with classifiers. The figures are
4 informative. For further details, refer to the specific sections in this document.
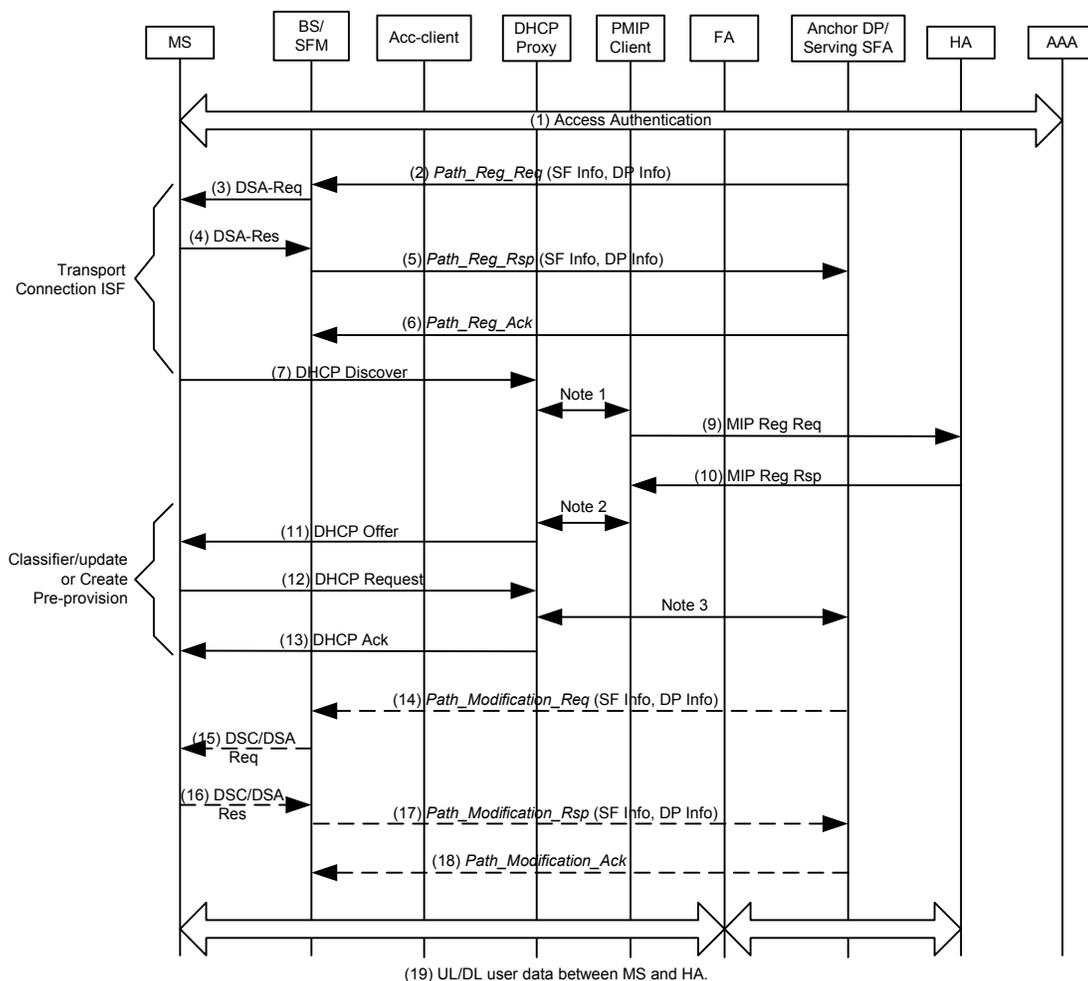
Note 1: DHCP Proxy triggers PMIP client to initiate MIP registration (out of scope).
Note 2: PMIP Client triggers DHCP proxy and passes MIP registration response information (out of scope).
Note 3: DHCP Client in the ASN triggers the Anchor DP/Serving SFA to update the SF classifier (out of scope).

1

2 **Figure 4-37 – ISF Classifier Update for PMIP4**

3 'The purpoe of the figure in this section is to contextualize the ISF data path setupwith classifiers. The figures are
4 informative. For further details, refer to the specific sections in this document.
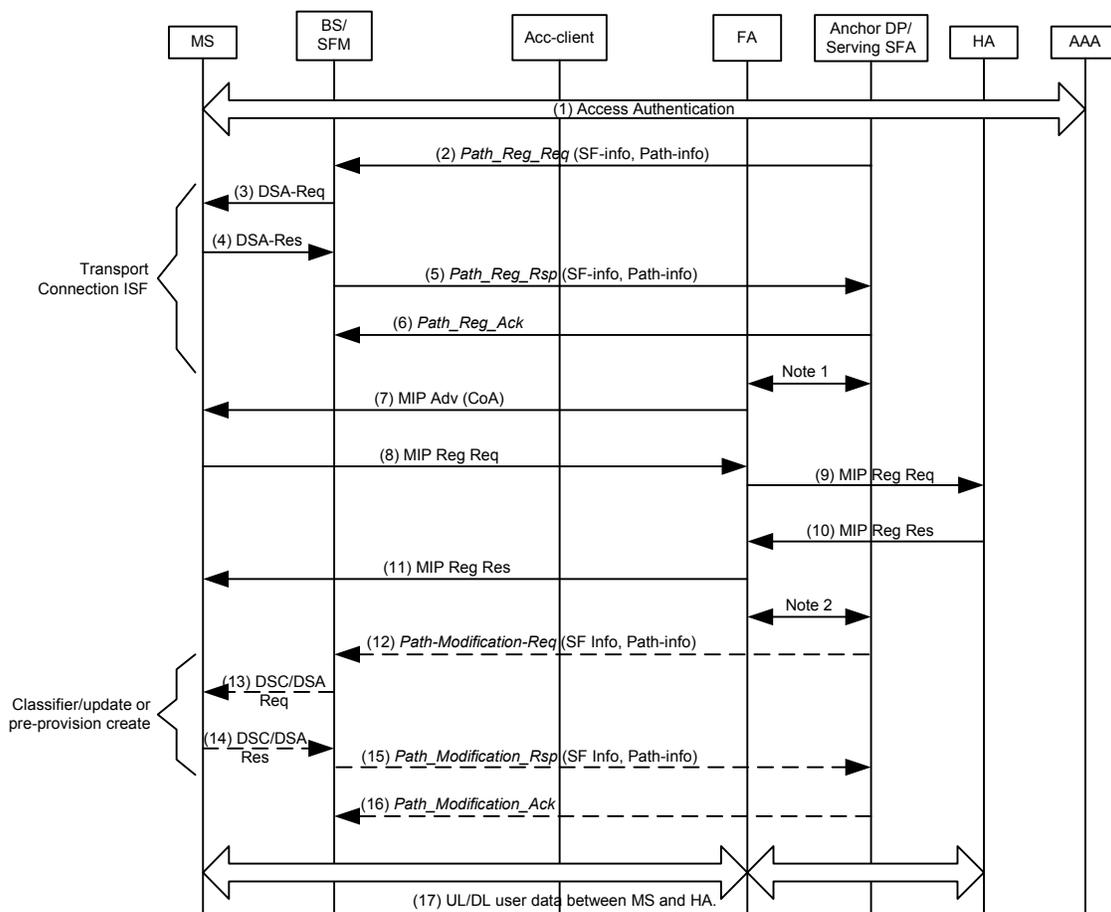
Note 1: Serving SFA triggers FA to initiate MIP registration (out of scope).
Note 2: FA in the ASN triggers the Anchor DP/Serving SFA to update the SF classifier (out of scope).

1

2 **Figure 4-38 – ISF Classifier Update for CMIP4**

3 'The purpoe of the figure in this section is to contextualize the ISF data path setupwith classifiers. The figures are
4 informative. For further details, refer to the specific sections in this document.

5 **4.6.4.2.2 Ethernet-CS Related Information**

6 An Ethernet specific ISF SHALL be established when the authentication procedure IS completed successfully. This
7 ISF SHALL be used for any initial traffic specific for the protocol defined by the Ethernet Type. For IP over
8 Ethernet, the Ethernet specific ISF SHALL be used in the same way as the IP-CS specific ISF (see 4.6.4.2.1).

9 **4.6.4.2.3 Common Issues**

10 At the ASN, the SFA is responsible for assigning SFID to the service flow. As the pre-provisioning service flow
11 information including the Packet Data Flow ID (PDFID) is downloaded to the ASN after the successful MS access
12 authentication, the SFA is responsible to map one or more PDFIDs to a set of unidirectional service flows dependent
13 on the service flow policy configuration information. Note that the PDFID can represent a unidirectional flow.

14 To allow an option of the special monitoring of the ISF which is created for different CS types, this specification
15 recommends the first 20 PDFID(s) from the unicast group of PDFIDs to be assigned to the ISF (i.e. 1 – 20) in both
16 the uplink and downlink directions for each MS – i.e. the service flow pair for the given ISF will be assigned with a
17 PDFID in the uplink , downlink or both directions.

1 By default, the ISF is assigned with the following set of policies; however, the default local policies can be modified
2 dependent on the MS's subscription profile that is downloaded from the H-AAA or V-AAA after the successful MS
3 access authentication as well as dependent on the local BS's policy.

4 • Best effort service class

5 • Wildcard classifier

6 • Transport both IP/Ethernet control and user traffic

7 • Per service flow level of the granularity

8 • HARQ disabled and ARQ enabled

9 • Paging preference is set to 1

10 • Traffic indication is set to 1

11 To ensure the deterministic connection status of the ISF that the WiMAX application can rely on to leverage the ISF
12 as the IP/Ethernet based management connection, the ISF SHALL remain operational as long as the MS is attached
13 to the ASN. However, if any of the ISFs fails to be supported by the local ASN, the MS SHALL be denied of the
14 service by the local ASN. Similar to other service flows maintenance in the ASN, the SFA is responsible for
15 maintaining the ISF.

4.6.4.2.4 Create Service Flow

17 The creation of an ISF takes place as part of the network entry procedure where the creation will be triggered by the
18 ASN. It SHALL be guaranteed by the ASN that the Initial Service Flow (ISF) is the first flow of the pre-provisioned
19 service flows to be activated. There is no other moment where creation of service flows could take place.

20 The service flow being created SHALL be active. Support for provisioned and admitted type is deferred to a future
21 Release.

4.6.4.2.5 Delete Service Flow

23 Deletion of service flows can only take place as part of the network exit procedure. Also, the ISF SHALL be the last
24 to be deleted when the MS is de-registered its service from the ASN. Explicit triggers to delete service flows are not
25 supported.

4.6.4.2.6 Modify Service Flow

27 A modification of service flows may only happen for the ISF. A modification of the ISF may be necessary if an
28 ASN creates it's own ISF which need to be adapted according to the QoS profile received from the home CSN after
29 the allocation of an IP-address. The modification may be prevented if an ASN uses the ISF parameters provided by
30 the CSN at the initial initiation as far as it contains no classifier referencing the IP address of the MS.

4.6.4.3 Data Path Handling

32 The serving SFA SHALL trigger the establishment of the Data Path. The granularity could be per BS, per MS or per
33 SF where the creation per SF SHALL be mandatorily supported.

1   **4.6.4.4   Message Flows and Flow Description**

2   **4.6.4.4.1   Service Flow Creation/Modification**
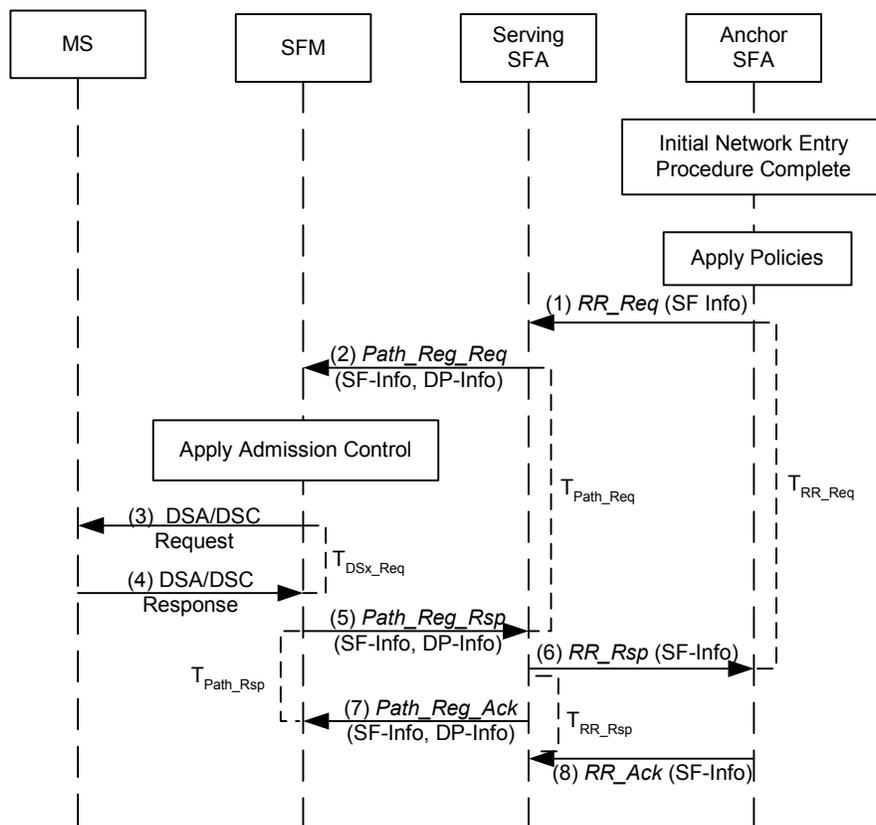
3

4   **Figure 4-39 – SFA-Triggered Service Flow Creation (Profile Downloaded in SFA)**

5   **STEP 1**

6   The QoS profile was received at the Anchor-SFA. *RR_Req* according to Table 4-47 is sent to the Serving-SFA
7   where the QoS-parameters are set according to the received QoS-profile.

8   **STEP 2**

9   Serving-SFA checks if a Data Path needs to be created. Depending on the result a *Path_Reg_Req* according to Table
10   4-53 (if a new DP is required) or a *Path_Modification_Req* according to Table 4-55 (if an existing DP is used) is
11   sent to the SFM. The *Path_Reg_Req* and *Path_Modification_Req* include the received QoS-Info TLV received from
12   the Anchor-SFA.

13   **STEP 3**

14   The SFM verifies whether there are sufficient radio resources and it decides (based on the QoS-Info parameters and
15   the available resources) whether the request should be accepted or not. In case of acceptance, a DSA-Request
16   according to IEEE802.16e [2] is sent to the MS.

17   **STEP 4**

18   MS accepts or rejects the DSA-Request according to IEEE802.16e [2].

1   **STEP 5**

2   Assuming acceptance by SFM in step 3 and acceptance by MS in step 4 (i.e. confirmation code of DSA-Response
3   is OK/success) the SFM sends *Path_Reg_Rsp* and *Path_Modification_Rsp* messages according to Table 4-54 / Table
4   4-56 to the Serving SFA to confirm the reservation. In the case that reduced resources was granted by the SFM, the
5   QoS parameter set of the granted resources SHALL be returned by the SFM in the response back to the Serving
6   SFA.

7   **STEP 6**

8   In case of successful response from the SFM, the Serving SFA sends a *RR_Rsp* message according to Table 4-49
9   with the QoS-Info parameters containing granted QoS values to the Anchor SFA to confirm the reservation. A
10   response message not matching to a sent request (e.g. if SFID of a *Path_Reg_Req* do not match to a received
11   *Path_Reg_Ack*) should be silently discarded.

12   **STEP 7**

13   A *Path_Reg_Ack* and *Path_Modification_Ack* according to section 5.2.3.10 is sent to the SFM.

14   **STEP 8**

15   In case of successful response from the Serving-SFA, the Anchor SFA sends back an *RR_Ack*, as shown in section
16   5.2.1.1, to the Serving-SFA. No further action is necessary by the Anchor-SFA except to keep the context until the
17   MS performs network exit.

18   A response message not matching to a sent request (e.g. if SFID of a *RR_Req* does not match to that of a *RR_Rsp*)
19   should be silently discarded.

20   **4.6.4.4.2 Service Flow Deletion**
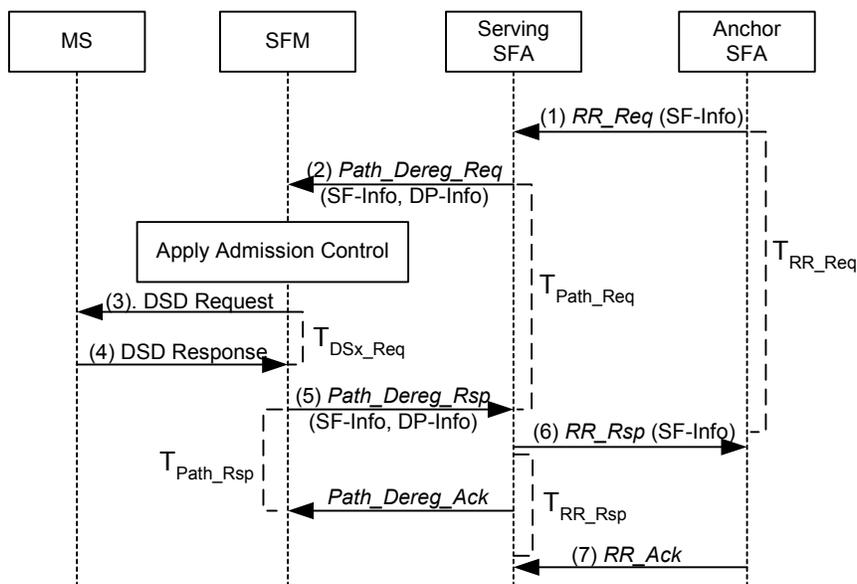
22   **Figure 4-40 – SFA-Triggered Service Flow Deletion**

23   **STEP 1**

24   When a trigger for deletion of SF(s) received at the Anchor-SFA, the Anchor SFA sends an *RR_Req* message
25   according to Table 4-48 to the Serving-SFA where the SF(s) to be deleted.

1 **STEP 2**

2 Serving-SFA checks if a Data Path needs to be released. Depending on the result the Serving SFA sends a
3 *Path_Dereg_Req* according to 4.6.5.6 (if DP should be released) or a *Path_Modification_Req* according to Table
4 4-57 (if existing DP should not be released) to the SFM. The message includes the QoS-Info TLV received from the
5 Anchor-SFA.

6 **STEP 3**

7 The SFM send a DSD-Request according to IEEE802.16e [2] to the MS.

8 **STEP 4**

9 The MS sends a DSD-Response according to IEEE802.16e [2] back to the SFM.

10 **STEP 5**

11 Upon receiving the reponse from the MS, the SFM sends *Path_Dereg_Rsp* and *Path_Modification_Rsp* messages
12 according to Table 4-59 / Table 4-58 to the Serving SFA to confirm the deletion.

13 **STEP 6**

14 Upon receiving a response from the SFM, the Serving SFA sends a *RR_Rsp* message according to Table 4-50 to the
15 Anchor SFA to confirm the service flow deletion. In addition, a *Path_Dereg_Ack* and *Path_Modification_Ack* are
16 sent to the SFM.

17 **STEP 7**

18 Upon receipt of the *RR_Rsp* with Reservation Result set to 0x0005, the Anchor-SFA SHALL release the context for
19 the deleted SFs; a *RR_Ack* according to Table 4-51 SHALL be sent to the Serving-SFA as acknowledgement.

20 **4.6.4.4.3 SF Management Timers and Timing Considerations**

21 This section identifies the timer entities participating in the SF management procedure. The SF management
22 procedure employs five timers (see Table 4-44):

23 • T_{RR_Req}: is started by an Anchor-SFA upon sending a *RR_Req* message. It is stopped upon receiving a
24   corresponding *RR_Rsp*.

25 • T_{Path_Req}: is started when the Serving-SFA sends a *Path_Reg_Req* and *Path_Modification_Req* and is
26   stopped upon receiving a corresponding *Path_Reg_Rsp* and *Path_Modification_Rsp*.

27 • T_{DSx_Req}: is started by the SFM when DSA-request is sent on R1. It is stopped upon receiving a
28   corresponding R1 DSA-Response. It should be implemented according to T_7 specified in IEEE802.16e.

29 • T_{Path_Rsp}: is started by the SFM when it sends a *Path_Reg_Rsp* and *Path_Modification_Rsp* message and is
30   stopped upon receiving a corresponding *Path_Reg_Ack* and *Path_Modification_Ack* message.

31 • T_{RR_Rsp}: is started by the Serving SFA when it sends a *RR_Rsp* message and is stopped upon receiving a
32   corresponding *RR_Ack* message.

33 Table 4-44 shows the maximum value of timers and also indicates the range of the recommended duration of these
34 timers. Note that these values are provisioned in Release 1.0.0.

35 **Table 4-44 – Timer Values for SF Management Procedure**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
T_{RR_Req}			TBD
T_{Path_Req}			TBD

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
T_{DSx_Req}			1 sec *
T_{Path_Rsp}			TBD
T_{RR_Rsp}			TBD

1 * According to T_7 of IEEE802.16e

2 **4.6.4.4.4 SF Management Error Conditions**

3 This section describes error conditions associated with the SF management procedure.

4 **4.6.4.4.4.1   Timer Expiry**

5 The following table shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each
6 timer expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
7 should be performed as indicated in Table 4-45.

8 **Table 4-45 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T_{RR_Req}	Anchor SFA	The Authenticator ASN SHALL initiate network exit procedure and send an Accounting Start message (if not already sent) followed by an Accounting Stop message including an error cause
T_{Path_Req}	Serving SFA	Sends *RR_Rsp* message with Failure Indication TLV set to "Timer expired without response"
T_{DSx_Req}	SFM	Sends *Path_Dereg_Rsp* and *Path_Modification_Rsp* with Failure Indication TLV set to "Timer expired without response". In the case of SF deletion the SFM SHALL release the associated resources
T_{Path_Rsp}	SFM	The requested or deleted resources should be released. The deletion of the SFs on the MS should be triggered as described in [Figure 4-40] step 3 and 4.
T_{RR_Rsp}	Serving SFA	The requested or deleted resources should be released. The deletion of the SFs on the MS should be triggered as described in [Figure 4-40] step 2 to 5.

9 **4.6.4.4.4.2   Path_Reg_Rsp / Path_Modification_Rsp Error**

10 Upon receipt of the *Path_Reg_Req* and *Path_Modification_Req* if the SFM determines that resources are
11 unavailable or in case of non successful response of MS (confirmation code of DSA-Response is different from
12 OK/success), it SHALL send a *Path_Reg_Rsp* and *Path_Modification_Rsp* with the Failure Indication TLV with
13 appropriate error code to the serving-SFA. Upon receipt of the *Path_Modification_Req* if the SFM determines that
14 the modify request does not match an existing SF (e.g. the paramaters of the *Path_Modification_Req* do not match
15 any existing context), it SHALL send the *Path_Modification_Rsp* with the Failure Indication TLV set to "Requested
16 Context Unavailable" to the serving-SFA.

17 **4.6.4.4.4.3   RR_Rsp Error**

18 Upon receipt of the *RR_Req* message to modify an existing context if the Serving-SFA determines that the modify
19 request does not match an existing SF (e.g. the paramaters of the *RR_Req* do not match any existing context), it
20 SHALL send the *RR_Rsp* with the Failure Indication TLV set to "Requested Context Unavailable" to the serving-
21 SFA.

1   Upon receipt of the *Path_Reg_Rsp* and *Path_Modification_Rsp* with the Failure Indication TLV, the serving-SFA
2   will stop timer T$_{Path\_Req}$. The serving-SFA may re-send the *Path_Reg_Req* and *Path_Modification_Req*. If the
3   serving-SFA does not re-send the *Path_Reg_Req* and *Path_Modification_Req* message or if subsequent attempts are
4   also unsuccessful, the serving-SFA SHALL send the *RR_Rsp* message with Reservation Result TLV set to the
5   appropriate error code value.

6   Upon receipt of the *RR_Rsp* message with Reservation Result TLV indicating non-successful response, the Anchor-
7   SFA has to reject the network entry of the MS and SHALL trigger the Authenticator ASN to initiate network exit
8   procedure and to send an Accounting Stop message including an error cause. The Anchor SFA, will stop timer
9   T$_{RR\_Req}$.

10   4.6.5   QoS Messages

11   For QoS specific support, the ASN control plane function type header "0x01"as defined in section 5.2 SHALL be
12   used. This section describes ASN profile agnostic in detail each QoS messages and their associated information
13   elements (IE) in detail.

14   Note: PF is out of the scope of this release.

15   The following IEs are contained in this message, encoded in the TLV format. The notations (M) and (O) are used to
16   indicate Mandatory and Optional, respectively.

17   4.6.5.1   Messages and Information Elements (IEs) for QoS control in the ASN

18   QoS-related messages have been described in IEEE 802.16-2004 [1]. The general format of each such message is
19   described in WiMAX End-to-End Network Systems Architecture Stage 2 [11].

20   WiMAX End-to-End Network Systems Architecture Stage 2 allows the QoS Control message IEs to be combined
21   with Data Path Control messages, when the QoS Control messages are sent along with the data path control
22   messages over R4 and R6 reference points. The service flow creation, modification, and deletion QoS Control
23   messages IEs SHOULD map to the following Data Path Control messages:

24   **Table 4-46 – Data Path Control Messages**

QoS Control Message	Data Path Control Message
RR_Req / RR_Rsp (Create)	*Path_Reg_Req*, *Path_Reg_Rsp* and *Path_Reg_Ack*, or *Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack* if new SF uses existing DP.
RR_Req / RR_Rsp (Modification)	*Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack.*
RR_Req / RR_Rsp (Delete)	*Path_Dereg_Req, Path_Dereg_Rsp* and *Path_Dereg_Ack*, or *Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack* if DP is shared by another SF.

25   4.6.5.2   RR_Req

26   This message is sent from the anchor SFA to the serving SFA. Optionally this message may be sent by the anchor
27   SFA directly to the SFM (if supported by the SFM). A single *RR_Req* message may include more than one SF-Info
28   IE to allow the creation of more than one QoS service flow with a single request. The format of *RR_Req* message
29   and its message type are defined in section 5.2.1.2. *RR_Req* message SHALL not be sent from serving SFA to SFM.

1 **4.6.5.2.1 Service Flow Creation or Modification**

2 **Table 4-47 – RR_Req: SF Creation or Modification**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
> Combined Resources Required	5.3.2.35	O	This is only valid if a single message performs multiple SF reservation. If this flag is set, all SFs within this single message depend on each other. Reservation of all the marked SFs succeeds only if the reservation succeeded for each of these SFs. If reservation fails for one of the marked SFs, none of them will be reserved.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to "Create" or Modification.
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>CS Type	5.3.2.39	O	Specifies Service Flow Convergence Sublayer to be used. If omitted, IPv4 CS is assumed as a default value.
>>Packet Classification Rule	5.3.2.114	O	Packet classifier as defined on R1. This parameters is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classifier Rule Priority	5.3.2.114	M	See IEEE802.16e for further details.
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	M	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.
>>>ROHC/ECRTP Context ID	5.3.2.155	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	
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.

IE	Reference	M/O	Notes
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>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	
>>>Reduced Resources	5.3.2.143	O	
>>Classifier Action	5.3.2.31	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	O	
>>>PHSS	5.3.2.129	O	
>>>PHSF	5.3.2.124	O	
>>>PHSM	5.3.2.126	O	
>>>PHSV	5.3.2.130	O	
>>PHS Rule Action	5.3.2.128	O	Mandatory if PHS-Rules are present.

1 **4.6.5.2.2 Service Flow Deletion**

2 **Table 4-48 – RR_Req: Deletion of a SF**

IE	Reference	M/O	
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Delete".
>>SFID	5.3.2.184	M	SFID as defined on R1.

1   **4.6.5.3   RR_Rsp**

2   This message is sent in response to an *RR_Req*. It is sent by the serving SFA to the anchor SFA. Optionally it may
3   be sent by the SFM directly to Anchor SFA. *RR_Rsp* SHOULD include the SF-Info and the result code of the
4   reservation request. If SFM receives and processes *RR_Req* message from Anchor SFA, this SFM should create/
5   update the data path toward the Anchor DP function for the requested service flows. The format of *RR_Rsp* message
6   and its message type are defined in section 5.2.1.3. The *RR_Rsp* message should not be sent from SFM to the
7   serving SFA.

8   **4.6.5.3.1   Service Flow Creation**

9   **Table 4-49 – RR_Rsp: SF Creation**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Reservation Result	5.3.2.152	M	
>>QoS Parameters	5.3.2.141	O	This is only allowed to be present if "Reduced Resources" was set at the corresponding *RR_Req* message.
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.

1   **4.6.5.3.2 Service Flow Deletion**

2   **Table 4-50 – RR_Rsp: Deletion of a SF**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Reservation Result	5.3.2.152	M	

3   **4.6.5.3.3 RR_Ack**

4   **Table 4-51 – RR_Ack**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.

5   **4.6.5.3.4 Path_Reg_Ack**

6   **Table 4-52 – Path_Reg_Ack**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.

7   **4.6.5.4   Combined Data Path and QoS Control Messages IEs**

8   In the case that data path granularity is per-SF or SF-Info is sent along the data path, the parameters of *RR_Req* may
9   also be delivered by Data Path Control messages instead of the *RR_Req* message.

10 **4.6.5.4.1 Combined Service Flow Creation**

11 *Path_Reg_Req*, *Path_Reg_Rsp* and *Path_Reg_Ack*, or *Path_Prereg_Req*, *Path_Prereg_Rsp* and *Path_Prereg_Ack*
12 messages SHOULD be used to create service flow and data path. These messages are sent from the
13 AnchorDP/serving SFA to the Serving DP/SFM. A single *Path_Reg_Req* or *Path_Prereg_Req* message may include
14 more than one SF-Info IE to allow the creation of more than one QoS service flow with a single request. The format
15 of *Path_Reg_Req* or *Path_Prereg_Req* message and its message type are defined in the section 6.3.1.7.

16   **Table 4-53 – Path-Registration-Request: Creation of SF and DP**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	

IE	Reference	M/O	Notes
>Anchor ASN GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
> Combined Resources Required	5.3.2.35	O	This is only valid if a single message performs multiple SF reservation. If this flag is set, all SFs within a single message depend on each other. Reservation of all the marked SFs succeed only, if the reservation succeeded for each of these SFs. If reservation fails for one of the marked SFs, none of them will be reserved.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Create"
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM.
>>CS Type	5.3.2.39	O	Specifies Service Flow Convergence Sublayer to be used. If omitted, IPv4 CS is assumed as a default value.
>>Paging Preference	5.x.x	O	Indicates paging preference.
>>Packet Classification Rule	5.3.2.114	O	Packet classifier as defined on R1. This parameters is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classifier Rule Priority	5.3.2.114	M	See IEEE802.16e for further details.
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	M	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.
>>>ROHC/ECRTP Context ID	5.3.2.155	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15		See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.

IE	Reference	M/O	Notes
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>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	
>>>Reduced Resources	5.3.2.143	O	
>>Data Path Info	5.3.2.45	O	Identifies the Data Path which should be used for the service flow. This parameter is included only if data path granularity is per-SF. Otherwise, if Data Path is per MS, DP Info TLV is included at the MS Info level.
>>>Data Path ID	5.3.2.44	M	
>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.
>>>SDU SN	5.3.2.178	M	
>>>SDU BSN Map	5.3.2.175	M	
>>Classifier Action	5.3.2.31	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	O	
>>>PHSS	5.3.2.125	O	
>>>PHSF	5.3.2.124	O	
>>>PHSM	5.3.2.126	O	
>>>PHSV	5.3.2.130	O	
>>PHS Rule Action	5.3.2.128	O	Mandatory if PHS-Rules are present.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.

IE	Reference	M/O	Notes
>> Data Path ID	5.3.2.44	M	
>> Data Path Encapsulation Type	5.3.2.42	M	Valid value is only GRE.
>> Data Path Type	5.3.2.47	M	
>> Data Path Integrity Mechanism	5.3.2.46	O	
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

1 **Table 4-54 – Path-Registration-Response: Creation of SF and DP**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	
>Anchor ASN GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM.
>>Reservation Result	5.3.2.152	M	
>>QoS Parameters	5.3.2.141	O	This is only allowed to be present if "Reduced Resources" was set at the corresponding *RR_Req* message.
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.

IE	Reference	M/O	Notes
>>Data Path Info	5.3.2.45	O	Compound TLV including information about Data Path. Included in SF Info TLV only if Data Path is per Service Flow.
>>>Data Path ID	5.3.2.44	M	Data Path Identifier (e.g. GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message
>>Failure Indication	5.3.2.69	O	If present, indicates error conditions and their possible reasons.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.
>>Data Path Type	5.3.2.47	O	Type of the Data Path. Mandatory if DP Info TLV is included.
>>Data Path ID	5.3.2.44	O	Data Path Identifier (e.g. GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

4.6.5.5 Path_Modification_Req

This message is sent from the serving SFA to the SFM. A single DP-Modification-Request message may include more than one SF-Info IE to allow the creation/modification of more than one QoS service flow with a single request. The format of DP-Modification-Request message and its message type are defined in the section 6.3.1.7.

4.6.5.5.1 In Case of Creation of a SF Related to an Existing DP

Table 4-55 – Path-Modification-Request: Creation of SF and Adaptation of an Existing DP

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	
>Anchor GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
> Combined Resources Required	5.3.2.35	O	This is only valid if a single message performs multiple SF reservation. If this flag is set, all SFs within a single message depend on each other. Reservation of all the marked SFs succeed only, if the reservation succeeded for each of these SFs. If reservation fails for one of the marked SFs, none of them will be reserved.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Create".
>>SFID	5.3.2.184	M	SFID as defined on R1.

IE	Reference	M/O	Notes
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM.
>>Packet Classification Rule	5.3.2.114	O	Packet classifier as defined on R1. This parameters is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classifier Rule Priority	5.3.2.32	M	See IEEE802.16e for further details.
>>>IP TOS/DSCP range and mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	M	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.
>>>ROHC/ECRTP Context ID	5.3.2.155	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>Media Flow Type	5.3.2.94	O	
>>>Reduced Resources	5.3.2.143	O	

IE	Reference	M/O	Notes
>>Data Path Info	5.3.2.45	O	Identifies the Data Path which should be used for the service flow.
>>>Data Path ID	5.3.2.44	M	
>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.
>>>SDU SN	5.3.2.178	M	
>>>SDU BSN Map	5.3.2.175	M	
>>Classifier Action	5.3.2.31	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	O	
>>>PHSS	5.3.2.129	O	
>>>PHSF	5.3.2.124	O	
>>>PHSM	5.3.2.126	O	
>>>PHSV	5.3.2.130	O	
>>PHS Rule Action	5.3.2.128	O	Mandatory if a PHS-Rules are present.
>Data Path Info	5.3.2.45	M	
>> Data Path ID	5.3.2.44	M	
>> Data Path Encapsulation Type	5.3.2.42	O	Valid value is only GRE.
>> Data Path Type	5.3.2.47	O	
>> Data Path Integrity Mechanism	5.3.2.46	O	

1   **4.6.5.5.2 In Case of Modification of a SF and the Related DP**

2   **Table 4-56 – Path-Modification-Request: Modification of SF and DP**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	
>Anchor GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
> Combined Resources Required	5.3.2.35	O	This is only valid if a single message performs multiple SF reservation. If this flag is set, all SFs within a single message depend on each other. Reservation of all the marked SFs succeed only, if the reservation succeeded for each of these SFs. If reservation fails for one of the marked SFs, none of them will be reserved.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Modify".
>>SFID	5.3.2.184	M	SFID as defined on R1.

IE	Reference	M/O	Notes
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM.
>>Packet Classification Rule	5.3.2.114	O	Packet classifier as defined on R1. This parameters is mandatory for n-1 SFs when set to Active state. This parameter is optionally if the SF will not already be activated.
>>>Classifier Rule Priority	5.3.2.32	O	See IEEE802.16e for further details.
>>>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.
>>>ROHC/ECRTP Context ID	5.3.2.155	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	O	
>>>BE Data Delivery Service	5.3.2.24	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>UGS Data Delivery Service	5.3.2.196	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Single choice value of the parameters "BE", "UGS", "NRT-VR", "RT-VR" and "ERT-VR"-Data Delivery Service. Only one of the delivery service is allowed to be set.
>>>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.

IE	Reference	M/O	Notes
>>>Media Flow Type	5.3.2.94	O	
>>>Reduced Resources	5.3.2.143	O	
>>Data Path Info	5.3.2.45	M	Identifies the Data Path which should be used for the service flow.
>>>Data Path ID	5.3.2.44	O	
>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.
>>>SDU SN	5.3.2.178	O	
>>>SDU BSN Map	5.3.2.175	O	
>>Classifier Action	5.3.2.31	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	O	
>>>PHSS	5.3.2.129	O	
>>>PHSF	5.3.2.124	O	
>>>PHSM	5.3.2.126	O	
>>>PHSV	5.3.2.130	O	
>>PHS Rule Action	5.3.2.128	O	Mandatory if a PHS-Rules are present.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.
>> Data Path ID	5.3.2.44	M	
>> Data Path Encapsulation Type	5.3.2.42	O	Valid value is only GRE.
>> Data Path Type	5.3.2.47	O	
>> Data Path Integrity Mechanism	5.3.2.46	O	
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

1 **4.6.5.5.3 Deletion of SFs**

2 **Table 4-57 – Path-Modification-Request: Deletion of Service Flow**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Delete"

IE	Reference	M/O	Notes
>>SFID	5.3.2.184	M	SFID as defined on R1.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.
>> Data Path ID	5.3.2.44	M	
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

1 **Table 4-58 – Path-Modification-Response: Deletion of Service Flow**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration
MS Info	5.3.2.103	M	
>Anchor GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Reservation Result	5.3.2.152	M	
>>Failure Indication	5.3.2.69	O	If present, indicates error conditions and their possible reasons.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.
>>Data Path ID	5.3.2.44	O	Data Path Identifier (e.g. GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

2 **4.6.5.6   Path_Dereg_Req**

3 This message is sent from the serving SFA to the SFM or from the SFM to the serving SFA (in Release 1.0.0 the
4 second case can only take place in case of error handling). A single DP-De-Registration-Request message may
5 include more than one SF-Info IE to allow the deletion of more than one QoS service flow with a single request. The
6 format of *Path_Dereg_Req* message and its message type are defined in the section 6.3.1.7.

1 **4.6.5.6.1 In Case of Deletion of a SF**

2 **Table 4-59 – Path-De-Registration-Response: Deletion of Service Flow**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration
MS Info	5.3.2.103	M	
>Anchor GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity)
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Reservation Result	5.3.2.152	M	
>>Failure Indication	5.3.2.69	O	If present, indicates error conditions and their possible reasons.
>Data Path Info	5.3.2.45	O	DP Info compound TLV is included at the MS Info level only if Data Path is per MS and not per SF. Otherwise, if Data Path is per Service Flow, DP Info TLV is included in SF Info.
>>Data Path ID	5.3.2.44	O	Data Path Identifier (e.g. GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	O	

3

4 **4.6.6 SFID Management**

5 The Anchor/Serving SFA takes care of SFID assignment on the Service Flows. An SFID SHALL uniquely represent
6 a Service Flow within the MS.

7 Thus the Anchor/Serving SFA SHALL keep track of the SFIDs that have been already assigned to the MS. This is
8 possible because the SFA is by definition the entity that takes care of service authorization for each particular MS.
9 Thus the Anchor/Serving SFA simply assigns a new SFID by selecting a value, which is not yet in use in the MS
10 with which the Service Flow is associated. This discipline guarantees that {MSID, SFID} pair is unique network
11 wide.

12 If the Anchor/Serving SFA initiates Service Flow creation, then the SFIDs are delivered to the SFM with DP-
13 Registration Request sent from the Anchor/Serving SFA to the SFM. The SFM (in the Base Station) then uses the
14 assigned SFIDs in the IEEE 802.16e DSx message exchange with the MS.

15 Upon a Service Flow release the Anchor/Serving SFA releases the associated SFID, which might be reused later for
16 another, newly created, Service Flow.

17 The SFID assignment for MBS services is TBD.

18 **4.7 ASN Anchored Mobility**

19 **4.7.1 Introduction**

20 This section discusses handover between different ASNs. The internal decomposition of ASN is not discussed. In
21 general the ASNs that participate in HO process are logically divided into four types. These are:

1   a.   Serving ASN that hosts Serving HO Function and serves the MS prior to HO.

2   b.   Target ASN that hosts Target HO Function. There might be one or more Target ASNs. One of them is
3   selected as the final HO Target and becomes Serving ASN after HO completion.

4   c.   Anchor ASN that hosts the Anchor DP Function for the MS.

5   d.   Authenticator ASN that hosts Authenticator/Key Distributor Function for the MS.

6   All ASNs involved in HO SHALL be interconnected with R4 interfaces.

7   Data integrity may be optionally applied during the HO procedure to minimize or prevent data loss as a result of the
8   HO.

9   Support for data integrity is outside the scope of Release 1.0.0.

10   **4.7.2 Fully Controlled HO**

11   **4.7.2.1 HO Preparation Phase**

12   Upon reception of a MOB-MSHO_REQ message from a mobile station (MS), the Serving ASN SHALL initiate a
13   handover to one or more candidate Target ASNs by sending an R4 *HO_Req* message to each Target ASN over the
14   R4 interface.

15   The R4 *HO_Req* message MAY contain an Authenticator ID TLV that points to the Authenticator/Key Distributor
16   Function hosted in the Authenticator ASN. Thus upon receiving an R4 *HO_Req* message, the Target ASN(s) MAY
17   retrieve AK context from the Authenticator ASN. The Target ASN(s) is/are not required to retrieve this information
18   immediately upon receipt of the R4 *HO_Req* message and MAY postpone the retrieval until the Handover Action
19   Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-41.

20   Alternatively, the Serving ASN MAY request on behalf of the target ASN the AK Context from the Authenticator
21   ASN and include it in the R4 *HO_Req* message. This call flow scenario (subsequently referred to as Scenario 2) is
22   shown in Figure 4-42.

23   If the Authenticator ID TLV is not included in the R4 *HO_Req* message, it SHALL be assumed that the Serving
24   ASN is collocated with Authenticator ASN and the Originator of the R4 *HO_Req* message also hosts the
25   Authenticator/Key Distributor Function. In this case the R4 *Context_Req* message SHALL be sent by the Target
26   ASN to the Serving ASN with the IP Address of the R4 *HO_Req* originator. As in the case of Scenario 1, the Target
27   ASN MAY postpone the retrieval until the Handover Action Phase.

28   The Target ASN(s) MAY pre-establish the data path for the MS with the Anchor ASN. If the R4 *HO_Req* message
29   includes the Anchor ASN GW ID TLV which points to the Anchor DP Function hosted in the Anchor ASN and the
30   Target ASN(s) decides to pre-establish the data path, the Target ASN SHALL initiate Data Path Pre-Registration
31   procedure with the Anchor ASN. This call flow scenario is shown in Figure 4-41.

32   If the Anchor ASN GW ID TLV is not included in the R4 *HO_Req* message, it SHALL be assumed that the Serving
33   ASN is collocated with the Anchor ASN hosting the Anchor DP Function. If the Target ASN wants to initiate Data
34   Path Pre-Registration procedure for this configuration, it SHALL send the R4 *Path_Prereg_Req* message to the IP
35   Address of the R4 *HO_Req* message originator.

36   Data Path Pre-Registration at the Handover Preparation Phase is optional and may be executed only when both
37   Target and Anchor ASNs support this functionality. If the Anchor ASN does not support Data Path Pre-Registration
38   and the Target ASN attempts to initiate Data Path Pre-Registration procedure, the transaction should be rejected (i.e.
39   *Path_Prereg_Rsp* message with a rejection code TLV will be sent back to the Target ASN).

40   The Target ASN SHALL respond to the R4 *HO_Req* message with the R4 *HO_Rsp* message, and the Serving ASN
41   SHALL acknowledge the Handover Preparation transaction completion by sending an R4 *HO_Ack* message (see
42   Figure 4-41 and Figure 4-42 for the call flow scenarios).

43   If the Serving and Anchor ASNs are collocated, the Serving/Anchor ASN MAY initiate Path Pre-Registration
44   procedure by sending an R4 *Path_Prereg_Req* message toward the Target ASN as shown in the call flow scenario
45   (subsequently referred to as Scenario 3) shown in Figure 4-43.

1   Note that in Scenario 3, the R4 HO Control messages which arrive to the Target ASN(s) are interleaved with the
2   Data Path Control messages. The Target ASN(s) expect the R4 *HO_Req* message to arrive before the R4
3   *Path_Prereg_Req* message because the R4 *HO_Req* message informs the Target ASN about the pending handover.
4   Since IP routed infrastructure doesn't guarantee in-order delivery of datagrams, the Target ASN(s) MAY reject the
5   R4 *Path_Prereg_Req* message if it arrives prior to R4 *HO_Req* message. Rejection means sending the R4
6   *Path_Prereg_Rsp* message with an appropriate error code. If the R4 *HO_Req* message arrives after the Target
7   ASN(s) have rejected the data path pre-registration by sending the R4 *Path_Prereg_Rsp* message, the Target ASN
8   MAY initiate Data Path Pre-Registration procedure on its own (i.e. proceed according to the Scenario 2, shown on
9   the Figure 4-42).

10 Optionally the Serving/Anchor and Target ASNs, if they work according to the call flow shown in the Scenario 3,
11 MAY include the relevant Data Path Info TLVs within the relevant HO Control messages. In other words the R4
12 *HO_Req* message may also include the data path control information contained in the R4 *Path_Prereg_Req* message
13 and the R4 *HO_Rsp* message may include the information contained in the R4 *Path_Prereg_Rsp* message. The R4
14 *HO_Ack* message will also serve as the R4 *Path_Reg_Ack* message. This scenario (subsequently referred to as
15 Scenario 4) is shown in Figure 4-43.

16 Such combining or piggybacking of data path pre-registration messages over handover control messages is possible
17 only when both Anchor and Target ASNs support this feature. The Anchor ASN MAY initiate this procedure, but if
18 the Target ASN doesn't support message combining it will simply ignore the Data Path Info TLVs in the R4
19 *HO_Req* message and respond with an R4 *HO_Rsp* message which doesn't contain any Data Path Info TLVs. In this
20 case the Target ASN MAY initiate Data Path Pre-Registration on its own (i.e. proceed according to the Scenario 2,
21 shown in Figure 4-42).

22 If the Target ASN supports HO Control and DP Control message combining and receives an R4 *HO_Req* message
23 combined with *Path_Prereg_Req* TLVs, it SHALL respond with the R4 *HO_Rsp* message combined with
24 *Path_Prereg_Rsp* TLVs. And, an R4 *HO_Ack* message combined with *Path_Prereg_Ack* TLVs SHALL be sent by
25 the Serving ASN as the acknowledgment of the R4 *HO_Rsp* message.

26 The Target ASN(s) need to know whether or not it may expect an R4 *Path_Prereg_Req* message coming from the
27 Anchor ASN.

28 If the Serving ASN and Anchor ASN are collocated, and the Serving ASN intends to initiate Data Path Pre-
29 Registration procedure, then the Serving ASN SHALL include the Data Path Establishment Option TLV in the R4
30 *HO_Req* message. If the TLV is included and if the Target ASN(s) support Data Path Pre-Registration, the Target
31 ASN(s) MAY wait for the Serving ASN to initiate the Data Path Pre-Registration procedure or MAY optionally
32 initiate Data Path Pre-Registration procedure on its own.

33 If the Data Path Establishment Option TLV is included, the Target ASN(s) should expect DP Pre- Registration
34 Request message from the Serving/Anchor ASN. The Target ASN(s) MAY still however initiate Data Path Pre-
35 Registration procedure.

36 If the Data Path Establishment Option TLV is not included, the Target ASN MAY initiate Data Path Pre-
37 Registration procedure on its own.

38 To summarize, data path pre-registration during the handover preparation phase is optional and may occur when
39 both the Target ASN and Anchor ASN support the procedure. The Target or Anchor ASN may choose not to
40 perform data path pre-registration. Retrieval of AK Context from the Authenticator during the Handover
41 Preparation phase is also optional and may optionally occur during the Handover Action phase.

42 **4.7.2.1.1 R4 Message Definitions for HO Preparation Phase**

43 This section describes the R4 message definitions for the HO Preparation Phase

44 **Table 4-60 – HO_Req**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Anchor ASN GW ID	5.3.2.10	O	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. Included if the originator of *HO_Req* does not host the Anchor DP Function for the MS.
>Authenticator ID	5.3.2.19	O	Identifies the node that hosts Authenticator and Key Distributor Function. Inlcluded if the originator of the *HO_Req* does not host the Authenticator and Key Distributor Function for the MS.
>Anchor MM Context	5.3.2.11	O	The TLV MAY be included in order to optimize FA Relocation to the Target ASN after HO. If included, notifies the Target ASN that FA relocation to the Target ASN will be initiated after HO. The Target ASN MAY use it to decide whether or not to accept the HO.
>SBC Context	5.3.2.174	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>REG Context	5.3.2.144	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>PKM Context	5.3.2.131	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>SA Descriptor	5.3.2.170	O	MAY be included if the Serving ASN retrieves the information for the Target ASN from the Authenticator ASN. If not included the Target ASN SHALL retrieve the information
>Data Path Info	5.3.2.45	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the R4 tunneling granularity is per MS. The TLV MAY be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.

IE	Reference	M/O	Notes
>Tunnel Endpoint	5.3.2.194	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the tunnel endpoint IP Address is different from the message sender's IP Address
>SF Info (one or more)	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Direction	5.3.2.59	M	
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Data Path Info	5.3.2.45	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the R4 tunneling granularity is per SF. The TLV MAY be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
>>Packet Classification Rule (one or more)	5.3.2.114	O	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classifier Rule Priority	5.3.2.32	M	
>>>Classifiers	5.3.2.30	M	
>>QoS Info	5.x.x	M	
>>>QoS Parameters	5.3.2.141	M	
BS Info (Serving)	5.3.2.26	M	
>BS ID	5.3.2.25	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Serving
>Round Trip Delay	5.3.2.156	O	MAY be included in order to allow the Target ASN to estimate whther the MS can receive the same quality of service as in the Serving ASN.
>DL PHY Quality Info	5.3.2.60	O	MAY be included in order to allow the Target ASN to estimate whther the MS can receive the same quality of service as in the Serving ASN.
>UL PHY Quality Info	5.3.2.197	O	MAY be included in order to allow the Target ASN to estimate whther the MS can receive the same quality of service as in the Serving ASN.

IE	Reference	M/O	Notes
BS Info (Target, one or more)	5.3.2.26	M	Relative Delay, DL/UL PHY Quality Info as viewed by MS
>BS ID	5.3.2.25	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
AK Context	5.3.2.6	O	MAY be included if the Serving ASN retrieves the AK Context for the Target ASN from the Authenticator ASN. If not included the Target ASN SHALL retrieve AK context.
>Data Path Establishment Option	5.3.2.43	O	If included, notifies the Target ASN that the Serving/Anchor ASN is going to initiate Data Path Pre-Registration.
>Relative Delay	5.3.2.146	O	MAY be included in order to allow the Target ASN to estimate whether the MS can receive the same quality of service as in the Serving ASN.
>DL PHY Quality Info	5.3.2.60	O	MAY be included in order to allow the Target ASN to estimate whether the MS can receive the same quality of service as in the Serving ASN.
>UL PHY Quality Info	5.3.2.197	O	MAY be included in order to allow the Target ASN to estimate whether the MS can receive the same quality of service as in the Serving ASN.

1

2   The Context_Req that is sent from the Target ASN to the Authenticator ASN is shown on the Table 4-61.

3   **Table 4-61 – Context_Req from Target ASN to Authenticator ASN**

IE	Reference	M/O	Notes
Context Purpose Identifier	5.3.2.36	M	Set to indicate that that the AK Context is for retrival AK Context and Authorizaqtion Policy for HO
Authenticator ID	5.3.2.19	M	
BS Info (Serving)	5.3.2.26	O	May be included in order to allow the Authenticator to apply authorization policies depending on SBS.
> Serving/Target Indicator	5.3.2.181	M	Set to Serving
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

4   The *Context_Rpt* sent from the Authenticator GW to the Target GW appears as shown on the Table 4-62:

1

Table 4-62 – Context_Rpt from Authenticator ASN to Target ASN

IE	Description	M/O	Notes
Context Purpose Identifier	5.3.2.37	M	Set to indicate that that the Report contains AK Context and Authorization Policy for HO
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
> MS NAI	5.3.2.106	O	MS NAI
>Service Authorization Code	5.3.2.181	O	May be included to convey Authorization Policy to the Target BS
> AK Context	5.3.2.6	M	
>MS IP Address	-	O	IP address of the MS. If Path Pre-registration is used, this TLV SHALL be included.
BS Info (Target)	5.3.2.26	M	
>BS ID	5.3.2.25	M	
Failure Indication	5.3.2.69	O	Provide failure indication for this message

2   *HO_Rsp* format is shown on the Table 4-63.

3

Table 4-63 – HO_Rsp

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Data Path Info	5.3.2.45	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the R4 tunneling granularity is per MS. The TLV MAY be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.

IE	Reference	M/O	Notes
>Tunnel Endpoint	5.3.2.194	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the tunnel endpoint IP Address is different from the message sender's IP Address
>SF Info (one or more)	5.3.2.185	O	It MAY be included if a) Target ASN suggests per SF QoS parameters different from those the Serving ASN has sent in *HO_Req* or b) the Target ASN needs to deliver per-SF Data Path Info.
>>SFID	5.3.2.184	M	
>>Result Code	5.3.2.154	M	
>>Direction	5.3.2.59	M	Specifies the direction of the flow; 0=DL, 1=UL
>>QoS Info	5.x.x	O	It MAY be included if the Target ASN suggests QoS profile different from that sent by the Serving ASN.
>>Data Path Info	5.3.2.45	O	The TLV MAY be included in order to optimize Data Path registration via combining it with HO Control messages. It MAY be included if a) the Serving ASN is collocated with the Anchor ASN, b) the Target ASN supports combining of Data Path Control and HO Control messages and c) the R4 tunneling granularity is per SF. The TLV MAY be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
BS Info (Serving)	5.3.2.26	M	It MAY be included in order to facilitate message delivery in the presence of HO Relay.
> Serving/Target Indicator	5.3.2.181	M	Set to Serving
>BS ID	5.3.2.25	M	
BS Info (Target, one or more)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	
BS HO RSP Code	TBD	O	0: success 1: Target BS doesn't support this HO Type; 2: Target BS rejects for other reasons. 3-255: Reserved

IE	Reference	M/O	Notes
>HO ID	Defined in [2]	O	MAY be included if Optional HO ID is assigned to the MS for use in initial ranging to the Target BS (within the Target ASN) during HO. If included, its value has to be delivered to the MS with MOB_BSHO-REQ or MOB_BSHO-RSP.
>Service Level Prediction	5.3.2.180	O	If not included it dfaults to 3 (No Service Level Predicion Available) in the Serving ASN. The value has to be delivered to the MS with MOB_BSHO-REQ or MOB_BSHO-RSP.
>HO Process Optimization	5.3.2.78	O	If not included defaults to 0b11111111 (Full Optimization). The value has to be delivered to the MS with MOB_BSHO-REQ or MOB_BSHO-RSP.
>HO Authorization Policy Support	Defined in [2]	O	If not included defaults to TBD The value has to be delivered to the MS with MOB_BSHO-REQ or MOB_BSHO-RSP.
>Action Time	5.3.2.4	O	If not included defaults the airframe in which the response is sent plus 10 airframe durations (50 ms),. The value has to be delivered to the MS with MOB_BSHO-REQ or MOB_BSHO-RSP.
> Spare Capacity Indicator	5.3.2.186	O	May be included if the Target ASN reports to the Serving ASN how many MSs with the same PHY Quality Info and the same QoS Parameters might be accommodated in the Target ASN.
>SF Info (one or more)	5.3.2.185	O	TBD
>>SFID	5.3.2.184	M	TBD
>>Data Integrity Info	5.3.2.41	M	TBD

1   *HO_Ack* format is shown on the Table 4-64:

2   **Table 4-64 – HO_Ack**

IE	Reference	M/O	Notes
BS Info (Target, one or more)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

3   The content of the *Path_Prereg_Req* is specified in the Table 4-65.

4   **Table 4-65 – Path_Prereg_Req**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	

IE	Reference	M/O	Notes
>MSID	5.3.2.102	O	
>Anchor ASN GW ID	5.3.2.10	O	MAY be omitted if the IP Destination (for Target Centric) or IP Source (for Anchor Centric) is Anchor ASN GW.
>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per MS. The TLV SHALL be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
>Tunnel Endpoint	5.3.2.194	O	Included if the tunnel endpoint IP Address is different from the message sender's IP Address
>SF Info (one or more)	5.3.2.185	O	It SHALL be included if the R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>CID	5.3.2.29	O	It SHALL be included if the Anchor ASN allocates CID.
>>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per SF. The TLV SHALL be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

1 The content of *Path_Reg_Rsp* is shown on the Table 4-66.

2 **Table 4-66 – Path_Reg_Rsp**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103		
>MSID	5.3.2.102	O	
>Anchor ASN GW ID	5.3.2.10	O	MAY be omitted if the IP Destination (for Anchor Centric) or IP Source (for Target Centric) is Anchor ASN GW.
>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per MS. The TLV SHALL be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
>Tunnel Endpoint	5.3.2.194	O	Included if the tunnel endpoint IP Address is different from the message sender's IP Address

IE	Reference	M/O	Notes
>SF Info (one or more)	5.3.2.185	O	It SHALL be included if the R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>CID	5.3.2.29	O	
>>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per SF. The TLV SHALL be included either as a sub-TLV of MS Info (here) or as a sub-TLV of SF Info, but never both.
>>Data Integrity Info	5.3.2.41	O	TBD
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

1   The content of *Path_Reg_Ack* is shown on the Table 4-67.

2   <div align="center">**Table 4-67 – Path_Reg_Ack**</div>

IE	Reference	M/O	Notes

3 **4.7.2.1.2   Handover Preparation Scenario 1: AK Context Retrieval and Path Pre-Registration**
4   **Initiated by Target ASN**

5   The following call flow describes a successful handover preparation scenario where the Serving ASN provides the
6   Target ASN with the Authenticator ASN ID and the Target ASN pre-establishes the data path during the preparation
7   phase.

1
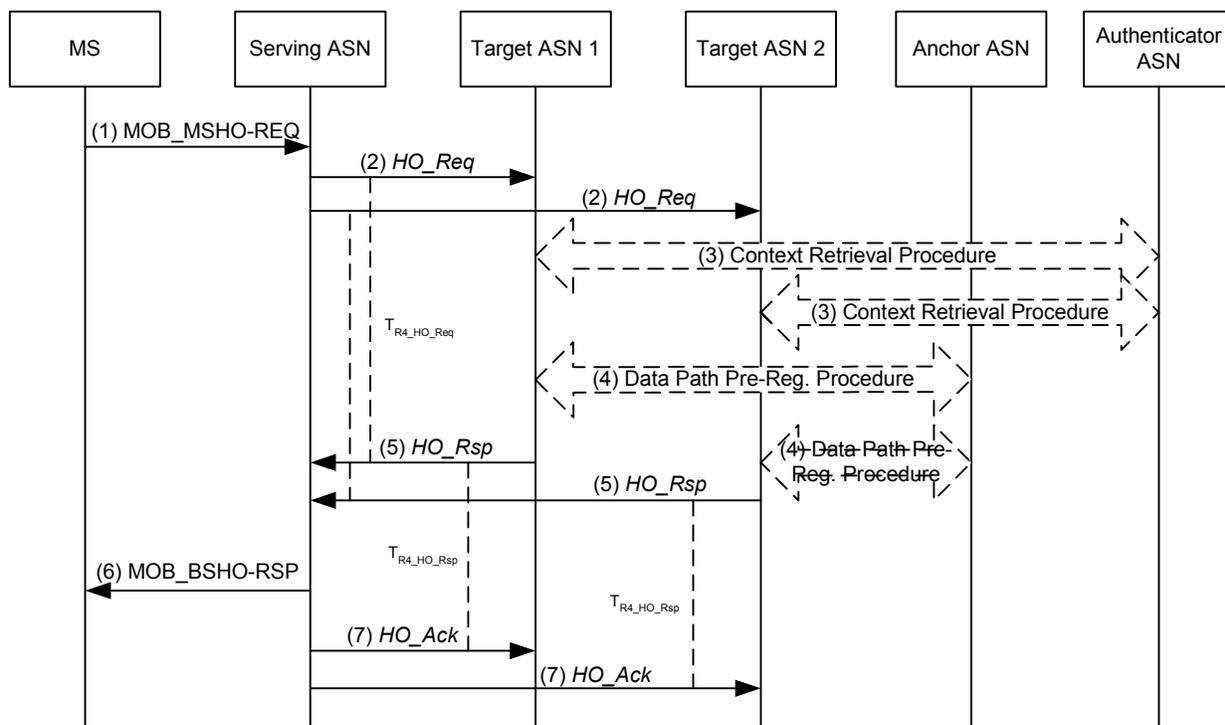
Figure 4-41 – Successful HO Preparation Phase, Scenario 1

STEP 1

The MS initiates a handover by sending a MOB_MSHO-REQ message to the Serving ASN which includes one or more potential target BS's.

STEP 2

The Serving ASN sends an R4 *HO_Req* message to one or more Target ASNs controlling potential target BS's selected for the handover and starts timer $T_{R4\_HO\_Request}$ for each message. The message includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN and the Anchor ASN GW ID of the Anchor Data Path function at the Anchor ASN.

STEP 3

The Target ASN(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.13) with the Authenticator ASN. If no Authenticator ID TLV was received (this means Serving ASN is co-located with the Authenticator ASN), the Target ASN initiates a Context Retrieval procedure with the Serving ASN. Note: The Target ASN(s) may optionally choose to defer this procedure to the handover action phase.

STEP 4

As soon as the context is made available, the Target ASN(s) may initiate pre-establishment of a data path for the MS with the Anchor ASN. It can be initiated if the Serving ASN included the Anchor ASN GW ID in the R4 *HO_Req* message by initiating a Data Path Pre-Registration procedure (see section 4.13) with the Anchor ASN. If the Anchor ASN GW ID was not included, the Serving ASN hosts the Anchor Data Path function and the Target ASN(s) initiates the Data Path Pre-Registration procedure with the Serving ASN. If the Anchor ASN does not support the Data Path Pre-Registration procedure, the R4 *Path_Prereg_Req* message from the Target ASN will be responded by the R4 *Path_Prereg_Rsp* message with an appropriate failure indication. Note: The Target ASN(s) may optionally choose to defer this procedure to the handover action phase.

1 **STEP 5**

2 The Target ASN(s) sends an R4 *HO_Rsp* message to the Serving ASN to acknowledge the handover request and
3 starts $T_{R4\_HO\_Response}$. Upon receipt of the R4 *HO_Rsp* message, the Serving ASN stops timer $T_{R4\_HO\_Req}$.

4 **STEP 6**

5 The Serving ASN sends a MOB_BSHO-RSP message to the MS containing one or more potential target BS's
6 selected by the network for the MS to handover to.[3]

7 **STEP 7**

8 The Serving ASN sends an R4 *HO_Ack* message to the Target ASN(s) controlling the potential target BS(s) selected
9 for the MS. Upon receipt of the R4 *HO_Ack* message, the Target ASN(s) stops timer $T_{R4\_HO\_Rsp}$.

10 **4.7.2.1.3   Handover Preparation Scenario 2: AK Context sent by Serving ASN and Path Pre-**
11 **Registration Initiated by Target ASN**

12 The following call flow describes a successful handover preparation scenario where the Serving ASN requests AK
13 context on behalf of a target ASN from the Authenticator ASN, and then includes this information when initiating a
14 handover to a Target ASN. In the scenario, the Target ASN pre-establishes the data paths during the preparation
15 phase.
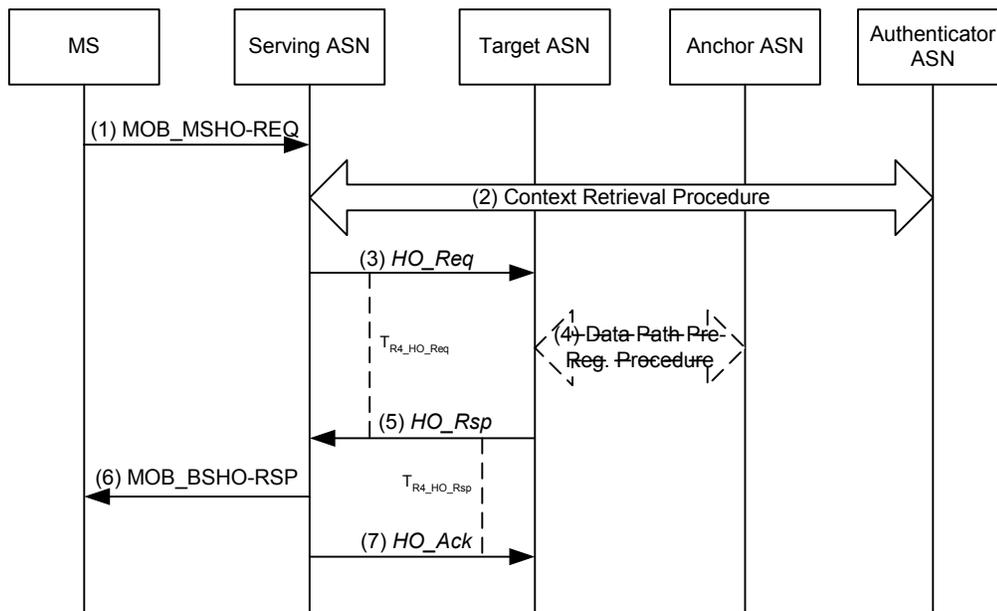
16

17 **Figure 4-42 – Successful HO Preparation Phase, Scenario 2**

18 **STEP 1**

19 The MS initiates a handover by sending a MOB_MSHO-REQ message to the Serving ASN which includes one or
20 more potential target BS's.

---

[3] For example, upon sending of the MOB_BSHO-RSP, the Serving ASN may start the timer $T_{MOB\_HO\_IND}$ to wait for the MS to respond with the MOB_HO-IND message. The value of the $T_{MOB\_HO\_IND}$ SHALL be greater than the MS processing time of the MOB_BSHO_RSP plus the Serving BS scheduling and processing times to process the reception of MOB_HO_Ind from the MS by the Serving BS.

1 **STEP 2**

2 The Serving ASN retrieves AK context for the MS by initiating a Context Retrieval procedure (see section 4.13)
3 with the Authenticator ASN.

4 **STEP 3**

5 The Serving ASN sends an R4 *HO_Req* message containing the AK context for the MS to the Target ASN and starts
6 timer $T_{R4\_HO\_Req}$. The message includes the Anchor ASN GW ID of the Anchor ASN. The Serving ASN may send
7 the message to multiple Target ASNs controlling potential target BS's selected for the handover. Note: The context
8 retrieval and sending it in the R4 *HO_Req* message by the Serving ASN in the handover preparation phase is
9 optional and may be deferred to the handover action phase.

10 **STEP 4**

11 The Target ASN pre-establishes a data path for the MS by initiating the Data Path Pre-Registration procedure (see
12 section 4.13) with the Anchor ASN. If the Anchor ASN GW ID was not included, the Serving ASN hosts the
13 Anchor Data Path function and the Target ASN initiates the Data Path Pre-Registration procedure with the Serving
14 ASN. Note: The Target ASN(s) may optionally choose to defer this procedure to the handover action phase.

15 **STEP 5**

16 The Target ASN sends an R4 *HO_Rsp* message to the Serving ASN to acknowledge the handover request and starts
17 timer $T_{R4\_HO\_Rsp}$. Upon receipt of the R4 *HO_Rsp* message, the Serving ASN stops timer $T_{R4\_HO\_Req}$.

18 **STEP 6**

19 The Serving ASN sends a MOB_BSHO-RSP message to the MS containing one or more target BS's selected by the
20 network for the MS to handover to.[4]

21 **STEP 7**

22 The Serving ASN sends an R4 *HO_Ack* message to the Target ASN(s) controlling the potential target BSs selected
23 for the MS. Upon receipt of the R4 *HO_Ack* message, the Target ASN stops timer $T_{R4\_HO\_Rsp}$.

24 **4.7.2.1.4   Handover Preparation Scenario 3: Anchor ASN Collocated with Serving ASN and R4**
25 **Path Pre-Registration Initiated by Serving/Anchor ASN**

26 The following call flow describes a successful handover preparation scenario where the Anchor ASN is co-located
27 with the Serving ASN. In this scenario, the Serving/Anchor ASN initiates data path pre-establishment with the
28 Target ASN(s). Data path pre-registration messages arrive interleaved with handover control signaling in this call
29 flow example.

---

[4] Same note as the Note 1

1
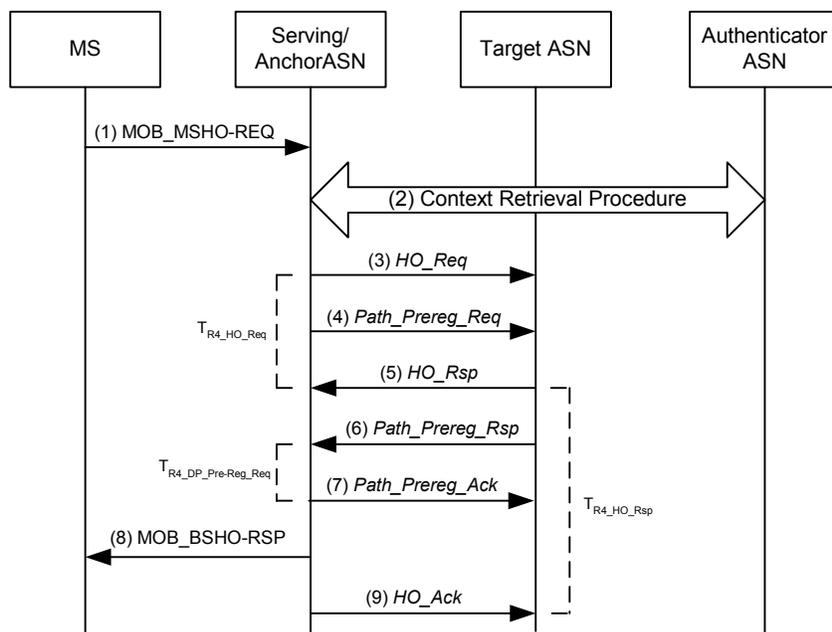
2 **Figure 4-43 – Successful HO Preparation Phase, Scenario 3**

3 **STEP 1**

4 The MS initiates a handover by sending a MOB-MSHO_REQ message to the Serving ASN which includes one or
5 more potential target BSs.

6 **STEP 2**

7 The Serving ASN on behalf of the potential target retrieves AK context for the MS by initiating a Context Request
8 procedure (see section 4.13) with the Authenticator ASN.

9 **STEP 3**

10 The Serving ASN sends an R4 *HO_Req* message containing the AK context for the MS to the Target ASN and starts
11 timer $T_{R4\_HO\_Req}$. The Serving ASN may send the message to multiple Target ASNs controlling candidates target
12 BS's selected for the potential handover.

13 **STEP 4**

14 The Serving/Anchor ASN initiates pre-establishment of a data path for the MS by sending an R4 *Path_Prereg_Req*
15 message to the Target ASN and starts timer $T_{R4\_DP\_Pre\_Reg}$.

16 **STEP 5**

17 The Target ASN sends an R4 *HO_Rsp* message to the Serving ASN to acknowledge the handover request and starts
18 timer $T_{R4\_HO\_Rsp}$. Upon receipt of the R4 *HO_Rsp* message, the Serving/Anchor ASN stops timer $T_{R4\_HO\_Req}$.

19 **STEP 6**

20 The Target ASN sends an R4 *Path_Prereg_Rsp* message to the Serving/Anchor ASN and starts timer $T_{R4\_DP\_Pre\text{-}}$
21 $_{Reg\_Rsp}$. Upon receipt of the R4 *Path_Prereg_Rsp* message, the Serving/Anchor ASN stops timer $T_{R4\_DP\_Pre\text{-}Reg\_Rsp}$.

22 **STEP 7**

23 The Serving/Anchor ASN sends an R4 *Path_Prereg_Ack* message to the Target ASN. Upon receipt of the R4
24 *Path_Prereg_Ack* message, the Target ASN stops timer $T_{R4\_DP\_Pre\text{-}Reg\_Rsp}$.

1 **STEP 8**

2 The Serving ASN sends a MOB_BSHO-RSP message to the MS containing one or more potential target BS's
3 selected by the network for the MS to handover to.[5]

4 **STEP 9**

5 The Serving ASN sends an R4 *HO_Ack* message to the Target ASN controlling the candidate target BS's selected
6 for the MS. Upon receipt of the R4 *HO_Ack* message, the Target ASN stops timer $T_{R4\_HO\_Rsp}$.

7 **4.7.2.1.5 Handover Preparation Scenario 4: Anchor ASN Collocated with Serving ASN and Path**
8 **Pre-Registration Piggybacked onto HO Control messages**

9 The following call flow describes a successful handover preparation scenario where the Anchor ASN is co-located
10 with the Serving ASN. In this scenario, the Serving/Anchor ASN initiates data path pre-establishment with the
11 Target ASN(s). The handover signaling is optimized by "piggybacking" data path pre-registration signaling onto R4
12 handover control messages.
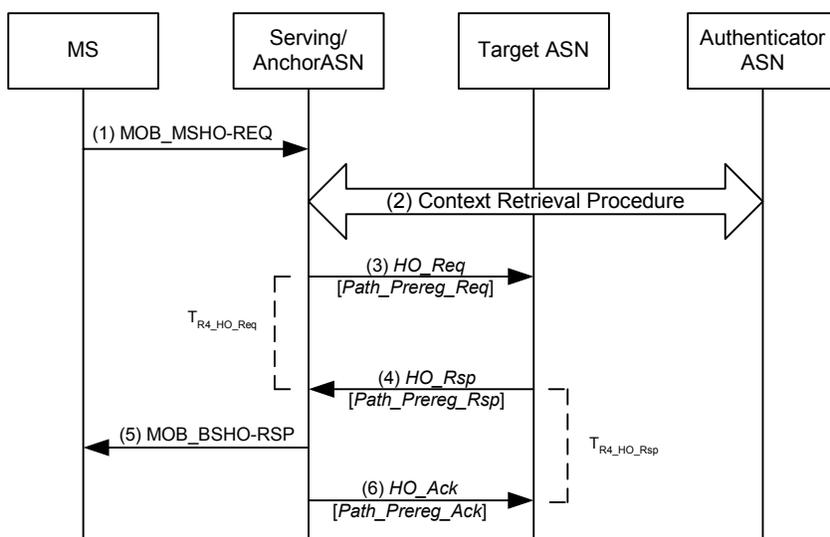
13

14 **Figure 4-44 – Successful HO Preparation Phase, Scenario 4**

15 **STEP 1**

16 The MS initiates a handover by sending a MOB-MSHO_REQ message to the Serving ASN which includes one or
17 more candidate target BS's.

18 **STEP 2**

19 The Serving ASN on behalf of the potential target requests AK context for the MS from the Authenticator ASN by
20 initiating a Context Request procedure (see section 4.13) with the Authenticator ASN.

21 **STEP 3**

22 The Serving ASN sends an R4 *HO_Req* message containing the retrieved AK context for the MS and the Data Path
23 Info TLV to the Target ASN and starts timer $T_{R4\_HO\_Req}$. The Serving ASN may send the message to multiple Target
24 ASNs controlling potential target BS's for the handover.

---

[5] Same note as the Note 1

1 **STEP 4**

2 The Target ASN responds by sending an R4 *HO_Rsp* message which includes the Data Path Info TLV to the
3 Serving ASN to acknowledge the handover request and *Path_Prereg_Req*, and starts timer $T_{R4\_HO\_Rsp}$. Upon receipt
4 of the R4 *HO_Rsp* message, the Serving ASN stops timer $T_{R4\_HO\_Req}$. Note: if the Target ASN does not support
5 piggybacking of data path pre-registration signaling onto handover signaling, the Target ASN may respond by
6 initiating a data path pre-registration procedure with the Serving/Anchor ASN.

7 **STEP 5**

8 The Serving ASN sends a MOB_BSHO-RSP message to the MS containing one or more potential target BS's
9 selected by the network for the MS to handover to.

10 **STEP 6**

11 The Serving ASN sends an R4 *HO_Ack* message to the Target ASN(s) controlling the candidate Target BS(s)
12 selected by the MS. This message also serves as a three-way handshake for the R4 Data Path Pre-Registration.
13 Upon receipt of the R4 *HO_Ack* message, the Target ASN(s) stops timer $T_{R4\_HO\_Rsp}$.

14 **4.7.2.1.6 Network Initiated HO Scenarios**

15 Inter-ASN message transactions associated with the Network Initiated HO Preparation Phase are identical to the
16 transactions associated with the MS Initiated HO Preparation Phase. The difference is in the air interface
17 transactions. Handover is triggered by the internal logic in the Serving ASN (or Serving/Anchor ASN if collocated),
18 without receiving any handover related messages inititiated by the MS. The Network Initiated HO Preparation Phase
19 ends with sending MOB_BSHO-REQ to the MS.

20 Figure 4-45 shows a Network Initiated HO Preparation scenario (Scenario 5) which, from the networking point of
21 view, is identical to the Scenario 1 discussed in 4.7.2.1.3.
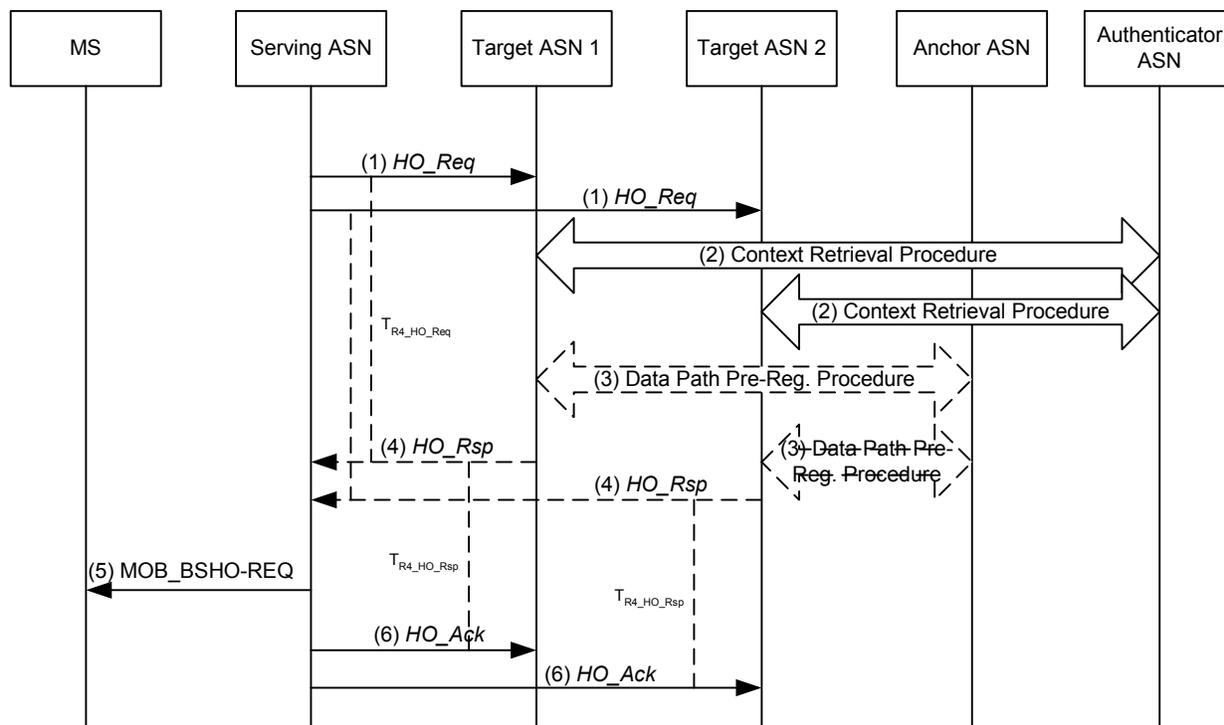
23 **Figure 4-45 – Successful HO Preparation Phase, Scenario 5**

STEP 1

The Serving ASN sends an R4 *HO_Req* message to one or more Target ASNs controlling potential target BS's selected for the handover and starts timer $T_{R4\_HO\_Req}$ for each message. The message
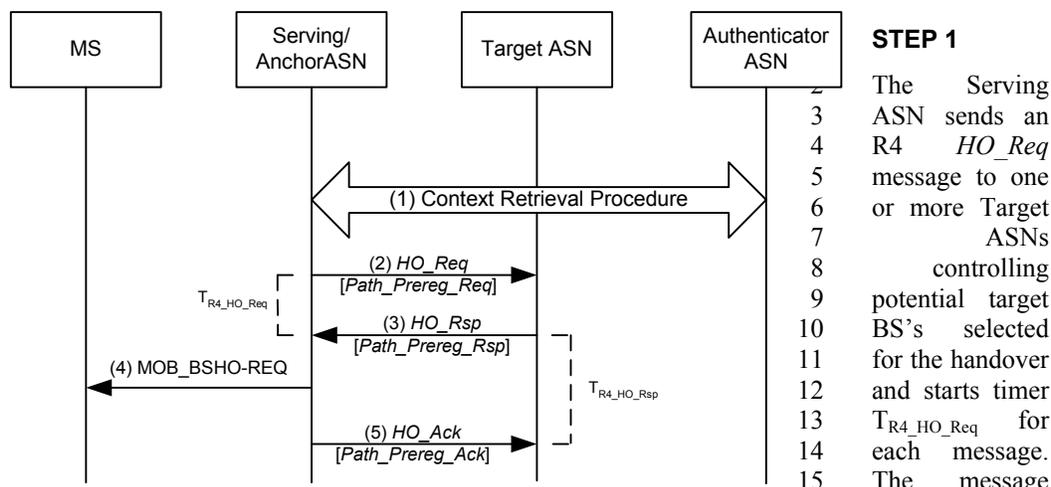
16 includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator
17 ASN and the Anchor ASN GW ID TLV of the Anchor DP function at the Anchor ASN.

18 **STEP 2**

19 The Target ASN(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.13)
20 with the Authenticator ASN. If no Authenticator ID was received (Serving ASN is co-located with the Authenticator
21 ASN), the Target ASN initiates a Context Request procedure with the Serving ASN. Note: The Target ASN(s) may
22 optionally choose to defer this procedure to the handover action phase.

23 **STEP 3**

24 The Target ASN(s) may initiate pre-establishment of a data path for the MS with the Anchor ASN after receiving R4
25 *HO_Req* message. It can be initiated, if the Serving ASN included the Anchor ASN GW ID TLV in the R4 *HO_Req*
26 message, by initiating a Data Path Pre-Registration procedure (see section 4.13) with the Anchor ASN. If the
27 Anchor ASN GW ID TLV was not included, the Serving ASN hosts the Anchor Data Path function and the Target
28 ASN(s) initiates the Data Path Pre-Registration procedure with the Serving ASN. Note: The Target ASN(s) may
29 optionally choose to defer this procedure to the handover action phase.

30 **STEP 4**

31 The Target ASN(s) sends an R4 *HO_Rsp* message to the Serving ASN to acknowledge the handover request and
32 starts timer $T_{R4\_HO\_Rsp}$. Upon receipt of the R4 *HO_Rsp* message, the Serving ASN stops timer $T_{R4\_HO\_Req}$.

33 **STEP 5**

34 The Serving ASN sends a MOB_BSHO-REQ message to the MS containing one or more potential target BS's
35 selected by the network for the MS to handover to.

36 **STEP 6**

37 The Serving ASN sends an R4 *HO_Ack* message to the Target ASN(s) controlling the candidate target BS(s)
38 selected for the MS. Upon receipt of the R4 *HO_Ack* message, the Target ASN(s) stops timer $T_{R4\_HO\_Rsp}$.

39 Figure 4-46 shows a successful Network Initiated Handover Preparation scenario where the Anchor ASN is co-
40 located with the Serving ASN (Scenario 6). From the networking point of view this scenario is identical to Scenario
41 4 discussed in 4.7.2.1.5.

42
43

44 **Figure 4-46 – Successful HO Preparation Phase, Scenario 6**

1   **STEP 1**

2   The Serving ASN on behalf of the target ASN requests AK context for the MS from the Authenticator ASN by
3   initiating a Context Request procedure (see section 4.13) with the Authenticator ASN.

4   **STEP 2**

5   The Serving ASN sends an R4 *HO_Req* message containing the retrieved AK context for the MS and the Data Path
6   Info TLV to the Target ASN and starts timer $T_{R4\_HO\_Req}$. The Serving ASN may send the message to multiple Target
7   ASNs controlling candidate target BS's for the potential handover.

8   **STEP 3**

9   The Target ASN responds by sending an R4 *HO_Rsp* message which includes the Data Path Info TLV to the
10   Serving ASN to acknowledge the handover request and *Path_Prereg_Req*, and starts timer $T_{R4\_HO\_Rsp}$. Upon receipt
11   of the R4 *HO_Rsp* message, the Serving ASN stops timer $T_{R4\_HO\_Req}$. Note: if the Target ASN does not support
12   piggy backing of data path pre-registration signaling onto handover signaling, the Target ASN may respond by
13   initiating a Data Path Pre-Registration procedure with the Serving/Anchor ASN.

14   **STEP 4**

15   The Serving ASN sends a MOB_BSHO-REQ message to the MS containing one or more potential target BS's
16   selected by the network for the MS to handover to.

17   **STEP 5**

18   The Serving ASN sends an R4 *HO_Ack* message to the Target ASN controlling the potential target BS selected by
19   the MS. This message also serves as a three-way handshake for the R4 data path pre-registration. Upon receipt of
20   the R4 *HO_Ack* message, the Target ASN stops timer $T_{R4\_HO\_Rsp}$.

21   **4.7.2.1.7 MS-Initiated HO Preparation Phase – Colocated Serving and Authenticator ASN**
22   **(Scenario 7)**
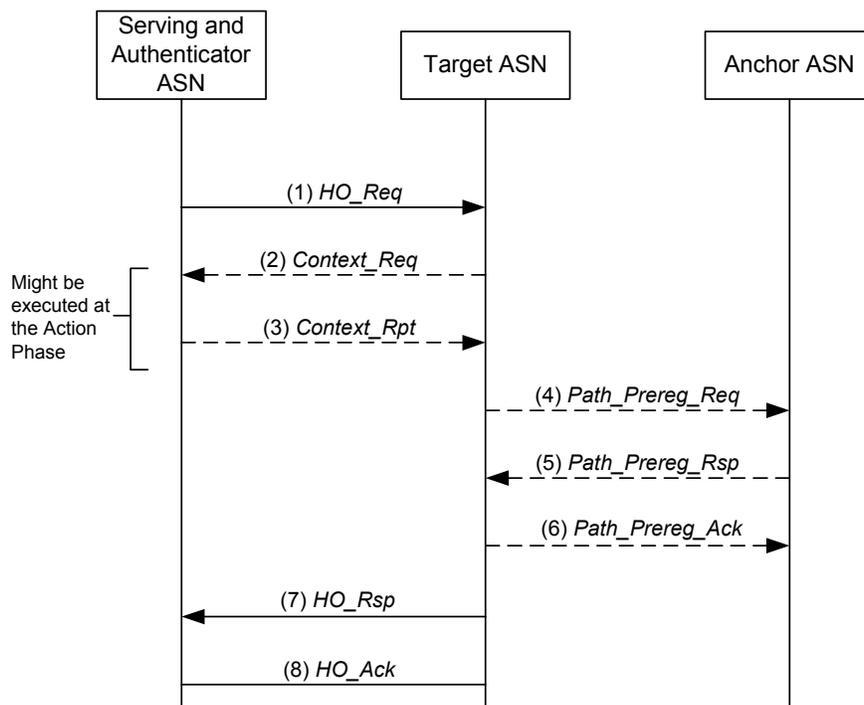
24   **Figure 4-47 – Successful HO Preparation Phase, Scenario 7**

1 **4.7.2.1.8 HO Preparation Stage Timers and Timing Considerations**

2 This section identifies the timer entities participating in the HO Preparation Phase. The following timers are defined
3 over R4:

4 • $T_{R4\_DP\_Pre\_Reg}$: is started by the ASN initiating pre-establishment of the data path for an MS, upon sending
5 the R4 *Path_Prereg_Req* message and is stopped upon receiving a corresponding R4 *Path_Prereg_Rsp*
6 message.

7 • $T_{R4\_DP\_Pre\_Rsp}$: is started by the ASN responding to pre-establishment of the data path for an MS, upon
8 sending the R4 *Path_Prereg_Rsp* message and is stopped upon receiving a corresponding R4
9 *Path_Prereg_Ack* message.

10 • $T_{R4\_Cntxt\_Req}$: is started by the ASN requesting context for a specific MS, upon sending the R4 *Context_Req*
11 message and is stopped upon receiving a corresponding R4 *Context_Rpt* message.

12 • $T_{R4\_HO\_Req}$: is started by a Serving ASN upon sending the R4 *HO_Req* message for an MS to a Target ASN
13 and is stopped upon receiving a corresponding R4 *HO_Rsp* message from the Target ASN.

14 • $T_{R4\_HO\_Rsp}$: is started by a Target ASN upon sending the R4 *HO_Rsp* message for an MS to a Serving ASN
15 and is stopped upon receiving a corresponding R4 *HO_Ack* message from the Serving ASN.

16 Table 4-68 shows the default value of timers and also indicates the range of the recommended duration of these
17 timers. Note that these values are provisioned in Release 1.0.0.

18 **Table 4-68 – HO Preparation Phase Timer Values for R4**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R4\_DP\_Pre\_Reg}$	TBD		TBD
$T_{R4\_DP\_Pre\_Rsp}$	TBD		TBD
$T_{R4\_Cntxt\_Req}$	TBD		TBD
$T_{R4\_HO\_Req}$	TBD		TBD
$T_{R4\_HO\_Rsp}$	TBD		TBD

19 **4.7.2.1.9 HO Preparation Stage Error Conditions**

20 This section describes error conditions associated with the HO Preparation Phase.

21 **4.7.2.1.9.1   Timer Expiry**

22 Table 4-69 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
23 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
24 should be performed as indicated in Table 4-69

25 **Table 4-69 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R4\_DP\_Pre\_Reg}$	ASN initiating Data Path Pre-Registration procedure	No action required.
$T_{R4\_DP\_Pre\_Rsp}$	ASN responding to *Path_Prereg_Req* message	No action required
$T_{R4\_Cntxt\_Req}$	ASN Requesting context info	No action required
$T_{R4\_HO\_Req}$	Serving ASN	The Serving ASN may re-try HO to another Target ASN. If no Target ASN can be

		reached, the ASN SHALL send MS a MOB_BSHO-RSP with Mode set to 0b111
$T_{R4\_HO\_Rsp}$	Target ASN	No action required.

4.7.2.1.9.2   R4 Context_Rpt Error

Upon receipt of the R4 *Context_Req* message, if the ASN is unable to provide the requested information it SHALL send an R4 *Context_Rpt* message to the sender of the R4 *Context_Req* message. The R4 *Context_Rpt* message SHALL include the Failure Indication TLV. Upon receipt of the R4 *Context_Rpt* message with Failure Indication TLV, the ASN SHALL stop timer $T_{R4\_Cntxt\_Req}$ (if running). If the R4 *Context_Req* message was triggered by the Serving ASN, then upon receipt of the R4 *Context_Rpt* message with Failure Indication TLV, the Serving ASN MAY resend the R4 *Context_Req* message. If the Serving ASN does not resend the R4 *Context_Req* message or if the subsequent attempts are also unsuccessful, then in the case of MS initiated handover, the Serving ASN SHALL send a MOB_BSHO_RSP with mode = 0b111 to the MS. If the R4 *Context_Req* message was triggered by the Target ASN, then upon receipt of the R4 *Context_Rpt* message with Failure Indication TLV, the Target ASN MAY resend the R4 *Context_Req* message. If the Target ASN does not resend the R4 *Context_Req* message or if subsequent attempts are also unsuccessful, then the Target ASN SHALL send a R4 *HO_Rsp* message with suitable error code included in the Result Code TLV.

4.7.2.1.9.3   R4 HO_Rsp Error

Upon receipt of the R4 *HO_Req* message, if the Target ASN is unable to support the HO, then it SHALL send R4 *HO_Rsp* message with suitable error code included in the Result Code TLV. Upon receipt of the R4 *HO_Rsp* message indicating HO cannot be supported, the Serving ASN SHALL stop $T_{R4\text{-}HO\_Request}$ (if running). The Serving ASN MAY re-send the R4 *HO_Req* message to a different Target ASN. If the Serving ASN does not re-send the R4 *HO_Req* message, of if all subsequent Target ASNs cannot support the HO, in the case of MS Initiated handover, the Serving ASN SHALL send a MOB_BSHO_RSP with mode = 0b111 to the MS.

4.7.2.1.9.4   R4 Path_Prereg_Rsp Error

Upon receipt of the R4 *Path_Prereg_Req* message, if the ASN is unable to support the pre-establishment of a data path, then it SHALL send a R4 *Path_Prereg_Rsp* message with suitable error code.

Upon receipt of the R4 *Path_Prereg_Rsp* message with suitable error code, the ASN SHALL stop $T_{R4\text{-}DP\_Pre\text{-}Reg}$ (if running).

4.7.2.2   HO Action Phase

If the MS accepts one of the target BSs offered by the serving BS in the MOB_BSHO-RSP (MS initiated) or MOB_BSHO-REQ (network initiated) message to handover to, the MS sends a MOB_HO-IND message with HO_IND_type TLV set to 0b00 to the Serving BS in which it specifies which of the Target BSs offered by the serving BS has been selected for the handover. If the MS accepts a target BS offered to it by the serving BS for handover, the the MOB_HO-IND message is the last message the MS sends to the Serving BS. After sending MOB_HO-IND the MS may start ranging with the Target BS.

Upon receiving a MOB_HO-IND, from the MS indicating acceptance by the MS to handover to a target BS offered by the serving BS in the MOB_BSHO-RSP (MS initiated) or MOB_BSHO-REQ (network initiated) message, the Serving ASN SHALL generate an R4 *HO_Cnf* message and send it to the Target ASN as shown in Figure 4-48. The R4 *HO_Cnf* message includes the "most recent MAC context" at the Serving ASN.

Upon receiving R4 *HO_Cnf* message with the valued for the HO_Indication type which is not set to "Cancel", the Target ASN MAY retrieve the AK Context if this information was not retrieved at the Handover Preparation Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-48.

If the data path between the Anchor ASN and the Target ASN was not pre-established at the Preparation Phase, it MAY be pre-established after receiving R4 *HO_Cnf* message and before the MS completes Network Re-Entry at the Target BS. In this case the Target ASN initiates Data Path Pre-Registration procedure if Data Path Establishment Option TLV was not included in the R4 *HO_Req* message. If the Data Path Establishment Option TLV was included, then the Target ASN can expect R4 *Path_Prereg_Req* message from the Serving/Anchor ASN.

1 *Path_Prereg_Req* and Response message may include Data Delivery Trigger TLV in the SF Info. If this TLV is
2 included it triggers immediate delivery of data for the specified Service Flow.

3 The data paths between the Anchor ASN and the Target ASN SHALL be established via Data Path Registration
4 procedure after the MS arrives at the Target BS. The instance of "MS arrival" at the Target BS could be marked by a
5 mobile initiated ranging, Network Entry completion or Network Re-Entry[6]. If Data Path Registration procedure is
6 invoked after the data path had been pre-registered, the procedure only confirms final establishment of the pre-
7 registered data paths and does not convey any parameters of the data paths except MSID. In such case a two-way
8 Data Path Registration handshake will follow since the Data-Path Pre-registration process had been completed. All
9 the parameters that are related to the data paths SHALL be exchanged during the preceding Data Path Pre-
10 Registration transaction. Furthermore, the Data Path Registration transaction is completed with a two-way
11 handshake; *Path_Reg_Req* and *Path_Reg_Rsp* message exchange and no *Path_Reg_Ack* message (i.e. two-way
12 handshake).

13 If no Data Path Pre-Registration procedure had been completed prior to the Data Path Registration procedure, the R4
14 *Path_Reg_Req* and *Path_Reg_Rsp* messages SHALL convey all parameters relevant for the setup of Data Paths. In
15 this case the R4 *Path_Reg_Ack* message SHALL be sent in response to R4 *Path_Reg_Rsp* message (i.e. three-way
16 handshake).

17 Upon completion of Data Path Registration procedure, the Anchor ASN SHALL initiate de-registration of all the
18 pre-registered data paths to the candidate Target ASNs that have not been selected for the final handover target.
19 Also, the Anchor ASN SHALL initiate de-registration of the data path between itself and the (old) Serving ASN.

20 If the Serving ASN determines that the MOB_HO_IND message was not received from the MS due to a
21 communication loss with the mobile[7] for example upon expiration of an internal timer[8], the Serving ASN may send
22 an R4 *HO_Cnf* message to target ASNs controlling potential target BSs the MS may chose to handover to. The R4
23 *HO_Cnf* message may be sent to target ASN(s) included in the MOB_BSHO-REQ or MOB_BSHO-RSP messages.
24 The R4 *HO_Cnf* message may also be sent to target ASNs which were not notified of a potential impending
25 handover from the MS during the handover preparation phase and whose target BSs where not included in the
26 MOB_BSHO-REQ or MOB_BSHO-RSP messages. The R4 *HO_Cnf* message includes the HO_Indication Type
27 TLV set to "Unconfirmed" and latest MAC context for the MS. When sent to target ASNs which weren't previously
28 notified of an impending handover from the MS during the handover preparation phase, the R4 *HO_Cnf* message
29 SHALL also include the Authenticator GW-ID or AK context, and Anchor GW ID (Anchor DP ASN) information.

30 Upon sending the R4 *HO_Cnf* message, if the Resource_Retain flag was not set, the Serving ASN and its BS
31 SHALL discard all MS's connections resource information including the MAC state machine and all outstanding
32 buffered PDUs, else the Serving BS SHALL retain the connections, MAC state machine and PDUs associated with
33 the MS for service continuation until the expiration of Resource Retain Timer.

34 The Serving BS SHALL release all MAC context and MAC PDUs associated with the MS upon reception of a R4
35 *HO_Complete* message from the Target ASN indicating MS completed a Network re-entry at the Target ASN.

36 If the MOB_HO-IND message is not received at the Serving ASN (message may be lost over the air) the Target
37 ASN will not receive the R4 *HO_Cnf* message. Also, the R4 *HO_Cnf* message may be delayed in the backbone
38 network and arrive after the MS completes Network Re-Entry. If the R4 *HO_Cnf* message is not received by the
39 Target ASN until the MS appears at the Target ASN, the Target ASN MAY request the "most recent MAC Context"
40 via *Context_Req* and *Context_Rpt* exchange with the Serving ASN as it is shown in Scenario 2.

41 After obtaining all the necessary MS Context, the Target ASN SHALL perform the Data Path Registration
42 procedure.

43 Immediately after the MS completes network re-entry, the Target ASN (which at that moment becomes new Serving
44 ASN) SHALL update the Authenticator ASN about successful HO completion via

---

[6] In the later case there is a probability that MS will not complete the Network Re-Entry where it has started because the RNG-
RSP might be lost in the air. In this case the Data Path will have to be registered again, possibly with another Target ASN.

[7] MOB_HO-IND message could be lost over the air or not sent by the MS because it didn't receive the MOB_BSHO-RSP
message from the BS in the MS initiated handover case, or it didn't receive the MOB_BSHO-REQ from the BS in the network
initiated handover case.

[8] For example, $T_{MOB\_HO\_IND}$

1 *NW_ReEntry_State_Change_Directive*. *NW_ReEntry_State_Change_Directive* SHALL deliver to the Authenticator
2 the value of the CMAC_KEY_COUNT the Target ASN holds. Normally this value will be identical to the one the
3 Target ASN received with *Context_Rpt* from the Authenticator ASN. However if the Target BS in the Target ASN
4 receives and authenticates an RNG-REQ message containing a CMAC_KEY_COUNT higher than its own, it
5 SHALL adopt the received count .The resulting count SHALL be delivered to the Authenticator ASN. For details of
6 CMAC Key Count Update, refer to section 4.3.4.2. As soon as the MS Network Re-entry procedure at the Target
7 ASN/BS is completed, the Target ASN MAY send an R4 *HO_Complete* message to the Serving ASN to expedite
8 the resource release in the Serving ASN.

9 If the target ASN can't retrieve the necessary context due to error code"no record found" from serving ASN or
10 authenticator ASN, it SHALL notify MS to conduct full network re-entry.

11 The *HO_Cnf* message with 'cancel' type may be sent to all candidate target ASNs that were not selected as a target
12 for handover. The candidate ASNs may initiate the DP release procedure.after receiving this message.

13 Unselected candidate target ASN may initiate Path Deregistration process if the timer associated with the Path
14 Deregistration expires.

15 If the MS rejects the target BS(s) offered by the serving BS in the MOB_BSHO-RSP (MS initiated handover) or
16 MOB_BSHO-REQ (network initiated handover) message for the MS to handover to by sending a MOB_HO-IND
17 message with HO_IND_type TLV set to 0b10 to the serving BS, the serving BS notifies the candidate target ASN
18 previously notified of a potential handover from the MS in the handover preparation phase by sending an R4-HO
19 Confirm message with a cancellation indication.

20 If the serving BS offers a new target BS candidate for the MS to handover to, it first notifies the target ASN(s)
21 controlling the candidate target BS(s) of a potential handover from the MS as described in the handover preparation
22 scenarios in section 5.7.1.1, then resends the MOB_BSHO-RSP (if MS initiated handover) or MOB_BSHO-REQ (if
23 network initiated handover) message containing the new target BS offered to the MS for handover. This scenario is
24 described in section 5.7.1.2.x

25 **4.7.2.2.1 R4 Message Definitions for HO Action Phase**

26 This section describes the R4 message definitions for the HO Action Phase

27 **Table 4-70 – HO_Cnf**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
HO Confirm Type	5.3.2.76	M	
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Authenticator ID	5.3.2.19	O	MAY be included if it is not sent during the HO Preparation phase.
>Anchor ASN GW ID	5.3.2.10	O	MAY be included if it is not sent during the HO Preparation phase.
>SBC Context	5.3.2.174	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>PKM Context	5.3.2.131	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.

IE	Reference	M/O	Notes
>REG Context	5.3.2.144	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>AK Context	5.3.2.6	O	MAY be included if the Serving ASN retrieves the AK Context for the Target ASN from the Authenticator ASN. If not included the Target ASN SHALL retrieve AK context.
>SA Descriptor	5.3.2.170	O	MAY be included if the Serving ASN retrieves the information for the Target ASN from the Authenticator ASN. If not included the Target ASN SHALL retrieve the information
>SF Info (one or more)	5.3.2.185	O	It is included if TEK or Data Integrity information needs to be delivered.
>>SFID	5.3.2.184	M	
>>Direction	5.3.2.59	M	Specifies the direction of the flow; 0=DL, 1=UL
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule (one or more)	5.3.2.114	O	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classifier Rule Priority	5.3.2.32	M	
>>>Classifiers	5.3.2.30	M	
>>QoS Info	5.x.x	M	
>>>QoS Parameters	5.3.2.141	M	
>>SA Descriptor	5.3.2.170	O	It is included in case of TEK Sharing.
>>Data Integrity Info	5.3.2.41	O	TBD
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Serving
>BS ID	5.3.2.26	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.26	M	
>HO ID	Defined in [2]	O	MAY be included as optional reference if the Target ASN has previously sent it with *HO_Rsp*.

1   The content of the *Context_Req* from Target ASN to Serving ASN appears in Table 4-71.

1 **Table 4-71 – Context_Req from Target ASN to Serving ASN**

IE	Reference	M/O	Notes
Context Purpose Identifier	5.3.2.36	M	Set to MAC Context Retrieval
MS Info	5.3.2.103	M	
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Serving
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

2 The content of the *Context_Rpt* from the Serving ASN to the Target ASN appears in Table 4-72

3 **Table 4-72 – Context_Rpt from Serving ASN to Target ASN**

IE	Reference	M/O	Notes
Context Purpose Identifier	5.3.2.37	M	Set to MAC Context Retrieval
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Service Authorization Code	5.3.2.181	O	
>AK Context	5.3.2.6	O	
Failure Indication	5.3.2.69	O	Provide failure indication for this message
>Anchor ASN GW ID	5.3.2.10	O	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. Included if the originator of *HO_Req* does not host the Anchor DP Function for the MS.
>Authenticator ID	5.3.2.19	O	Identifies the node that hosts Authenticator and Key Distributor Function. Inlcuded if the originator of the *HO_Req* does not host the Authenticator and Key Distributor Function for the MS.
>SBC Context	5.3.2.174	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>PKM Context	5.3.2.131	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>REG Context	5.3.2.144	O	The TLV is included if the corresponding Capabilities are different from the pre-configured default.
>SF Info (one or more)	5.3.2.185	O	It is included if TEK or Data Integrity information needs to be delivered.

IE	Reference	M/O	Notes
>>SFID	5.3.2.184	M	
>> Direction	5.3.2.59	M	Specifies the direction of the flow; 0=DL, 1=UL
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule (one or more)	5.3.2.114	O	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classifier Rule Priority	5.3.2.32	M	
>>>Classifiers	5.3.2.30	M	
>>QoS Info	5.x.x	M	
>>>QoS Parameters	5.3.2.141	M	
>>SA Descriptor	5.3.2.170	O	It is included in case of TEK Sharing.
>>Data Integrity Info	5.3.2.41	O	TBD
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

1 The content of *Path_Reg_Req* is shown in Table 4-73. If Pre-Registration took place prior to Registration, none of
2 the optional TLVs specified below needs to be included in the message.

3 **Table 4-73 – Path_Reg_Req**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Anchor ASN GW ID	5.3.2.10	O	MAY be omitted if the IP Destination is Anchor ASN GW. Otherwise, it SHALL be included.
>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per MS. The TLV SHALL be included either as a sub-TLV of MS Info or as a sub-TLV of SF Info, but never both.
>Tunnel Endpoint	5.3.2.194	O	Included if the tunnel endpoint IP Address is different from the message sender's IP Address
>SF Info (one or more)	5.3.2.185	O	It SHALL be included if the R4 Tunneling granularity is per SF.

IE	Reference	M/O	Notes
>>SFID	5.3.2.184	M	
>>CID	5.3.2.29	O	It SHALL be included if the Anchor ASN allocates CID.
>>Data Path Info	5.3.2.45	M	It SHALL be included if the R4 Tunneling granularity is per SF. The TLV SHALL be included either as a sub-TLV of MS Info or as a sub-TLV of SF Info, but never both.
BS Info (Target)	5.3.2.26	M	MAY be included to provide optional reference to the Target BS
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

1 The content of *Path_Reg_Rsp* is shown in Table 4-74. If Pre-Registration took place prior to Registration, none of
2 the optional TLVs specified below needs to be included in the message.

3 **Table 4-74 – Path_Reg_Rsp**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
MS Info	5.3.2.103	M	
>MSID	5.3.2.102	O	
>Anchor ASN GW ID	5.3.2.10	O	MAY be omitted if the IP Source is Anchor ASN GW. Otherwise, it SHALL be included.
>Data Path Info	5.3.2.45	O	It SHALL be included if the R4 Tunneling granularity is per MS. The TLV SHALL be included either as a sub-TLV of MS Info or as a sub-TLV of SF Info, but never both.
>Tunnel Endpoint	5.3.2.194	O	Included if the tunnel endpoint IP Address is different from the message sender's IP Address
>SF Info (one or more)	5.3.2.185	O	It SHALL be included if the R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>Data Path Info	5.3.2.45	M	It SHALL be included if the R4 Tunneling granularity is per SF. The TLV SHALL be included either as a sub-TLV of MS Info or as a sub-TLV of SF Info, but never both.
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target

IE	Reference	M/O	Notes
>BS ID	5.3.2.25	M	

1   The content of *Path_Reg_Ack* is shown in Table 4-75.

2   **Table 4-75 – Path_Reg_Ack**

IE	Reference	M/O	Notes

3

4   The content of the *CMAC_Key_Count_Update* appears in Table 4-76

5   **Table 4-76 – CMAC_Key_Count_Update**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
> CMAC_KEY_COUNT	5.3.2.33	M	Delivers the CMACv2 Counter to the Authenticator
>Authenticator ASN GW ID	5.x.x	M	
BS Info	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

6   The content of CMAC_Key_Count_Ack is shown in Table 4-77.

7   **Table 4-77 – CMAC_Key_Count_Ack**

IE	Reference	M/O	Notes
>Authenticator ASN GW ID	5.3.2.19	M	Authenticator ID for the MS.
BS Info	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.181	M	Set to Target
>BS ID	5.3.2.25	M	

8

9   The content of the HO Complete from selected Target ASN to Serving ASN appears in Table 4-78

10   **Table 4-78– HO Complete**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Result of the HO
BS Info (Target)	5.3.2.26	M	

IE	Reference	M/O	Notes
> Serving/Target Indicator	5.3.2.181	M	Set to Target
> BS ID	5.3.2.25	O	BS ID of the target where MS attempted to reenter in network
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	M	6 octet MSID (MAC Address)
>SDU Info (one or more)	5.3.2.176	O	Each element in the list contains context of an SDU affected by the Data Integrity Operations. For Type-1 Data Path.
>>SDU SN	5.3.2.178	O	Last transmitted SDU sequence number

1

4.7.2.2.2 Handover Action Scenario 1: Serving ASN Sends R4 HO_Cnf to Target ASN

The following call flow describes a successful handover action scenario where the Target ASN receives the R4 *HO_Cnf* message from the Serving ASN, and received the Data Path Establishment Option TLV in the R4 *HO_Req* message.
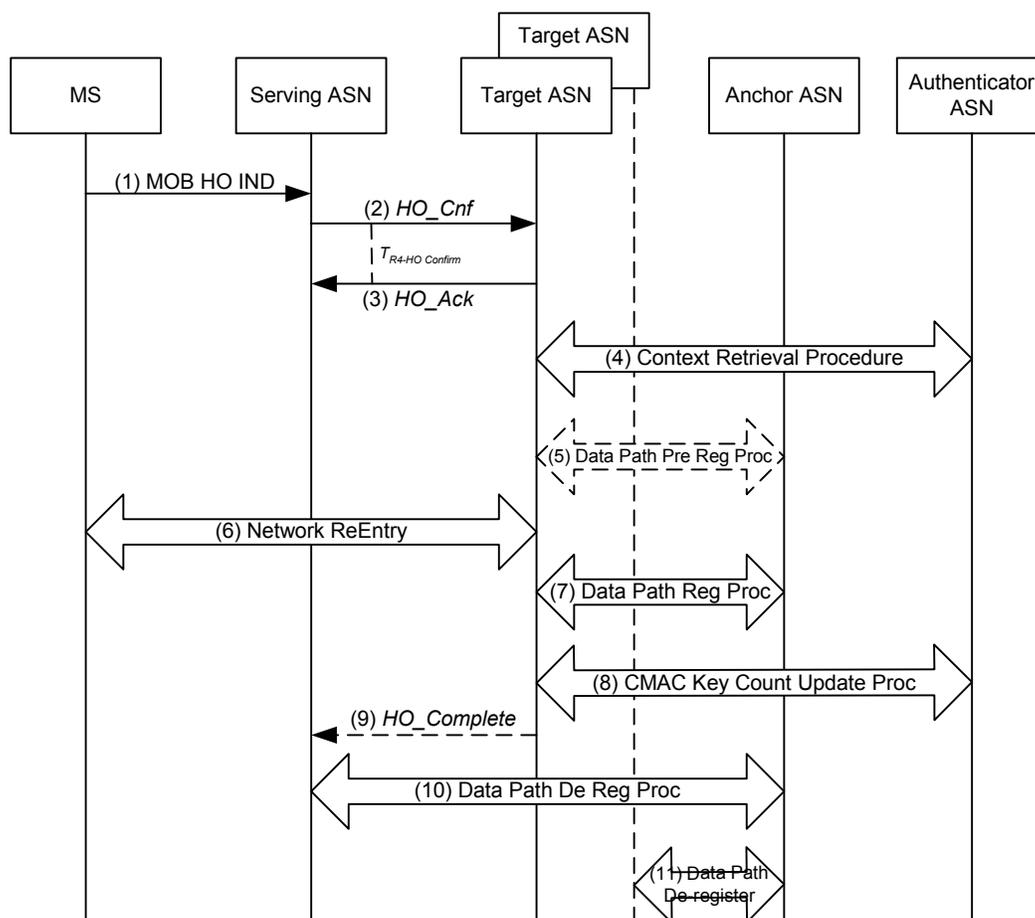
Figure 4-48 – Successful HO Action Phase, Scenario 1

1 **STEP 1**

2 The MS sends a MOB_HO-IND to the Serving ASN to notify a handover to one of the target BSs selected by the
3 Serving ASN in the Handover Preparation phase.

4 **STEP 2**

5 Upon reception of the MOB_HO-IND the Serving ASN sends an R4 *HO_Cnf* message to the Target ASN and starts
6 timer T$_{R4\_HO\_Conf}$.

7 **STEP 3**

8 The Target ASN sends an R4 *HO_Ack* message to the Serving ASN. Upon receipt of the R4 *HO_Ack* message, the
9 Serving ASN stops timer T$_{R4\_HO\_Conf}$.

10 **STEP 4**

11 If an Authenticator ID TLV was included in the R4 *HO_Req* or R4 *HO_Cnf* message and AK context for the MS
12 was not requested during the Handover Preparation phase, the Target ASN requests AK context for the MS by
13 initiating a Context Request procedure (see section 4.13) with the Authenticator ASN.

14 **STEP 5**

15 If the Anchor ASN GW ID TLV was included in the R4 *HO_Req* or R4 *HO_Cnf* message and Data Path Pre-
16 Registration procedure (see section 4.13) did not occur, the Data Path Pre-Registration procedure may optionally
17 take place at this moment.

18 **STEP 6**

19 The MS initiates network re-entry with the Target ASN.

20 **STEP 7**

21 Target ASN initiates Data Path Registration procedure (see section 4.13) with the Anchor ASN. Note: This
22 procedure SHALL be a two-way handshake if data path was pre-established.

23 **STEP 8**

24 Upon successful completion of network re-entry, Target ASN initiates CMAC Key Count Update procedure (see
25 section 4.13) and updates the Authenticator (located at the Authenticator ASN's GW) with the latest CMAC Key
26 Count value received from MS.

27 **STEP 9**

28 Upon completion of network re-entry, the Target ASN may send an R4 *HO_Complete* message to the Serving ASN
29 to notify the completion of the handover. Upon receipt of the R4 *HO_Complete* message, the Serving ASN releases
30 the MS context.

31 **STEP 10**

32 Upon completing the Data Path Registration procedure with the Target ASN, the Anchor ASN initiates Data Path
33 De-Registration procedure (see section 4.13) with the old Serving ASN.

34 **STEP 11**

35 The Anchor ASN SHALL de-register all the pre-registered data paths with the unselected Target ASNs.

36 **4.7.2.2.3 Handover Action Scenario 2: R4 HO_Cnf not Received at Target ASN**

37 The following call flow describes a successful Handover Action scenario where the MOB_HO-IND sent by the MS
38 to the Serving ASN was lost over the air and not received by the Serving ASN, and/or the R4 *HO_Cnf* message sent

1 by the Serving ASN to the Target ASN was either delayed or not received. The MS completes network re-entry at
2 one of the Target BSs selected by the Serving ASN during the Handover Preparation phase
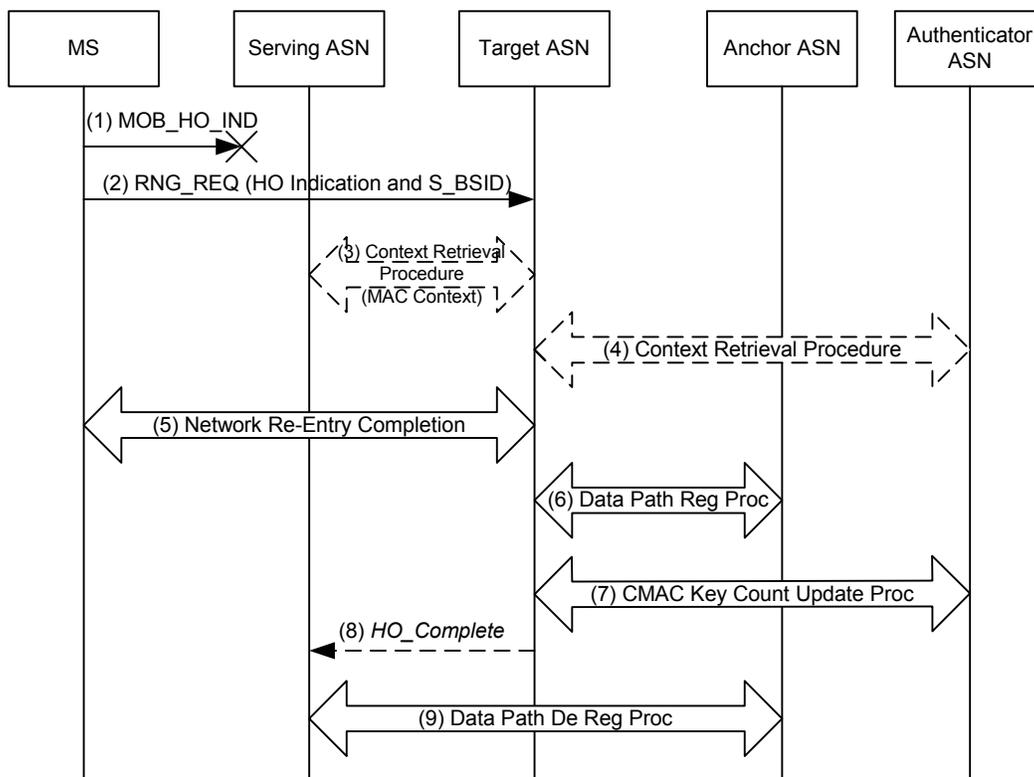
3

4 **Figure 4-49 – Successful HO Action Phase, Scenario 2**

5 **STEP 1**

6 The MOB_HO-IND message is sent by the MS to the serving ASN and lost over the air or not properly received by
7 the Serving ASN.

8 **STEP 2**

9 The MS sends Ranging Request message with HO_Indication and the serving BS ID information to one of the
10 Target BSs that was indicated by the Serving ASN during the Handover Preparation phase. If the Serving BS ID was
11 not included, an initial network entry is required and initial network entry procedures SHALL be followed.

12 **STEP 3**

13 The Target ASN initiates a Context Request procedure (see section 4.13) with the Serving ASN to retrieve the latest
14 MAC context for the MS. This step might have been executed in the preparation stage and shown as optional in the
15 Action phase.

16 **STEP 4**

17 If an Authenticator ID TLV for the Authenticator ASN was received in the R4 *HO_Req* or R4 *HO_Context_Req*
18 message but AK context was not obtained during the Handover Preparation phase, the Target ASN requests AK
19 context for the MS by initiating a Context Request procedure (see section 4.13) with the Authenticator ASN.

STEP 5

After completing the retrieval of the MS context, the Target ASN sends Ranging Response to the MS. The MS and Target_ASN complete the network Re-entry including the exchange of the required parameters (i.e. SBC-Req/Rsp).

STEP 6

The Target ASN initiates a data path registration procedure (see section 4.13) with the Anchor ASN. This step can be executed any time after the Context Request procedure in step 2.

STEP 7

Upon successful completion of network re-entry, the Target ASN initiates CMAC Key Count Update procedure (see section 4.13) and updates Authenticator in the Authenticator ASN with the latest CMAC Key Count value which is received from MS.

STEP 8

Upon completion of network re-entry, the Target ASN may send an R4 *HO_Complete* message to the Serving ASN to notify the completion of the handover. Upon receipt of the R4 *HO_Complete* message, the Serving ASN releases MS context.

STEP 9

Upon completing Data Path Registration procedure with the Target ASN, Anchor ASN initiates Data Path De-Registration procedure (see section 4.13) with the old Serving ASN. Also if pre-established, the Anchor ASN SHALL de-register all the pre-registered data paths with the Target ASNs that were not selected (not shown in the figure).

4.7.2.2.4 Handover Action Scenario 3: MOB_HO-IND not Received at Serving ASN

The following call flow describes a successful Handover Action scenario where the MOB_HO-IND sent by the MS to the Serving ASN was lost over the air and not received by the Serving ASN. The MS completes network re-entry at one of the target BSs selected by the Serving ASN during the Handover Action phase, or a target BS controlled by a target ASN which wasn't notified of a an impending handover from the MS during the handover preparation but was notified later upon detection of the lost MOB_HO-IND message from the mobile.

1
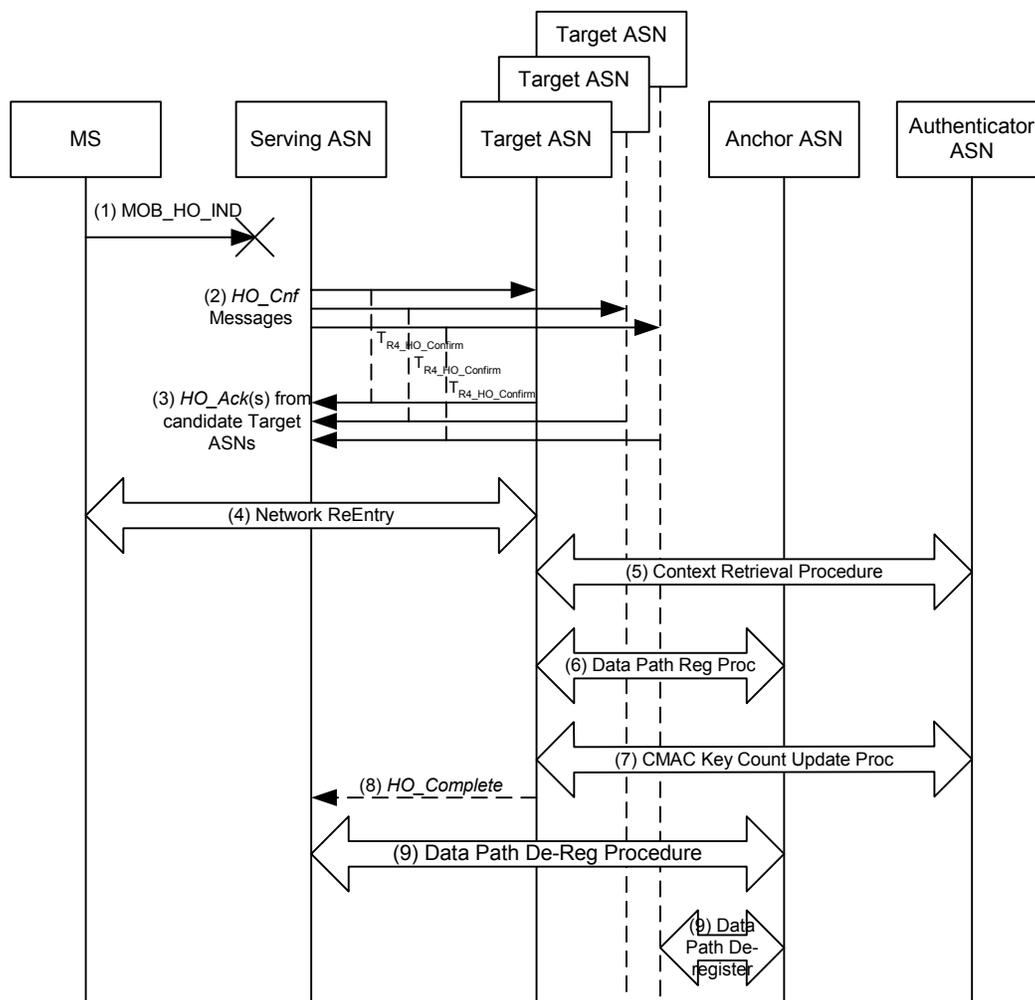
2 **Figure 4-50 – Successful HO Action Phase, Scenario 3**

3 **STEP 1**

4 The MOB_HO-IND sent by the MS to the Serving ASN is lost over the air and not received by the Serving ASN.

5 **STEP 2**

6 Upon expiration of internal timer at the Serving BS, the Serving ASN sends an R4 *HO_Cnf* message(s) with
7 "Unconfirmed" type to the set of Target ASN(s) controlling the candidate Target BS(s) which were indicated in the
8 MOB_BSHO-RSP or MOB_BSHO-REQ and starts the $T_{R4\_HO\_Conf}$ timer. The Serving ASN also sends R4 *HO_Cnf*
9 message to any candidate target ASNs controlling target BSs the MS may select to handover to which weren't
10 previously notified of a potential handover from the MS during the handover preparation. The R4 *HO_Cnf* message
11 contains the HO_Indication Type set to "Unconfirmed", Authenticator GW ID or AK context, Anchor GW ID, and
12 latest MAC context information.

13 **STEP 3**

14 Each Target ASN sends R4 *HO_Ack* message to the serving ASN. Upon receipt of the R4 *HO_Ack* message, the
15 Serving ASN stops the corresponding $T_{R4\_HO\_Conf}$ timer.

1 **STEP 4**

2 The MS completes network re-entry at one of the target BSs selected by the Serving ASN during the Handover
3 Action phase, or at a target BS controlled by a target ASN notified of an impending handover from the MS after the
4 serving BS detects the loss of communication with the MS due to loss of the MOB_HO-IND message..

5 **STEP 5**

6 If the Authenticator ID was included in the R4 *HO_Req* or R4 *HO_Cnf* message and AK context was not obtained
7 during the Handover Preparation phase, the Target ASN requests AK context for the MS by initiating a Context
8 Request procedure (see section 4.13) with the Authenticator ASN.

9 **STEP 6**

10 If the Anchor ASN GW ID TLV was included in the R4 *HO_Req* or R4 *HO_Cnf* message received during the
11 Handover Preparation phase and data path pre-registration did not occur, the Target ASN initiates a Data Path
12 Registration procedure (see section 4.13) with the Anchor ASN. This step can be executed any time after receiving
13 R4 *HO_Cnf* message.

14 **STEP 7**

15 Target ASN initiates CMAC Key Count Update procedure (see section 4.13) and updates Authenticator in the
16 Authenticator ASN with the latest CMAC Key Count value which is received from MS

17 **STEP 8**

18 The Target ASN may send an R4 *HO_Complete* message to the Serving ASN to expedite release of MS context
19 information. Upon receipt of the R4 *HO_Complete* message, the Serving ASN releases the MS context and stops the
20 Resource Retain Timer.

21 **STEP 9**

22 If the data path is still maintained, upon completing Data Path Registration procedure (see section 4.13) with the
23 Target ASN, the Anchor ASN SHALL initiate Data Path De-Registration procedure with the old Serving ASN. Also
24 if pre-established during HO preparation stage, the Anchor ASN SHALL de-register all the pre-registered data paths
25 with the other (not selected) Target ASNs.

26 **4.7.2.2.5 Handover Action Scenario 4: Anchor ASN and Anchor Authenticator Collocated with**
27 **Serving ASN – Serving ASN Initiates Path Registration**

28 The following call flow describes a successful handover action scenario where the Anchor ASN is collocated with
29 the Serving ASN and the Serving/Anchor ASN initiates Data Path Registration procedure with the Target ASN
30 during the Handover Action phase. The Target ASN receives the R4 *HO_Cnf* message from the Serving ASN and
31 did not receive the Data Path Establishment Option TLV in the R4 *HO_Req* message.

1
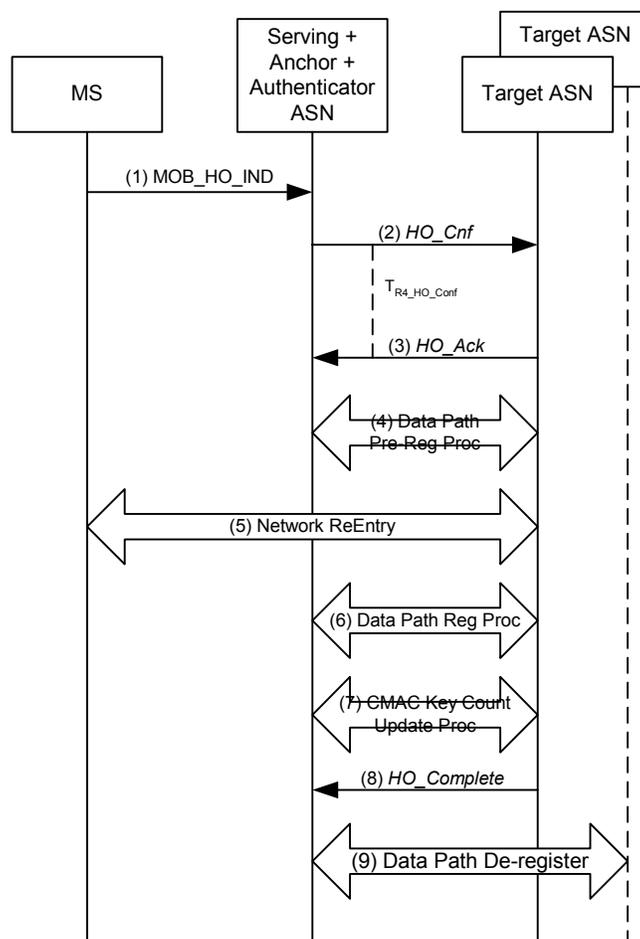
2 **Figure 4-51 – Successful HO Action Phase, Scenario 4**

3 **STEP 1**

4 The MS sends a MOB_HO-IND to the Serving ASN to notify a handover to one of the Target BSs candidates
5 selected by the Serving ASN during the Handover Preparation phase.

6 **STEP 2**

7 The Serving ASN sends an R4 *HO_Cnf* message to the Target ASN and starts timer $T_{R4\_HO\_Conf}$.

8 **STEP 3**

9 The Target ASN sends an R4 *HO_Ack* message to the Serving ASN. Upon receipt of the R4 *HO_Ack* message, the
10 Serving ASN stops timer $T_{R4\_HO\_Conf}$.

11 **STEP 4**

12 The Serving ASN may initiate a Data Path Pre-Registration procedure (see section 4.13) with the Target ASN if
13 Data Path Pre-Registration did not occur. If the Target ASN doesn't support Serving/Anchor ASN initiated Data
14 Path Pre-Registration procedure, it may initiate the procedure on its own.

15 **STEP 5**

16 The MS initiates network re-entry with the Target ASN.

STEP 6

If not already established, the Target ASN initiates a Data Path Registration procedure (see section 4.13) with the Anchor ASN. This step can be executed any time after receiving R4 *HO_Cnf* message.

STEP 7

Upon successful completion of network re-entry, the Target ASN initiates CMAC Key Count Update procedure (see section 4.13) and updates the Authenticator with the latest CMAC Key Count value which is received from MS.

STEP 8

Upon completion of network entry, the target ASN may send an R4 *HO_Complete* message to the serving ASN to acknowledge the completion of the handover. Upon receipt of the R4 *HO_Complete* message, the Serving ASN releases the MS context.

STEP 9

If pre established during HO preparation stage, the Serving/Anchor ASN SHALL de-register all the pre-registered data paths with the other not selected Target ASNs candidates.

4.7.2.3   HO Cancellation

HO Cancellation is a variant of HO Action Phase, when the Serving BS signals to one or more Target BSs that the HO is to be cancelled.   The HO Cancellation will be invoked only if the Target BS has completed the HO Preparation procedures.   Thus HO Cancellation, if invoked, happens instead of the Network Re-Entry Phase.   HO Cancel will be sent to the Target BSs that have not been chosen as the final HO Target by the MS or to all the Target BSs when the MS has decided to cancel the HO procedure completely.

Note: The reference of "Unselected Target ASN" below figures for various HO Cancellation scenarios is referred to the Target ASN that was previously selected as the potential target ASN that MS may handover to, and some system resource may have been pre-allocated at the target ASN including the data path resources towards the anchor ASN.

4.7.2.3.1 HO Cancellation Scenario 1: Serving and Anchor ASN are Colocated and "Unselected Target ASN" Receives R4 HO_Cnf from Serving ASN
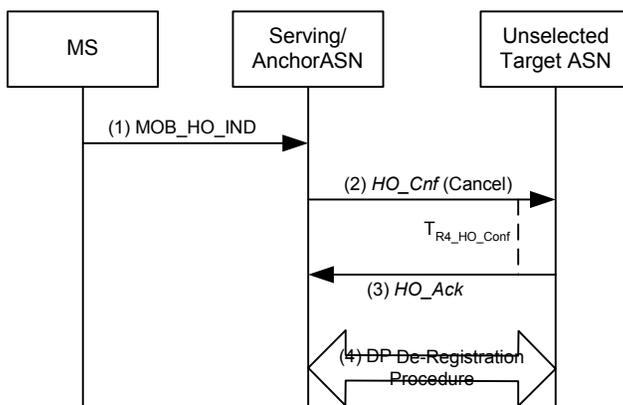
Figure 4-52 – R4 HO Cancellation, Scenario 1

STEP 1

The MS sends MOB_HO_IND to the Serving BS. In the MOB_HO_IND, the MS indicates the Serving BS with two possibilities:

- The selected target BS that the MS chooses to perform the handover, or

- The MS decides to cancel the handover procedures, in this case, the selected target BS is the Serving BS

STEP 2

Receiving the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel causes the Serving BS to send R4
HO_Cnf message with the value of the HO_Indication type set to "Cancel" to inform the previously selected
potential Target BS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP message to de-allocate
the reserved system resources that are prepared for the MS to handover.   After sending the message, the Serving BS
awaits for the *HO_Ack* message by starting the $T_{HO\_Acknowledge\_Timer}$. If the timer expires, the Serving BS may re-send
the R4 *HO_Cnf.* After a pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf.*
The Target BS shall perform the local clean up if R4 *HO_Cnf* is never received from the Serving BS.

STEP 3

If the Target BS receives the R4 *HO_Cnf* with HO_Indication type set to "Cancel", the Target BS sends R4 *HO_Ack*
to the Serving BS and release the pre-allocated system resources, which are to support the MS handover. The Target
BS may also initiate the DP release process towards the Anchor ASN if DP has been pre-established.

STEP 4

Upon expiry of the MS Context Retain Timer, the Serving BS may send the R4 *Path_Dereg_Req* to the Target ASN
if R4 Path Pre-Registration or R4 Path Regisration has been received by the Target ASN during the HO Preparation
phase, and the Serving BS sets the timer $T_{Registration\_Acknowledge\_Timer}$ to wait for the response from the Target ASN. If
the R4 *Path_Reg_Rsp* is not received by the Serving BS before the expiry of the $T_{Registration\_Acknowledge\_Timer}$, the
Serving BS may re-transmit the message until the maximum number of retransmissions. If the MS is no longer
attached to the Serving MS, the Serving MS shall release all the allocated system resource for the MS.

**4.7.2.3.2 HO Cancellation Scenario 2: Serving and Anchor ASN are not Colocated and
        "Unselected Target ASN" receives R4 HO_Cnf from Serving ASN**
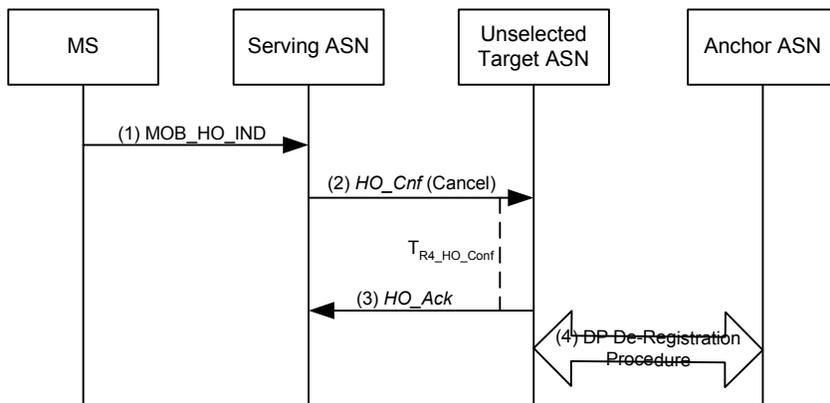
Figure 4-53 – R4 HO Cancellation, Scenario 2

STEP 1

The MS sends MOB_HO-IND to the Serving BS. In the MOB_HO-IND, the MS indicates the Serving BS with two
possibilities:

- The selected target BS that the MS chooses to perform the handover, or

- The MS decides to cancel the handover procedures, in this case, the selected target BS is the Serving BS

STEP 2

Receiving the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel causes the Serving BS to send R4
HO_Cnf message with the value of HO_Indication type set to "Cancel" to inform the previously selected potential
Target BS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP message to de-allocate the
reserved system resources that are prepared for the MS to handover. After sending the message, the Serving BS

1 awaits *HO_Ack* by starting the $T_{HO\_Acknowledge\_Timer}$. If the timer expires, the Serving BS may re-send the R4 *HO_Cnf*.
2 After a pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf*. The Target BS shall
3 perform the local clean up if R4 *HO_Cnf* is never received from the Serving BS.

4 **STEP 3**

5 Target BS receives the R4 *HO_Cnf* with HO_Indication type set to "Cancel". Target BS sends R4 *HO_Ack* to the
6 Serving BS and may release the pre-allocated system resources, which are to support the MS handover. .

7 **STEP 4**

8 The Target BS may send the R4 *Path_Dereg_Req* to the Anchor ASN if data path has already been established
9 between the Target ASN and the Anchor ASN. Serving BS sets the timer $T_{Registration\_Acknowledge\_Timer}$ to wait for the
10 response from the Target ASN. If the R4 *Path_Reg_Rsp* is not received by the Serving BS before the expiry of the
11 $T_{Registration\_Acknowledge\_Timer}$, the Serving BS may re-transmit the message until the maximum number of
12 retransmissions. . If the MS is no longer attached to the Serving MS, the Serving MS shall release all the allocated
13 system resource for the MS.

14 **4.7.2.3.3 HO Cancellation Scenario 3: Serving and Anchor ASN are not Colocated and**
15 **"Unselected Target ASN" does not Receive R4 HO_Cnf from Serving ASN**
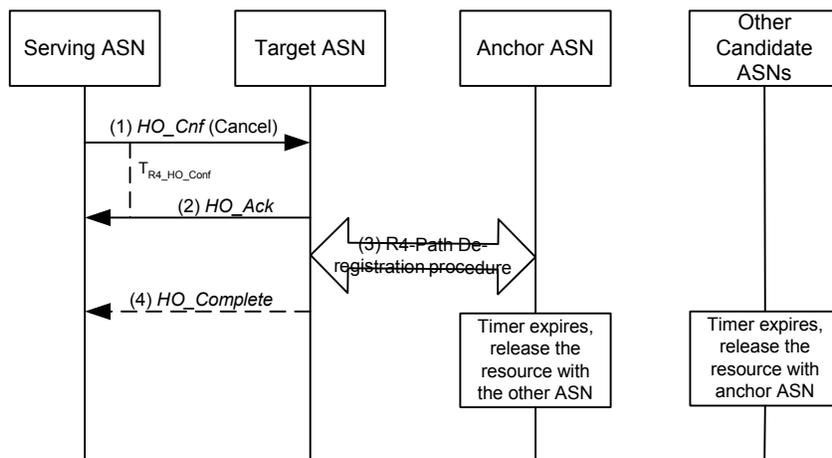
16

17 **Figure 4-54 – R4 HO Cancellation, Scenario 3**

18 **STEP 1**

19 The MS sends MOB_HO-IND to the Serving BS. In the MOB_HO-IND, the MS indicates the Serving BS with two
20 possibilities:

21 • The selected target BS that the MS chooses to perform the handover, or

22 • The MS decides to cancel the handover procedures, in this case, the selected target BS is the Serving BS

23 **STEP 2**

24 Receiving the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel causes the Serving BS to send R4
25 *HO_Cnf* message with the value of HO_Indication type set to "Cancel" to inform the previously selected potential
26 Target BS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP message to de-allocate the
27 reserved system resources that are prepared for the MS to handover.   After sending the message, the Serving BS
28 awaits *HO_Ack* by starting the $T_{HO\_Acknowledge\_Timer}$. If the timer expires, the Serving BS may re-send the R4 *HO_Cnf*.
29 After a pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf*. The Target BS shall
30 perform the local clean up if R4 *HO_Cnf* is never received from the Serving BS.

1   **STEP 3**

2   The Target BS does not receive the R4 *HO_Cnf*. Target BS releases the pre-allocated system resources which are to
3   support the MS handover.

4   **STEP 4**

5   After the timer associated with the pre-registered DP expires, the Target BS may send the R4 *Path_Dereg_Req* to
6   the Anchor ASN if data path has already been established between the Target ASN and the Anchor ASN. Serving
7   BS sets the timer $T_{Registration\_Acknowledge\_Timer}$ to wait for the response from the Target ASN. If the R4 *Path_Reg_Rsp* is
8   not received by the Serving BS before the expiry of the $T_{Registration\_Acknowledge\_Timer}$, the Serving BS may re-transmitt
9   the message until the maximum number of retransmissions. . If the MS is no longer attached to the Serving BS, the
10   Serving BS shall release all the allocated system resource for the MS.

11   **4.7.2.4   MS Handover Rejection**

12   The following call flow describes the scenario when the MS rejects target BSs offered to it by the serving BS for
13   handover.
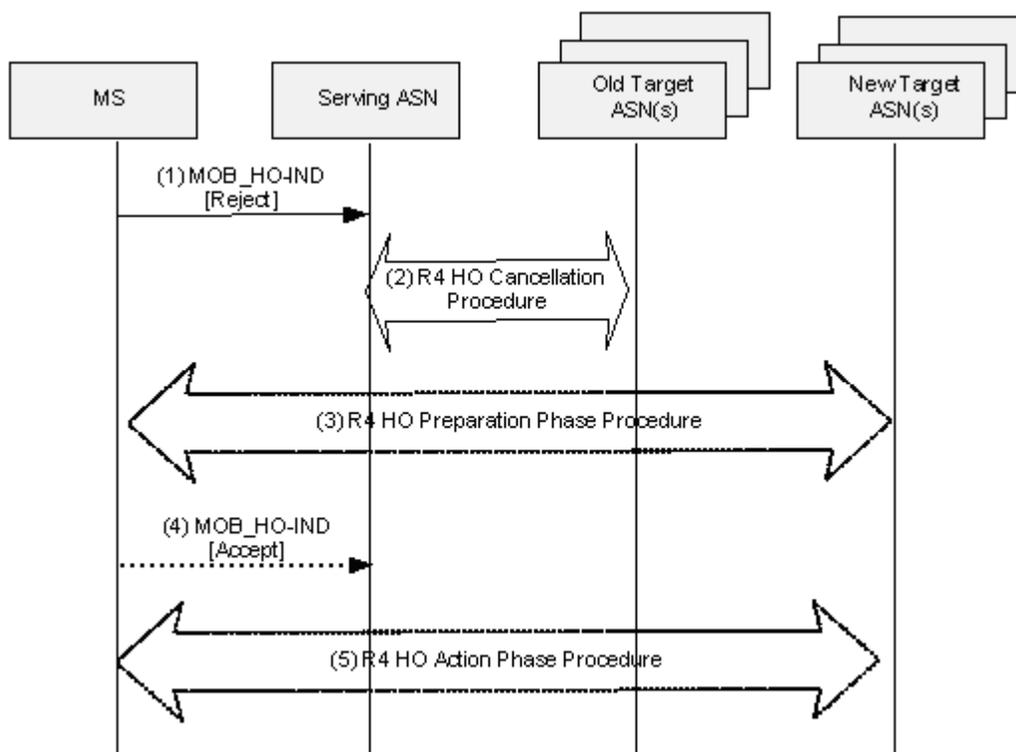
14

15   **Figure 4-55**

16   1.   The MS sends a MOB_HO-IND containing HO_IND_Type TLV set to 0b10 indicating rejection of the
17   target BS(s) offered by the serving BS for handover in the MOB_BSHO-RSP (MS initiated handover) or
18   MOB_BSHO-REQ (network initiated handover) message.

19   2.   The serving ASN initiates the handover cancellation procedures described in section 5.7.x with the target
20   ASN(s) controlling target BS(s) which were rejected for handover by the MS.

21   The following steps only occur if the serving ASN is able to offer an alternate target BS(s) to the MS.

22   3.   The serving ASN initiates the R4 handover preparation procedures with a target ASN(s) controlling a new
23   candidate target BS(s) to be offered to the MS for handover to.

1 4. The MS indicates acceptance of a new target BS offered by the serving BS to the MS for handover in the
2   MOB_BSHO-RSP or MOB_BSHO-REQ message by sending a MOB_HO-IND message with
3   HO_IND_Type TLV set to 0b00.

4 5. The Serving ASN completes the handover action procedures described in section 5.7.1.2 and the MS
5   completes successful handover to the new target BS.

6 Note: If the MS rejects the target BS offered by the serving BS as described in step 1, steps 1-2 are repeated. If the
7 serving ASN decides to offer a new target BS for handover to the MS, steps 3-5 are repeated.

8

9 4.7.2.5   HO Action Phase Timers and Timing Considerations

10 This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over
11 R4:

12 • $T_{R4\_DP\_Reg\_Req}$: is started by the Target ASN to initiate establishment or provide confirmation of the data
13   paths for an MS, upon sending the R4 *Path_Reg_Req* message, and is stopped upon receiving a
14   corresponding R4 *Path_Reg_Rsp* message.

15 • $T_{R4\_DP\_Reg\_Rsp}$: is started by the Anchor ASN upon sending the R4 *Path_Reg_Rsp* message if no data path
16   has been pre-established for the MS, and is stopped upon receiving a corresponding R4 *Path_Reg_Ack*
17   message.

18 • $T_{R4\_DP\_De\_Reg\_Req}$: is started by the Anchor ASN after completion of the Data Path Registration procedure for
19   an MS, upon sending the R4 *Path_Dereg_Req* message, and is stopped upon receiving a corresponding R4
20   *Path_Dereg_Rsp* message.

21 • $T_{R4\_CMAC\_Key\_Count\_Upd}$: is started by a Target (now new Serving) ASN after MS completes network re-entry,
22   upon sending the R4 *CMAC_Key_Count_Update* message to the Authenticator ASN, and is stopped upon
23   receiving a corresponding R4 *CMAC_Key_Count_Update_Ack* message from the Authenticator ASN.

24 • $T_{R4\_HO\_Conf}$: each such timer is started by the serving ASN when sending the R4 *HO_Cnf* message to each of
25   the candidate Target ASNs. Each timer is stopped upon receiving a R4 *HO_Ack* message from the
26   corresponding Target ASN.

27 Table 4-79 shows the default value of timers and also indicates the range of the recommended duration of these
28 timers. Note that these values are provisioned in Release 1.0.0.

29 **Table 4-79 – HO Action Phase R4 Timer Values**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R4\_Path\_Reg\_Req}$	TBD		TBD
$T_{R4\_Path\_Reg\_Resp}$	TBD		TBD
$T_{R4\-Path\_De\-Reg\_Req}$	TBD		TBD
$T_{R4\-Path\_De\-Reg\_Rsp}$	TBD		TBD
$T_{R4\_CMAC\_Key\_Count\_Upd}$	TBD		TBD
$T_{R4\_HO\_Conf}$	TBD		TBD

30 4.7.2.6   HO Action Phase Error Conditions

31 This section describes error conditions associated with the HO Action Phase.

1 **4.7.2.6.1 Timer Expiry**

2 Table 4-80 shows details on the corresponding actions associated with timer expiry. Upon each timer expiry, if the
3 maximum retries has not exceeded, the related message is retransmitted and the timer is restarted. Otherwise, the
4 corresponding action(s) should be performed as indicated in Table 7-5.

5 **Table 4-80 – Actions after MAX Re-transmit Retries**

Timer	Entity where Timer Started	Action(s)
$T_{R4\_Path\_Reg\_Req}$	Target ASN	ASN shall force MS to perform initial network entry
$T_{R4\_Path\_Reg\_Resp}$	Anchor ASN	ASN shall defer sending the downlink packets until it receives any packets for MS from Target(new Serving) ASN. ASN shall reset data paths for MS if no packets are received until a pre-specified system timer expires.
$T_{R4\_Path\_De-Reg\_Req}$	Anchor ASN	No action required
$T_{R4\_Path\_De-Reg\_Rsp}$		
$T_{R4\_CMAC\_Key\_Count\_Upd}$	Target (new Serving) ASN	ASN shall force MS to perform initial network entry
$T_{R4\_HO\_Conf}$	Serving ASN	No action required

6 **4.7.2.6.2 R4 Path_Reg_Rsp Error**

7 Upon receipt of the R4 *Path_Reg_Req* message, if the Anchor ASN is unable to support the requested establishment
8 of the data path(s), then it SHALL send a R4 *Path_Reg_Rsp* message with suitable error code.

9 Upon receipt of the R4 *Path_Reg_Rsp* message with suitable error code, the Target (new serving) ASN SHALL stop
10 $T_{R4\text{-}DP\_Reg\text{-}Req}$ (if running). The Target ASN MAY re-send the R4 *Path_Reg_Req* message. If the Target ASN does
11 not resend the R4 *Path_Reg_Req* message or if subsequent attempts are also unsuccessful, the Target ASN SHALL
12 force the MS to perform a full network re-entry.

13 **4.7.2.6.3 R4 HO_Cnf Error**

14 If the timer expires, the Serving BS may re-send the R4 *HO_Cnf*. After a pre-defined number of retransmissions, the
15 Serving BS stops resending the R4 *HO_Cnf*. The Target BS SHALL perform the local clean up if R4 *HO_Cnf* is
16 never received from the Serving BS.

17 **4.7.3 Uncontrolled (Unpredictive) HO with Context Retrieval**

18 An Uncontrolled (Unpredictive) handover occurs when an MS starts ranging at a Target ASN that wasn't previously
19 notified of an impending handover from an MS and didn't participate in the Handover Preparation Phase. This may
20 occur due to suboptimal radio planning conditions or MS implementation (handover notification to the network by
21 the BS is optional).

22 If an MS starts ranging with an ASN that doesn't have MS Context information including Authenticator and Anchor
23 Data Path ASN identifiers, the RNG-REQ message from the MS cannot be authenticated. In a worst case scenario
24 an initial Network Re-Entry will be required which results in large delays, because some authentication methods
25 may take seconds to complete, especially if the Home AAA Server is located far away and the communication is
26 slow.

27 However if the MS includes the Serving BS ID TLV in the RNG-REQ message, the handover can still be completed
28 and the period of traffic unavailability can be greatly reduced. When an MS re-enters at a Target BS and supplies its
29 Serving BS ID in the RNG-REQ message, the Target ASN may retrieve the relevant MS Context from the Serving
30 ASN including the Authenticator ASN ID and Anchor DP ASN ID. Thus it becomes possible to retrieve the
31 Authenticator Context for the MS to authenticate the RNG-REQ and perform data path registration with the Anchor
32 DP ASN. This call flow scenario is described in Figure 4-56.

1   If the Anchor ASN GW ID is not included in the R4 *Context_Rpt*, the Serving ASN hosts the Anchor data path
2   function for the MS and data path registration occurs with the Serving ASN. The content of the messages are
3   described in sections 4.7.2.1.1 and 4.7.2.2.1. If the serving ASN is co-located with the Authenticator ASN, the
4   serving ASN provides AK context information to the target ASN in the R4 *Context_Rpt*.

5   Network Re-Entry might be completed immediately after receiving the MS Context or after data path establishment
6   (the latter case is shown in the call flows)[9]. The moment of Network Re-Entry completion does not affect
7   interoperability and is left as a vendor implementation option.

---

[9] The former method requires a lower Ranging Response Timeout in the MS, however it also requires holding the uplink traffic
until the data path is established. The latter method doesn't require traffic holding but relies on larger Ranging Response Timeout
in the MS.

1   **4.7.3.1   Successful Uncontrolled Handover**

2   The following call flow provides an example of a successful uncontrolled handover scenario. A MS begins ranging
3   at Target ASN that wasn't contacted by the Serving ASN to participate in the Handover Preparation phase.
4   Therefore the Target ASN was an unaware of an impending hand-in from the MS. The MS includes the Serving BS
5   ID in the RNG-REQ message. The Target ASN retrieves the MS context and authenticator information and
6   successfully completes the handover.
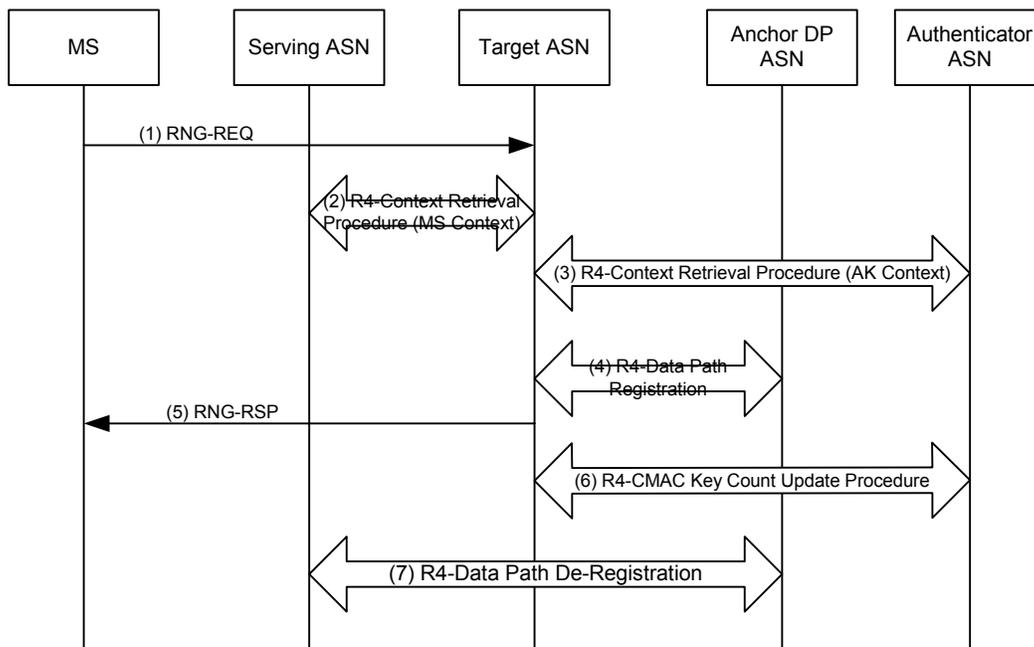
7

8   **Figure 4-56 – Uncontrolled (Unpredictive) HO**

9   **STEP 1**

10   An MS performs an uncontrolled handover by sending a RNG-REQ message to perform contention based ranging at
11   a Target ASN that didn't receive prior notification of an impending handover from the MS and therefore didn't
12   participate in the Handover Action phase. The MS includes the Serving BSID TLV in the RNG-REQ message.

13   **STEP 2**

14   The Target ASN initiates a Context Request procedure with the Serving ASN to retrieve context information for the
15   MS. See section 4.13 for this procedure. The Serving ASN responds by sending the context information which
16   includes the Authenticator ASN ID and Anchor ASN ID. If the Authenticator ASN ID and/or Anchor ASN ID was
17   not sent, the Serving ASN hosts the respective functions.

18   **STEP 3**

19   The Target ASN requests AK context for the MS by initiating a Context Request procedure with the Authenticator
20   ASN. See section 4.13 for this procedure. If no authenticator ID was received (Serving ASN is co-located with the
21   Authenticator ASN), the Target ASN initiates a Context Request procedure with the Serving ASN.

22   **STEP 4**

23   The Target ASN initiates data path registration for the MS with the Anchor Data Path ASN. See section 4.13 for this
24   procedure. If the Anchor DP ASN ID was not sent to it as part of the MS context from the Serving ASN, the Serving
25   ASN hosts the data path function and the Target ASN initiates Data Path Registration procedure (see section 4.13)
26   for the MS with the Serving ASN.

1 **STEP 5**

2 Target ASN uses the Authenticator context to authenticate the MS message. The Target ASN sends a RNG-RSP
3 message to the MS acknowledging the HMAC/CMAC tuple (expedited security authentication) and containing the
4 *HO Process Optimization TLV*.

5 **STEP 6**

6 The Target ASN initiates a CMAC Key Count Update procedure with the Authenticator ASN to update it with the
7 latest CMAC Key Count. See section 4.13 for this procedure.

8 **STEP 7**

9 The Anchor DP ASN initiates an R4 Data Path De-Registration procedure with the Serving ASN. See section 4.13
10 for this procedure. Note: This step may occur any time after step '4'.

11 ## 4.8   CSN Anchored Mobility Management

12 ### 4.8.1   Introduction

13 This section describes the CSN Anchored Mobility Management procedures. The term "mobility" means CSN
14 anchored mobility within the context of this section. The procedures described here are categorized into network
15 access based on IPv4 and IPv6.

16 The IPv4 network access and mobility management is either performed with Proxy Mobile IPv4 (PMIP4) or Client
17 Mobile IPv4 (CMIP4). The IPv6 network access and mobility management is performed with Client Mobile IPv6
18 (CMIP6) using authentication protocol ([21]).

19 A NAP operator may assign addresses from private address space range to the functional entities in its access
20 network. The CSN operator may choose to assign addresses from the same private address space to the MSs. Since
21 CSN and ASN are independent administrative domains and are not synchronizing their usage of private address
22 space, it may happen that the same address that the CSN assigned to a particular MS is also assigned to the ASN
23 GW to which this MS is attached. Some ASN entities, like DHCP Proxy, are originating IP datagrams destined to
24 MSs. If the ASN entity originating a datagram destined for the MS and the MS are assigned the same private
25 address, then the datagram will have the same IP address in both the destination and source address field in the IP
26 header. This should clearly not be allowed to happen.

27 In order to prevent this problem, the entities in the NAP's network that originate datagrams towards the MS SHALL
28 be configured with the public IP address. This will prevent the problem of the address collision. Entities affected by
29 this requirement include the DHCP Proxy and the entity acting as a default router for the MS (which originates
30 Router Advertisements). Those entities may have additional private addresses assigned but they SHALL use their
31 public IP address as a source IP address when originating datagrams towards a MS.

32 Simultaneous PMIP4 and CMIP4 operation by the same mobile is not supported in this specification.

33 ### 4.8.2   Proxy MIPv4 R3 Mobility Management

34 The proxy Mobile IPv4 procedure is entirely done in the network and the MS is agnostic to the related procedures.
35 There are certain events that take place with the MS e.g. MS requesting an IP address assignment at the connection
36 setup time or the MS performing an handover across BS boundaries that require relocation of the network layer
37 anchor point (e.g. change of CoA) that MAY serve as a trigger for Proxy Mobile IPv4 transactions in the network.

38 #### 4.8.2.1   Proxy MIPv4 Connection Setup Procedure

39 The basic connection setup procedure using PMIP4 is shown in Stage 2, section 7.8.1.8.3. The node requirements to
40 support the connection setup are described as follows.

41 During the initial network entry, PMIP4 Client, DHCP proxy or relay function, Authenticator and FA are all
42 collocated.

1 **4.8.2.1.1 MS Requirements**

2 The MS SHALL support the DHCP client function as defined in [22]. In order to acquire an IPv4 address, the MS
3 SHALL send a DHCPDISCOVER message to the network over the initial service flow. Upon receiving the
4 DHCPOFFER message from the network, the MS SHALL follow the procedures defined in [22] to select and
5 configure an IPv4 address included in the DHCPOFFER message.

6 The MS SHALL also, refresh the DHCP Lease Time based on the T_1 and T_2 parameters received in the Op Codes 58
7 and 59 in [25].

8 **4.8.2.1.2 DHCP Requirements**

9 There are two DHCP deployments for CSN anchored mobility:

10 • DHCP proxy is in the ASN (in the ASN-GW in profile A and C).

11 • DHCP relay in the ASN.

12 **4.8.2.1.2.1 DHCP Proxy Requirements**

13 Upon receiving a DHCPDISCOVER message from the MS, the DHCP proxy MAY ignore the "chaddr" field in the
14 DHCP header and use the pseudo NAI associated with the ISF data path tunnel(i.e., R6 for profile A and C) over
15 which the DHCP message was received as the identity of the MS to acquire a HoA. This is feasible without any
16 additional Option in the DHCP message since the DHCP proxy is collocated with the Anchor ASN. This is done to
17 prevent MAC address spoofing by a rogue MS.

18 The DHCP proxy prompts the collocated PMIP4 client to initiate the PMIP4 procedures to acquire a HoA from the
19 home agent

20 In case the DHCP proxy determines that the MS has included a MAC address in the chaddr field of the DHCP
21 discover message that is not matching with the known MAC address associated with the data path (i.e., R6 for
22 profile A and C) over which the DHCP message is received, the DHCP proxy MAY consider the following:

23 • A rogue MS trying to spoof MAC address. In this case, the DHCP proxy MAY inform the DPF to initiate
24 data path (i.e., R6 for profile A and C) teardown.

25 Upon receiving a response from the MIPv4 Client with an indication of successful CMIP4 registration, the DHCP
26 proxy SHALL extract the HoA that is assigned to the MS and respond back to the MS with a DHCPOFFER
27 message setting the Your IP address field to the received HoA, Server IP address field to the IP address of the
28 DHCP proxy, and Transaction ID copied from the DHCPDISCOVER message.

29 For the subsequent DHCPREQUEST with the assigned IPv4 address (HoA), the DHCP proxy SHALL respond back
30 to the MS with DHCPACK. In the DHCPACK message the DHCP proxy SHALL set the address lease time
31 parameters (T_1 and T_2 correspond to RENEWING and REBINDING state timers in the MS) as follows as default
32 setting:

33 • $T_1 = 0.5 *$ Lease Time

34 • $T_2 = 0.875 *$ Lease Time

35 However, these values are configurable based on local network policy for optimization of network resources.

36 In order to reduce frequent address renewal messaging over the air, the Lease Time SHOULD be set as reasonably
37 large value.

38 In order to facilitate seamless mobility movement from a MS's perspective, all DHCP proxy entities within a NAP
39 or at least within a group of ASNs belonging to a NAP which support inter-ASN mobility movement SHALL use
40 the same public IP address as the server identifier and the source IP address in the DHCP messages sent to the MS.
41 This will make it looks like the MS is communicating with the same DHCP proxy entity at all time, even after the
42 handoff to a different ASN, therefore guarantees the continuity of the DHCP state machine. This public IP address
43 SHALL be reserved for DHCP proxy entities only and SHALL NOT be used by any other functional entities within
44 the NAP. This public IP address SHALL NOT be propagated within the ASN routing domain in case there is a need
45 to turn on routing protocol in the user data plane. In profiles A and C, by definition DHCP proxy is on the ASN-GW

1   and is configured to use only the defined public IP address. For profile B systems, standalone DHCP proxies may be
2   used and DHCP proxies MAY be configured with other IP addresses for control or messaging purpose.

3   **4.8.2.1.2.2   DHCP Relay Requirements**

4   The DHCP relay SHALL support the procedures defined in [25] , [23] and [24].

5   The DHCP relay SHALL handle all DHCP messages sent by the MS to the broadcast IP address.

6   The DHCP relay is configured with the DHCP server address during the MS authentication. The AAA server MAY
7   send the address of the DHCP server in the AccessAccept message. The DHCP relay SHALL use this address to
8   relay the DHCP messages from the MS to the DHCP server.

9   Upon receiving a DHCPDISCOVER message from the MS, the DHCP relay SHOULD verify that the "chaddr" field
10 in the DHCP header matches the pseudo NAI associated with the R6/R4 over which the DHCP message is received.
11 This is feasible without any additional option in the DHCP message since the DHCP relay is collocated with the
12 Anchor ASN (ASN-GW for profiles A and C). This is done to prevent MAC address spoofing by a rogue MS.

13 In case, the DHCP relay determines that the MS has included a MAC address in the chaddr field of the
14 DHCPDISCOVER message that does not match with the known MAC address associated with the R6/R4 over
15 which the DHCP message was received, the DHCP relay MAY consider the following action:

16 •   A rogue MS trying to spoof MAC address. In this case, the DHCP relay MAY inform the DPF to initiate
17   R6 teardown.

18 After determining the pseudo NAI to be used for the request, the DHCP relay adds the relay agent option to the
19 original DHCP message and sets the Subscriber-ID suboption to the pseudo NAI associated with MS. If there is a
20 secure communication channel between the DHCP relay and the DHCP server, the relay and server MAY choose to
21 omit the authentication suboption.

22 The messaging between the DHCP relay and DHCP server is transported over R3 interface.

23 When DHCP relay receives the DHCPOFFER message from the DHCP server, it SHALL relay it to the MS. If the
24 DHCP server included the authentication suboption in the relay agent option, the DHCP relay SHALL validate it
25 before relaying the DHCPOFFER to the MS.

26 The DHCP relay behavior for handling DHCPREQUEST from the MS is same as in the case of DHCPDISCOVER.

27 When DHCP relay receives the DHCPACK message from the DHCP server, it SHALL prompt the PMIP4 client to
28 initiate MIPv4 registration procedures and pass the assigned IPv4 address (yiaddr in DHCP header of the
29 DHCPACK) and the HA information to the PMIP4 client. The PMIP4 client SHALL perform the registration with
30 the FA and HA on behalf of the MS. The PMIP4 client SHALL inform the DHCP relay that the MIPv4 registration
31 is successfully completed. Only upon receipt of such indication, the DHCP relay SHALL relay the DHCPACK
32 message to the MS.

33 The DHCP relay SHALL intercept the DHCP renewal message, verify the content of the message. If R3 is not
34 secured (e.g. by IPSec), the DHCP relay SHALL add the relay agent authentication suboption to the message before
35 relaying it to the DHCP server.

36 **4.8.2.1.2.3   DHCP Server Requirements**

37 The DHCP server SHALL support the procedures defined in [25], [23]and [24].

38 The DHCP server SHALL be located in the CSN. The DHCP server and the HA SHALL be located in the same
39 CSN. The HAAA SHALL ensure that the DHCP server is located in the same CSN as the HA at the time of
40 assigning these parameters to the NAS.

41 During the initial address assignment and the subsequent address renewals, the DHCP server receives DHCP
42 messages from the DHCP relay in the ASN. If the message received by the DHCP server includes the relay agent
43 authentication suboption, the DHCP server SHALL validate it and also include the relay agent authentication
44 suboption in its response, so that DHCP relay can do the same. The DHCP server SHALL process the
45 DHCPDISCOVER and DHCPREQUEST messages sent by the relay agent and the DHCP Client according to
46 [25]and [24].

1 All messages originated by the DHCP server SHALL always include the server identifier option set to its own IP
2 address.

3 In the case when DHCP lease time expires, the DHCP server MAY inform the HA that the HoA assigned to a MS
4 has expired. In response, the HA MAY send Registration Revocation to the FA, so that the PMIP4 client and related
5 resources can be released. Synchronization between the DHCP server and the HA is not specified by this document
6 and is left as an implementation option.

7 **4.8.2.1.3 PMIP4 Client Requirements**

8 The PMIP4 Client initiates PMIP4 registration (or HoA acquisition) procedures based on either internal trigger
9 received from collocated DHCP server/proxy or via HoA-Request message received from an external DHCP
10 server/proxy. It is assumed that in case of an external DHCP server/proxy, the PMIP4 client has a trust relationship
11 with the DHCP server/proxy.

12 Upon receiving an internal trigger or HoA-Request message from a DHCP server/proxy, the PMIP4 Client SHALL
13 extract the user info (pseudo NAI) from the message/trigger. With the extracted pseudo NAI, the PMIP4 Client
14 SHALL attempt to locate the PMIP4 Context that is cached in the ASN hosting the Anchor Authenticator (PMIP4
15 Client is collocated with the MS Anchored Authenticator). If the associated PMIP4 Context is found in the local
16 cache, the PMIP4 Client SHALL proceed with the Mobile IPv4 registration process. Otherwise, the PMIP4 Client
17 SHALL send a HoA-Request-NAK to the DHCP sever notifying it that corresponding NAI is missing PMIP4
18 Context.

19 The PMIP4 Context is established at the Anchor Authenticator during Device/User Network Access Authentication
20 and Authorization procedures (see section 4.4.1).

21 After identifying the PMIP4 Context for the pseudo NAI, the PMIP4 Client SHALL extract the following
22 information from the Context:

23   • PseudoIdentity@realm

24   • MN-HA key and MN-HA-SPI-PMIP4 [10]

25   • MN-FA key

26   • FA-HA key

27   • Home Agent address to be used for this registration.

28   • HoA (if any)

29 It is assumed that initially the PMIP4 Client is collocated with the FA in the same network element (ASN-GW in
30 profiles A and C and IBS in profile B). The PMIP4 Client SHALL generate a Mobile IPv4 Registration Request
31 (RRQ) as per [15]. For CMIP and PMIP co-existence network, the RRQ from PMIP client contains a value of the
32 SPI = SPI-PMIP4, associated with the PMIP MN-HA that was received during the EAP based Device/User Network
33 Access Authentication and Authorization. This value of SPI is used to indicate the mobility mode of this MS and
34 direct MIP signaling to PMIP client. The RRQ SHALL also contain the NAI extension carrying the pseudo NAI of
35 the user obtained from the PMIP4 Context. If the PMIP4 context contains the HoA (assigned by the Home AAA and
36 delivered through DHCP proxy) the RRQ SHALL include this HoA. Otherwise,.the HoA segment in MIP RRQ
37 need be set to 0. The Authorization-Enabling extension in this message SHALL be MN-HA AE. The RRQ MAY be
38 protected by FA-HA AE. The RRQ SHALL also contain the Revocation Support Extension as per [26] so that
39 registration revocation can be performed when needed.

40 Upon receiving a MIP4 Registration Reply (RRP) from the Home Agent, the PMIP4 Client SHALL authenticate the
41 message by processing the MN-HA AE and FA-HA AE and setup registration revocation capability for the session.
42 If authentication is successful and if the message passes replay verification, the PMIP4 Client SHALL inspect the
43 RRP for any error codes. If the reply code is set to 0 indicating successful registration, the PMIP4 Client SHALL
44 extract the HoA information from the RRP and notify the DHCP proxy with an indication of MIP4 registration
45 success including the assigned HoA address(assigned HoA). Otherwise, the PMIP4 Client SHALL notify the DHCP
46 proxy indicating the failed operation to acquire an IPv4 (HoA) for the pseudo NAI.

---

[10] The MN-HA key represents security association between PMIP4 client and the HA; the MN-HA SPI is set to the SPI-PMIP4
value that identifies the PMIP4 MN-HA key.

1 **4.8.2.1.4 FA Requirements**

2 FA should operate as defined in [15] and [26].

3 For PMIP and CMIP co-existence network, upon receiving RRQ with "PMIP flag" is set, FA SHALL consider its
4 PMIP operation and SHALL NOT send R3 mobility context to context server since DHCP proxy has already sent it
5 before.

6 If R3 is not secured (e.g, by IPsec), then FA SHALL append FA-HA AE to the RRQ before relaying the RRQ to the
7 HA. Also, the FA SHALL include the Revocation Support Extension as per [26] so that registration revocation can
8 be performed when needed. In the Revocation Support Extension, the FA SHALL set the I-bit to 0. If FA-HA AE is
9 used to protect these messages, the FA SHALL validate the FA-HA AE in the RRP before forwarding the same to
10 the PMIP4 client.

11 FA SHALL fetch the necessary MIP keys from the Authenticator.

12 FA relocation in this release SHALL only be supported between the AnchorDPF and serving ASN/ASN-GW.

13 **4.8.2.1.5 HA Requirements**

14 The HA SHALL process Mobile IPv4 messages as per [15] and [26]. The PMIP4 Client populates the HA address in
15 the RRQ with the HA address of the HA that receives the RRQ (HA assignment happens via the HAAA during the
16 EAP based Device/User Network Access Authentication and Authorization procedure, see section 4.4.1).

17 Upon receiving the CMIP4 RRQ message the HA SHALL perform replay verification as per [15]. If replay
18 verification succeeds, the HA SHALL extract the NAI included in the NAI extension. Since this is an initial
19 connection setup, the HA does not have a Binding Cache Entry (BCE) for the user (pseudo NAI). The HA SHALL
20 perform AAA transactions as described below to fetch the MN-HA key and if needed, HA-RK key. Note that the
21 HA is agnostic to PMIP4 vs. CMIP4.

22 After the MN-HA-PMIP4 key and the HA-RK key are available at the HA, the HA derives FA-HA from HA-RK as
23 described in section 4.3.5. The HA SHALL validate the MN-HA AE and FA-HA AE in the received RRQ.
24 Considering successful validation, the HA SHALL assign an IPv4 address to the user (Pseudo NAI) if not included
25 in the RRQ, and admit the binding and the associated keys in the BCE. If the RRQ contains a non-zero HoA value,
26 and that HoA is not supported or in use by other users, the HA SHALL reject the registration request and send code
27 129 in RRP (administratively prohibited). Otherwise, the HA SHALL send a RRP back to the destination address of
28 the received RRQ. The RRP SHALL include the assigned HoA. The other fields of the RRP SHALL be set as per
29 [15].

30 **4.8.2.1.5.1   HA Requirements - Initial Access-Request**

31 Upon receiving RRQ for a MS for which there is no mobility binding exists, the HA SHALL send a RADIUS
32 Access-Request as per [27] to fetch the MN-HA key needed to authenticate the MIP RRQ. If needed, the HA also
33 requests for the HA-RK key to validate+ the corresponding authentication extension.

34 The HA SHALL include the contents of the NAI Extension received in the CMIP4 RRQ in the User-Name attribute,
35 and the MN-HA SPI. The HA SHALL include the Message Authenticator (80) attribute used to integrity protect the
36 Access-Request message.   The value of the Message-Authenticator attribute is set in accordance with the
37 computation specified in [9]

38 The HA SHALL set the NAS-IP or NAS-IPv6 to the IPv4 or IPv6 address of the HA facing the AAA server
39 respectively (The IP address of the NAS Client running on the HA).

40 The HA SHALL set the NAS-Port-Type to TBD.

41 The HA-IP address SHALL be set to the value of the HA-IP address facing the FA.

42 If FA-HA key is required, the HA SHALL set a flag indicating it needs the HA-RK key.

43 The HA SHALL set its WiMAX capability in the WiMAX Capability attribute.

44 The HA SHALL include the CUI attribute set to NUL if it requires the HAAA to include the CUI of the user in the
45 Access-Accept.

46 [for binding different pseudo-IDs, the CUI could be used. If not present, use other attribute, e.g., last-pseudonym]

1 **4.8.2.1.5.2   HA Requirements - Processing Initial Access-Accept**

2 The RADIUS server's role is to transport the correct keys back to the HA.   The RADIUS server does not
3 authenticate the Mobile IP Registration Request. The RADIUS server MAY however return an Access-Reject if it
4 can not find the user session state cached during Device/User Authentication and Authorization procedures or if
5 there were other errors.

6 Upon receiving an Access-Accept packet (see 4.3.5) in response to its Access-Request packet the HA SHALL verify
7 the Message-Authenticator (80) attribute using the procedures defined in [9]. If the Message-Authenticator is not
8 valid the HA SHALL silently discard the Access-Accept packet.

9 The Access-Accept contains an MN-HA key that the HA uses to validate the MN-HA AE. If the HA requested the
10 HA-RK key by including the HA-RK-Key-Request VSA with value set to 1, then the HAAA includes the HA-RK
11 key in the Access-Accept packet.

12 The HA uses the HA-RK key to derive FA-HA from HA-RK as described in section 4.3.5. It validates the FA-HA
13 AE if optional FA-HA AE is used.

14 If the CUI attribute is include and the HA supports CUI then the HA SHALL include the received CUI in all
15 Accounting packets exchanged with the Home-AAA. See [51].

16 If the HA receives Prepaid attributes and the HA supports Prepaid, the HA SHALL provide the prepaid processing
17 as specified in section 4.4.3.3.

18 If the HA receives Hot-lining attributes and the HA supports Hot-lining, the HA SHALL support Hot-lining as
19 specified in section 4.4.3.5.

20 Upon successful processing of the Access-Accept packet, if the HA is configured to perform accounting function for
21 the user's Mobile IPv4 session, the HA SHALL generate a RADIUS Accounting-Request (Start) message indicating
22 to the HAAA that the Mobile IPv4 session for the user has started.

23 **4.8.2.1.5.3   HA Processes RADIUS Access-Reject**

24 If the HA receives a RADIUS Access-Reject packet in response to its Access-Request, the HA SHOULD reject the
25 MIP-Registration-Request by replying back with a Mobile IP Registration Reply according to [15]. In the RRP, the
26 HA SHALL include status code value 131 (mobile node failed authentication).

27 **4.8.2.1.5.4   HA Processing MIP4 Registration Request Indicating Termination**

28 When the HA receives a MIP4 Registration Request with lifetime = 0, the HA SHALL validate the MN-HA AE
29 included in the RRQ. If the validation is successful, the HA SHALL remove the mobility binding for the NAI (user)
30 and it SHALL generate a RADIUS Accounting-Request (Stop) packet if it is configured to do accounting for the
31 MIPv4 session. The HA SHALL respond back with an RRP (w/ lifetime=0) to confirm the successful de-
32 registration. If the MN-HA AE validation fails, the HA SHALL silently discard the RRQ and it MAY log the event
33 for help in system administration. In this case, the HA SHALL not remove the mobility binding of the user (NAI).

34 **4.8.2.1.6 AAA Server Requirements**

35 The HAAA server receives RADIUS Access-Request message from the HA during Mobile IP procedures.   The
36 following text describes the Mobile IPv4 procedures (CMIP4 and PMIP4) for HAAA server

37 Upon receiving the Access-Request messages that contains Message-Authenticator (80) attribute, the RADIUS
38 server SHALL validate the value of the Message-Authenticator (80) as described in [9]. If the authenticator fails to
39 validate, the RADIUS server SHALL silently discard the Access-Request. An Access-Request which does not
40 contain a Message-Authenticator (80) SHALL be silently discarded.

41 The User-Name attribute contains the pseudo-identity of the user established during Device/User Network Access
42 Authentication and Authorization. The HAAA SHALL use the pseudo-identity to fetch the session context for this
43 pseudo-identity.

44 With respect to Mobile IP, the session context contains:

45   • True identity of the user.

1 • HoA that MAY have been assigned to the user.

2 • Key Holder/Generator context

3 If the HAAA is unable to fetch the session context then this indicates that the user has not been previously
4 authenticated and the HAAA SHALL reply back with an Access-Reject to the HA.

5 The HAAA SHALL obtain the MN-HA key computed using the HA-IP address from the Key Holder/Generator
6 context, associated with the value of MN-HA SPI included in MN-HA Authentication Extension. If the SPI in the
7 received request is not associated with MN-HA key in the Key Holder/Generator context, the HAAA SHALL reply
8 back with an Access-Reject to the HA. If the HA requested the FA-HA key by including the FA-HA-Request set to
9 1, then the HAAA SHALL obtain the FA-HA key as well.

10 The HAAA server MAY need to include other attributes in the response back to the HA as follows:

11 • If the MS is a prepaid subscriber and the HA supports the Prepaid Client (as indicated in the WiMAX
12   Capability attribute received in the Access-Accept packet. If the policy is to use the HA for prepaid, then
13   the AAA server SHALL include the prepaid attributes in the Access-Accept (see section PREPAID).

14 • If the MS is to be hot-lined, as indicated by the user-profile, then if the HA supports Hot-lining capability
15   as specified by the WiMAX Capability attribute received in the Access-Request, then if the policy specifies
16   to use the HA as the hot-lining device, the AAA server SHALL include the hot-lining attributes in the
17   Access-Accept (see section HOT-LINING).

18 • If the Access-Request included the CUI attribute set to null, then the AAA server SHALL compute a value
19   for the CUI (see section CUI) and set the CUI attribute to this value.

20 • Prior to sending the Access-Accept packet the HAAA MAY (per local policies) sign the Access-Accept
21   packet using the Message-Authenticator(80) attribute as specified in [9].

22 **4.8.2.1.7 PMIP4 Connection Setup Call Flow**

23 **4.8.2.1.7.1   DHCP Proxy in ASN**
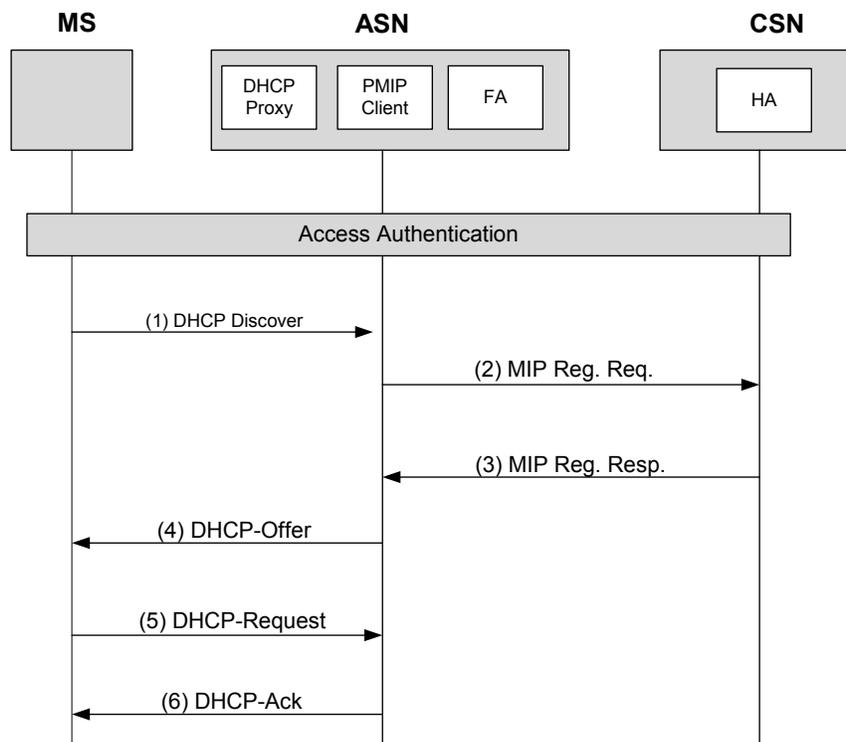
25 **Figure 4-57 – PMIP4 Connection Setup Procedure**

1 The NAS receives HA address and PMIP4 security context from the HAAA at the time of successful Device/User
2 Access Authentication. NAS may also receive HoA address if it is assigned by HAAA. Subsequently, the following
3 steps happen.

STEP 1

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

STEP 2

7 Upon receiving the DHCPDISCOVER message, the DHCP Proxy in the NAS triggers the PMIP4 client to initiate
8 the Mobile IPv4 Registration procedure. If HoA (HAAA only assigns static HoA) was received during access
9 authentication, then the PMIP4 client uses the HoA information and constructs a Mobile IPv4 Registration Request
10 message. If HoA was not access authentication received, then the HoA field is set to 0.0.0.0. In either case, the CoA
11 field is set to the FA-CoA address that is configured locally. PMIP4 client sends the Mobile IPv4 Registration
12 Request to the FA address. The FA forwards the registration request to the HA. The source address for this Mobile
13 IPv4 message over R3 is FA-CoA, and the destination address is HA address.

STEP 3

15 If a HoA is 0.0.0.0 in the Mobile IP Registration Request message, the HA assigns a HoA. Otherwise, the HoA in
16 the Mobile IP Registration Request message is used. The HA responds with the Mobile IP Registration Response
17 message. The source address for this Mobile IPv4 message over R3 is HA, and the destination address is FA-CoA.
18 The FA forwards the message to the PMIP4 client.

STEP 4

20 The PMIP4 client passes this information to the DHCP proxy. The DHCP proxy sends the DHCPOFFER message to
21 the MS.

STEP 5

23 MS sends a DHCPREQUEST to the DHCP Proxy with the information received in the DHCPOFFER.

STEP 6

25 The DHCP Proxy acknowledges the use of this IP address and other configuration parameters as defined in [22] by
26 sending the DHCPACK message

4.8.2.1.7.1.1   DHCP Proxy in ASN Timers and Timer Considerations

28 All timers are set and cleared according to DHCP ([22]) and MIP ([15]) specifications.

1   **4.8.2.1.7.2   DHCP Relay in ASN**
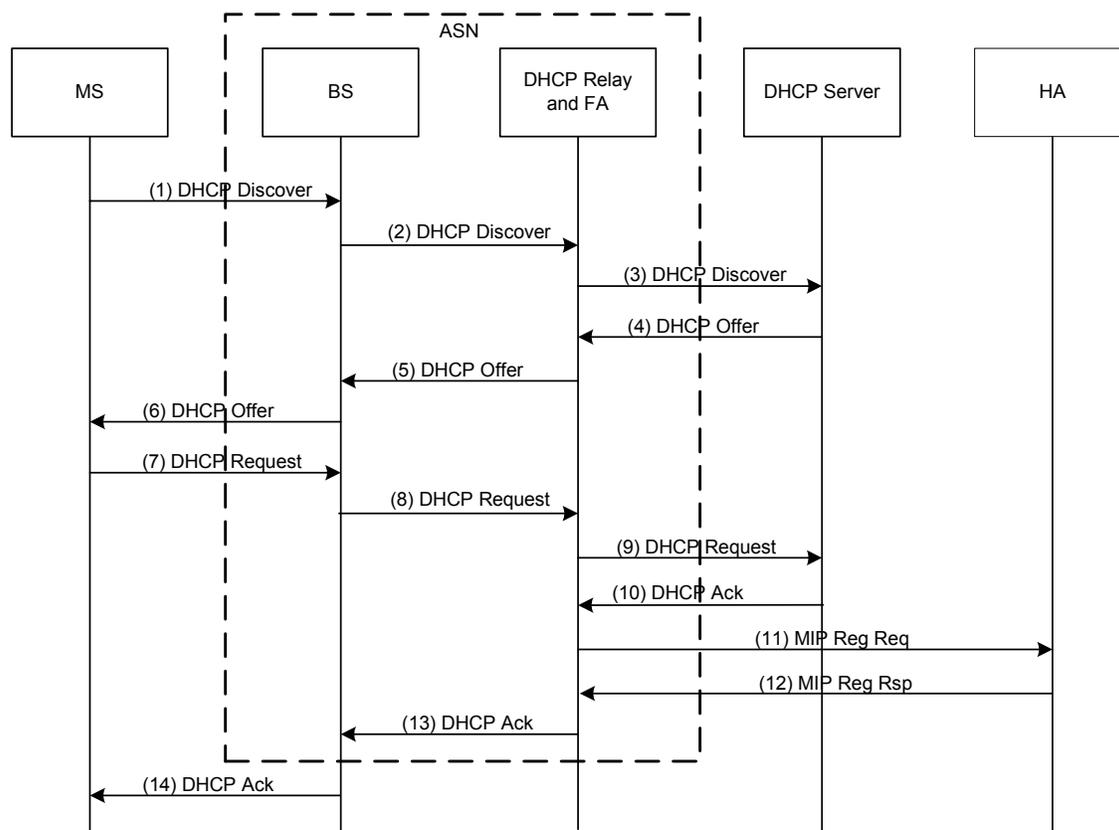
2

3   **Figure 4-58 – PMIP4 Connection Setup - DHCP Relay in ASN**

4   The following steps are written based on R3 is already secured. If R3 is not secured, the DHCP Relay SHALL add
5   the authentication sub-option as explained in [31] to have data integrity and replay protection for relayed DHCP
6   messages.

7   **STEP 1**

8   The MS sends a DHCP Discover as a broadcast message. The DHCP message is sent on the MS's Initial service
9   flow setup over R1 interface to the BS.

10   **STEP 2**

11   The DHCP Discover message is forwarded from BS to DHCP Relay present in ASN through the data path
12   established for the ISF (Initial Service Flow) traffic.

13   **STEP 3**

14   The DHCP Relay in ASN will intercept and change the destination IP address from broadcast to unicast and
15   configure the giaddr field in the DHCP payload and sends the DHCP Discover message to the DHCP server of the
16   MS based on configuration information. The configuration information in the most generic case will be downloaded
17   via AAA but it may also be statically provisioned

18   If the Datapath is per MS or per SF, the MS context can be found based on the Datapath and not on the MAC
19   address. If the Datapath is per BS the MS context can be found based on the MAC address or MS NAI

1 **STEP 4**

2 DHCP servers receiving the DHCP Discover request reply by sending a DHCP Offer message including an offered
3 IP address.

4 **STEP 5**

5 The DHCP Relay in ASN forwards the DHCP replies to the MS. The DHCP Offer message is sent from ASN GW
6 to BS through the Data Path.

7 The destination IP address of the DHCP Offer message sent to MS is a unicast one. Normally DHCP servers or relay
8 agents attempt to deliver the DHCP Offer to a MS directly using unicast delivery. Unfortunately some MS's
9 implementations are unable to receive such unicast IP datagram until they know their own IP addresses. To work
10 around with this kind of MS's broadcast address MAY be used in DHCP Offer message. ASN need to check the
11 BROADCAST (B) flag in the DHCP Offer message. If this flag is set, ASN need use broadcast address to send
12 DHCP Offer message, otherwise unicast address, but the delivery will be over a unicast CID.

13 **STEP 6**

14 BS sends DHCP Offer message to the MS on the MS's Initial Service Flow.

15 **STEP 7**

16 MS receives DHCP Offer message, and sends a DHCP Request to the selected DHCP server as a broadcast message
17 confirming its choice of the DHCP Server.

18 **STEP 8**

19 DHCP Request message is sent from BS to DHCP relay in ASN through the Data Path established.

20 **STEP 9**

21 The DHCP Relay in ASN will relay the DHCP Request to the DHCP server.

22 **STEP 10**

23 The selected DHCP server receives the DHCP Request and replies with a DHCP Ack containing the configuration
24 information requested by the MS.

25 **STEP 11**

26 The DHCP Relay in the ASN triggers the PMIP4 client to initiate the Mobile IP Registration procedure. The PMIP4
27 client uses the HoA information and constructs a Mobile IP Registration Request message. This message contains
28 HoA and CoA for this MS. The source address for this R3 message is CoA, and the destination address is HA
29 address.

30 **STEP 12**

31 The HA responds with the Mobile IP Registration Response message. The source address for this R3 message is
32 HA, and the destination address is CoA.

33 **STEP 13**

34 After the establishment of MIP tunnel the PMIP4 client triggers DHCP Relay to send the DHCP Ack to the BS.

35 **STEP 14**

36 BS sends DHCP Ack message to the MS on the MS's provisioned Initial Service Flow.

37 If MS doesn't receive a DHCP Ack, or DHCP Nak message when timeout, it will retransmit DHCP Request. If
38 neither DHCP Ack nor DHCP Nak received when the maximum retransmission reached, MS SHALL restart the IP
39 initialization process.

1 **4.8.2.1.7.2.1   DHCP Relay in ASN Timers and Timer Considerations**

2 All timers are set and cleared according to DHCP ([22]) and MIP ([15]) specifications.

3 **4.8.2.2   Proxy MIPv4 Session Renewal Procedure**

4 The PMIP4 Client SHALL refresh the MIPv4 binding with the FA and the HA on behalf of the MS. This procedure
5 is transparent to the MS since the DHCP RENEW and REBIND states are not tied to the Mobile IPv4 Registration
6 Lifetime (which the MS is unaware of).

7 **4.8.2.2.1 MS Requirements**

8 The MS SHALL support the DHCP client function as defined in [25]. The address renewal by the MS SHALL be
9 based on the T1 (RENEW) and T2 (REBIND) timers as defined in the RFC.

10 **4.8.2.2.2 DHCP Requirements**

11 **4.8.2.2.2.1   DHCP Proxy**

12 The DHCP proxy SHALL implement the DHCP lease renewal process as per [25]. When the DHCP proxy receives
13 a DHCPREQUEST message from the MS for an IPv4 address for which the Lease Time is either close to T1 or T2
14 value, it SHALL respond back to the MS with DHCPACK message. Note, that PMIPv.4 client performs MIP
15 binding renewal automatically and if it fails, it will update DHCP proxy (refer to section 4.8.2.2.3).

16 Since all DHCP proxies in the NAP are assigned with the same IP address, the DHCP message sent by the MS will
17 be terminated by the DHCP proxy collocated with anchor DPF/FA.

18 **4.8.2.2.2.2   DHCP Relay in ASN**

19 The anchor data path ASN GW SHALL act as a DHCP relay and SHALL intercept every DHCP message originated
20 by the MS. The DHCP relay SHALL perform the verification of the 'chaddr' field in the DHCP message and other
21 security related checks as described in 4.8.2.1.7.2.1. DHCP relay SHALL relay the DHCP message to the DHCP
22 server in the CSN, in accordance with the [23]. If R3 is not secured (e.g. by IPsec), the DHCP relay SHALL
23 authenticate relayed DHCP messages by providing the relay agent authentication suboption ([31]).

24 **4.8.2.2.3 PMIP4 Client Requirements**

25 The PMIP4 Client SHALL perform the same procedures as defined in section 4.8.2.1.3 to renew the MIPv4 binding
26 with the HA when Pmip4 client and FA are collocated in the same ASN. Otherwise, Pmip4 client shall use
27 FA_Register_Req and FA_Register_Rsp messages for MIP registration over R4 as shown in steps 4 to 7 of PMIP4
28 CSN MM Handover procedure in section 4.8.2.3.7.1.

29 **4.8.2.2.4 FA Requirements**

30 The FA requirements are the same as section 4.8.2.1.4.

31 **4.8.2.2.5 HA Requirements**

32 The HA SHALL process the RRQ for binding renewal for an existing binding cache entry the same way as defined
33 in section 4.8.2.1.5.

34 **4.8.2.2.6 AAA Server Requirements**

35 Same as section 4.8.2.1.6.

1 **4.8.2.2.7 PMIP4 Session Renewal Call Flows**

2 **4.8.2.2.7.1 DHCP Session Renewal Flows**

3 **4.8.2.2.7.1.1 DHCP Proxy**

4
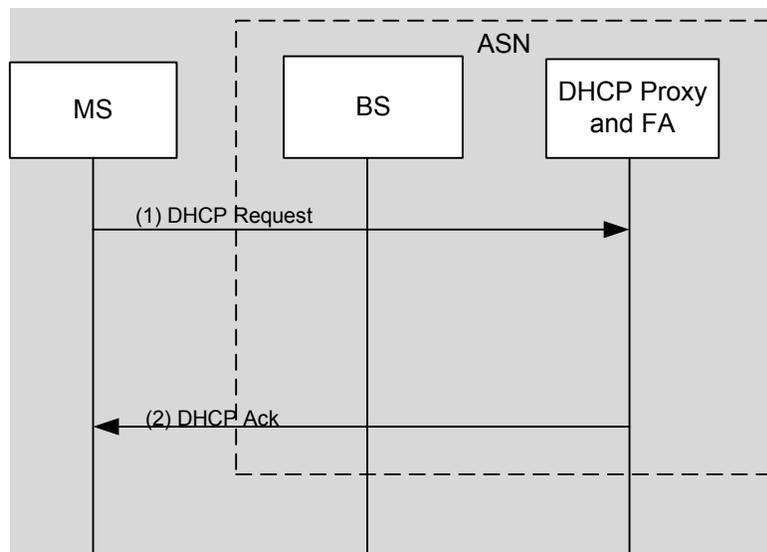
5 **Figure 4-59 DHCP Session Renewal in PMIP4 case- DHCP Proxy in ASN**

6

7 **STEP 1**

8 The MS sends a DHCP Request to the DHCP Proxy collocated with Anchor DPF/FA GW in order to renew its IP
9 address.

10 **STEP 2**

11 The Anchor ASN SHALL process the unicast DHCP Request message and reply with a DHCP Ack to MS.

12 In case of DHCPNAK message, the PMIP4 client may initiate the MIP deregistration procedure, if DHCP Proxy and
13 PMIP4 client are not collocated the DHCP Proxy may send FA_Revoke_Req to trigger PMIP4 client or alternatively
14 the MS MAY initiate network exit. If the MS does not receive any response from the DHCP Proxy, the MS does
15 number of retries and then MAY initiate network exit

16 .

1 **4.8.2.2.7.1.2   DHCP Relay in ASN**
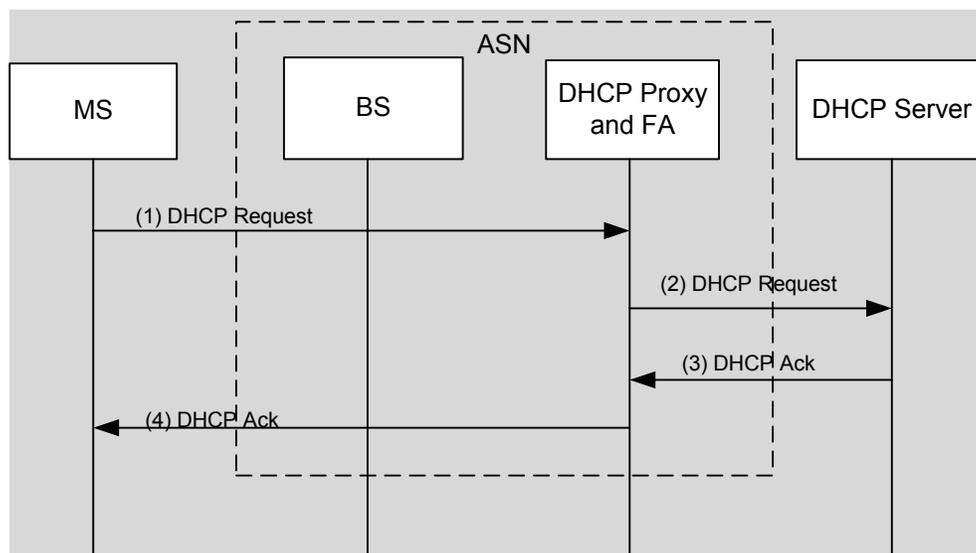
2

3   **Figure 4-60 – DHCP Session Renewal in PMIP4 case- DHCP Relay in ASN**

4 **STEP 1**

5 The MS sends a DHCP Request to the DHCP server in order to renew its IP address.

6 **STEP 2**

7 The Anchor ASN MAY monitor the unicast DHCP Request message and forwards it to the DHCP server.

8 **STEP 3**

9 The DHCP server replies with a DHCP Ack to ASN.

10 **STEP 4**

11 The DHCP relay forwards the DHCP ACK message to MS. In case of DHCP NAK message, the PMIP4 client may
12 initiate the MIP deregistration procedure, if DHCP relay and PMIP4 client are not collocated the DHCPrelay may
13 send FA_Revoke_Req to trigger PMIP4 client or alternatively the MS may initiate Network exit. If the MS does not
14 receive any response from the DHCP server the MS does number of retries and then MAY initiate Network exit.

15 **4.8.2.2.7.1.2.1   DHCP Relay in ASN Timers and Timer Considerations**

16 All timers are set and cleared according to DHCP ([22]) and MIP ([15]) specifications.

17 **4.8.2.2.7.2   MIPv4 Session Renewal Flows**

18 Same as the PMIP4 session establishment procedure described in section 4.8.2.1

19 **4.8.2.3   Proxy MIP CSN Anchored Mobility Handover**

20 The detailed call flows for the PMIP4 based CSN Anchored Mobility is described in section 4.8.2.3.7. This section
21 describes CSN anchored mobility handover without re-authentication.

22 If the FA relocation is due to MS moving from one FA to another FA, before the FA relocation, the ASN anchored
23 mobility events occur, and its detail procedure is shown in section 4.7. In order to prevent packet loss and reduce
24 handoff latency, the temporary R4 data path between two ASNs MAY be established.

25 The relocation of the FA SHALL always be negotiated between the Anchor ASN and the Serving ASN. Both the
26 Anchor ASN and the Serving ASN can initiate the negotiation. If the Anchor ASN initiates the negotiation, it

1 SHALL send an Anchor DPF *HO_Req* message with its own CoA address, DHCP context information for the MS

2 and other layer3 context maintained by the Anchor to the Serving ASN. This message SHALL be addressed to the

3 DPF in Serving ASN, whose address is known since it is on the data path to the MS. If the Serving ASN agrees to

4 take over the FA functionality after this negotiation, then it SHALL send an *Anchor_DPF_Relocate_Req* message to

5 the PMIP4 client using the information provided by the Anchor ASN.

6 If the Serving ASN initiates the negotiation, it SHALL send an Anchor DPF HO Trigger message to the anchor DPF

7 in Anchor ASN, and the Anchor ASN starts the source initiated negotiation as indicated above. In both cases, only

8 after both Anchor ASN and the Serving ASN agree with the Anchor relocation, the Serving ASN will send an

9 *Anchor_DPF_Relocate_Req* to the PMIP4 client to start MIP registration procedure.

10 **Table 4-81 – Anchor DPF HO_Req Message**

IE	Reference	M/O	Notes
Anchor MM context	5.3.2.11	M	DHCP Proxy Info, DHCP Server Info, MIPv4 Info etc

11 **Table 4-82 – Anchor DPF HO Trigger Message**

IE	Reference	M/O	Notes

12 The mobility event MAY not require relocation of the PMIP4 Client and the Authenticator, for that case, Only the

13 FA SHALL be relocated to a target ASN. During the FA relocation, DHCP context along with other Layer3 context

14 maintained by the Anchor ASN for the MS SHALL be transferred to the target ASN. The PMIP4 Client SHALL

15 initiate a MIPv4 registration on behalf of the MS via the target FA.

16 After the MIP registration, the Serving ASN will take over the FA role and it SHALL send an Anchor DPF *HO_Rsp*

17 message to the previous Anchor ASN. Upon receiving the Anchor DPF *HO_Rsp* message with success indication,

18 the previous Anchor ASN SHALL remove the mobility binding, the DHCP context information and the R4 data

19 path.

20 **Table 4-83 – Anchor DPF HO_Rsp Message**

IE	Reference	M/O	Notes
R3 Operation Status	5.3.2.167	M	Success or failure indication

21 **4.8.2.3.1 MS Requirements**

22 There are no specific MS requirements for CSN anchored mobility management with PMIP4.

23 **4.8.2.3.2 DHCP Proxy/Relay Requirements**

24 **4.8.2.3.2.1   DHCP Proxy in ASN**

25 The DHCP proxy, collocated with the Anchor DPF/FA SHALL be relocated to the target ASN if the R3 mobility

26 event occurs.

27 The old Anchor ASN SHALL remove the DHCP context information for the MS, once it receives a success

28 indication from the Target ASN that FA has been relocated.

29 **4.8.2.3.2.2   DHCP Relay in ASN**

30 The DHCP relay, collocated with the Anchor DPF/FA SHALL be relocated to the target ASN if the R3 mobility

31 event occurs.

1 After the successful R3 relocation event, the new anchor data path ASN GW SHALL act as a DHCP relay for the
2 MS. In the course of the R3 relocation, the address of the DHCP server is transferred as part of the MS context from
3 the serving to the target ASN GW.

4 The new anchor data path ASN GW SHALL intercept every DHCP message originated by the MS. It SHALL
5 perform the verification of the 'chaddr' field in the intercepted DHCP message and other security related checks as
6 described in 4.8.2.1.2.2. DHCP relay SHALL relay the intercepted DHCP message to the DHCP server in the CSN,
7 in accordance with the [23] . If R3 is not secured (e.g. by IPsec), the DHCP relay SHALL authenticate relayed
8 DHCP messages by providing the relay agent authentication suboption ([31]).

4.8.2.3.3 PMIP4 Client Requirements

10 Upon receiving an *Anchor_DPF_Relocate_Req* from the Serving ASN, and the Source FA-CoA matching the FA
11 Identity on its record, the PMIP4 Client SHALL send a *FA_Register_Req* message to the Serving ASN to initiate a
12 MIPv4 registration on behalf of the MS via the target FA. If the Source FA-CoA does not match the FA identity on
13 its record, the PMIP4 Client SHALL send a *Anchor_DPF_Relocate_Rsp* message to the Serving ASN with status
14 indicator set to Failure.

15 **Table 4-84 – Anchor_DPF_Relocate_Req Message**

IE	Reference	M/O	Notes
Care-Of Address	5.3.2.28	M	
Anchor MM Context	5.3.2.11	M	

16 **Table 4-85 – FA_Register_Req Message**

IE	Reference	M/O	Notes
RRQ	Section 5.3.2.20	M	Defined in MIP RFC.
FA-HA Key	Section 5.3.2.66	O	FA-HA if used

17 **Table 4-86 – FA_Register_Rsp Message**

IE	Reference	M/O	Notes
RRP	Section 5.3.2.97	M	Defined in MIP RFC

18 **Table 4-87 – Anchor_DPF_Relocate_Rsp Message**

IE	Reference	M/O	Notes
R3 Operation Status	5.3.2.167	M	Success or Failure indication.

4.8.2.3.4 FA Requirements

20 In general the requirements specified in 4.8.2.1.4 SHALL apply to the FA.

4.8.2.3.5 HA Requirements

22 The HA SHALL process the RRQ the same way as defined in 4.8.2.1.5. The HA SHALL modify the binding cache
23 entry for the MS to reflect the new CoA (of the target FA). After processing the RRQ successfully, the HA SHALL
24 begin to forward packets destined for the MS to the new CoA. The HA MAY send Revocation message to the
25 previous FA to terminate binding.

1 **4.8.2.3.6 AAA Server Requirements**

2 There are no specific AAA Server requirements for CSN anchored mobility management with PMIP4.

3 **4.8.2.3.7 PMIP4 Mobility Procedure**

4 **4.8.2.3.7.1   PMIP4 CSN MM Handover**
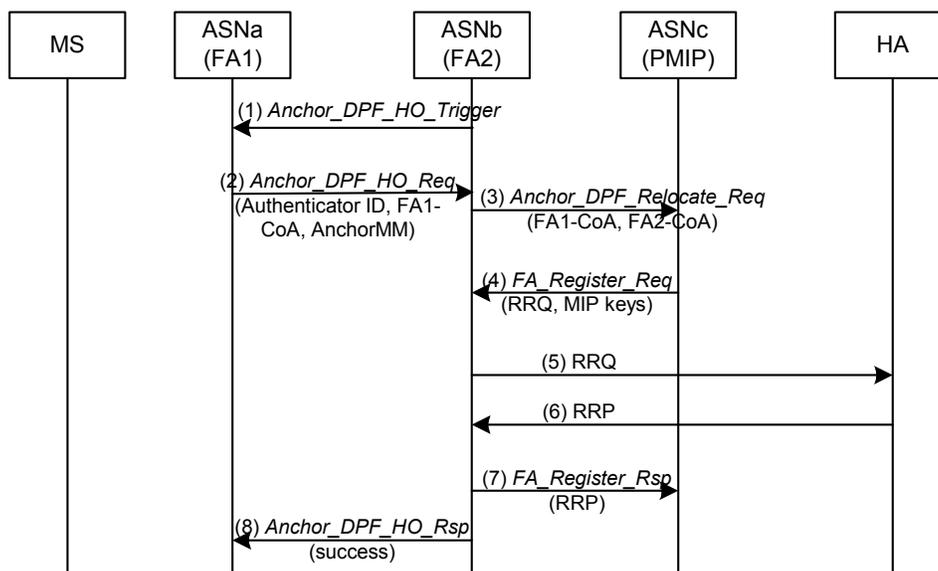
5

6 **Figure 4-61 – CSN-Anchored Mobility (PMIP)**

7 **STEP 1**

8 If the target ASNb initiates the FA relocation negotiation, it sends an *Anchor_DPF_HO_Trigger* message to the
9 anchor DPF in ASNa. If ASNa agrees with the FA relocation, it proceeds to Step 2. After sending
10 *Anchor_DPF_HO_Trigger*, ASNb starts a timer $T_{Anchor\_DPF\_HO\_Trigger}$ for *Anchor_DPF_HO_Req*.   Once
11 *Anchor_DPF_HO_Req*, indicating the FA relocation decision of ASNa, is received by ASNb, $T_{Anchor\_DPF\_HO\_Trigger}$ is
12 stopped.

13 If the source ASNa initiates the FA relocation procedure, the call flow starts from Step 2.

14 **STEP 2**

15 ASNa sends an *Anchor_DPF_HO_Req* message to the DPF in ASNb. The message contains the current FA-CoA
16 address and the DHCP context information for the MS, and ASNa will start a timer $T_{Anchor\_DPF\_HO\_Req}$[11] for
17 *Anchor_DPF_HO_Rsp* from ASNb.

18 **STEP 3**

19 Target ASN for FA relocation sends an *Anchor_DPF_Relocate_Req* message to the PMIP4 client, and starts a timer
20 $T_{Anchor\_DPF\_Relocate\_Req}$ for *FA_Register_Req*. This message relays some information about target ASN that is necessary
21 in order to construct and send the MIP RRQ message in step 4. The message contains CoA for the target FA, and
22 target FA address if it is different than the CoA. In addition to target FA-CoA, current FA-CoA is included in the
23 message.

---

[11] $T_{Anchor\_DPF\_HO\_Req}$ value should be larger than the sum of $T_{AnchorDPF\_Relocate\_Request}$ and $T_{FA\_Register\_Request}$ including retransmission

STEP 4

The PMIP4 client verifies that the current FA-CoA indeed matches the FA on its record, and starts the MIP registration with the target FA by sending *FA_Register_Req* message. This message contains a fully formed RRQ according to [15], with CoA field in the RRQ set to the CoA of the Target FA which is received in *Anchor_DPF_Relocate_Req* message in step 3. The source address of the RRQ is that of the MS and the destination address the CoA or the FA if FA address is different from CoA. In addition, *FA_Register_Req* message contains the FA-HA MIP key if this key is used. This message is sent to the Target ASN, whose address was identified as the source address of the *Anchor_DPF_Relocate_Req* message in step 3. A timer $T_{FA\_Reg\_Req}$[12] is started for *FA_Register_Rsp* from ASNb.

STEP 5

After receiving *FA_Register_Req*, ASNb stops $T_{Anchor\_DPF\_Relocate\_Req}$. The target FA relays the RRQ to the HA.

STEP 6

The HA responds with the RRP.

STEP 7

The target ASN relays the MIP RRP encapsulated in an *FA_Register_Rsp* message to the PMIP4 client. The PMIP4 client updates the FA in its record and stops $T_{FA\_Reg\_Req}$.

STEP 8

The target ASN also replies to the source ASNa with an *Anchor_DPF_HO_Rsp* message indicating a successful FA relocation. The source ASNa can then remove the mobility binding, DHCP context information and the R4 data path towards the ASNb. ASNa also stops $T_{Anchor\_DPF\_HO\_Req}$ started in step 2.

4.8.2.3.7.1.1 PMIP4 CSNMM Handover Timers and Timer Considerations

This section provides the description of the timer used during PMIP4 CSN MM Handover.

- $T_{Anchor\_DPF\_HO\_Trigger}$: is started by target ASNb upon sending an *Anchor_DPF_HO_Trigger* message. It is stopped upon receiving a corresponding *Anchor_DPF_HO_Req*.

- $T_{Anchor\_DPF\_HO\_Req}$: is started when serving ASNa sends an *Anchor_DPF_HO_Req* and is stopped upon receiving a corresponding *Anchor_DPF_HO_Rsp*.

- $T_{Anchor\_DPF\_Relocate\_Req}$: is started by the target ASNb when the *Anchor_DPF_Relocate_Req* is sent on R4. It is stopped upon receiving a corresponding *FA_Register_Req*.

- $T_{FA\_Reg\_Req}$: is started by the PMIP4 client when the *FA_Register_Req* is sent on R4. It is stopped upon receiving a corresponding *FA_Register_Rsp*

Table 4-88 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-88 – Timer Values for PMIP4 CSN MM Handover Messages over R4/R3

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Anchor\_DPF\_HO\_Trigger}$	TBD		TBD
$T_{Anchor\_DPF\_HO\_Req}$	TBD		TBD

---

[12] The value of $T_{FA\_Reg\_Req}$ and retransmission behavior should be per [15].

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T $_{Anchor\_DPF\_Relocate\_Req}$	TBD		TBD
T $_{FA\_Reg\_Req}$	TBD		TBD

1   **4.8.2.3.7.1.2   PMIP4 CSN MM Handover Error Conditions**

2   This section describes error conditions associated with the PMIP4 CSN MM Handover procedure.

3   **4.8.2.3.7.1.2.1   Timer Expiry**

4   Table 4-89 shows details on the corresponding actions associated with timer expiry. Upon each timer expiry, if the
5   maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s) should be
6   performed as indicated in Table 5-70B Timer Expiry Conditions.

7   **Table 4-89 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T$_{Anchor\_DPF\_HO\_Trigger}$	Target FA	PMIP4 CSN MM handover is aborted
T $_{Anchor\_DPF\_HO\_Req}$	Serving FA	PMIP4 CSN MM handover is aborted
T $_{Anchor\_DPF\_Relocate\_Req}$	Target FA	PMIP4 CSN MM handover is aborted and *Anchor_DPF_HO_Rsp* is sent to ASNa with status indicator set to Failure
T $_{FA\_Register\_Req}$	PMIP4 client	PMIP4 CSNMM Handover is aborted

8   **4.8.2.3.7.1.2.2   Current FA-CoA Mismatches the FA on PMIP4 client**

9   *Anchor_DPF_Relocate_Rsp* with status indicator set to Failure is sent to the sender of *Anchor_DPF_Relocate_Req*.
10   And PMIP4 CSN MM Handover is aborted. This message will also trigger *Anchor_DPF_HO_Rsp* with a failure
11   indication.

12   **4.8.2.3.7.1.2.3   MIP Registration Failure**

13   It can be caused due to many reasons, such as authentication failure. In this case, PMIP4 CSN MM handover is
14   aborted and *Anchor_DPF_HO_Rsp* is sent to ASNa with status indicator set to Failure.

15   **4.8.2.4   Proxy MIP Session Termination**

16   There are various reasons for termination of an ongoing session for a user. The termination MAY be due to:

17   • The MS sending a DHCPRELEASE message

18   • The IP address lease timer expires at the DHCP proxy or FA initiated session release

19   • Authenticator initiated release due to re-authentication timeout or AAA initiated release

20   • HA decides to release session of the MS and send Registration Revocation message to the FA (Refer to
21   [26]).

22   For PMIP4 session termination triggered network exit, see section 4.5.2.

23   **4.8.2.4.1 MS Requirements**

24   When the MS needs to terminate the connection with a WiMAX network, it SHOULD send a DHCPRELEASE
25   message to the DHCP proxy to gracefully terminate the L3 connection and release the assigned IP address.

1 **4.8.2.4.2 DHCP Requriements**

2 **4.8.2.4.2.1 DHCP Proxy**

3 Upon receiving a DHCPRELEASE from the MS or upon expiry of the lease timer for the HoA, the DHCP proxy
4 SHALL notify the PMIP4 Client to de-register the MIPv4 session for the MS.

5 The DHCP proxy SHALL release the IPv4 address lease (HoA) and any associated state for the MS upon receiving
6 a notification of successful MIPv4 de-registration from the PMIP4 Client.

7 **4.8.2.4.2.2 DHCP Relay in ASN**

8 Upon intercepting a DHCPRELEASE from the MS, in addition to relaying the DHCPRELEASE message to the
9 DHCP server, the DHCP relay SHALL notify the PMIP4 Client to de-register the MIPv4 session for the MS.

10 **4.8.2.4.3 PMIP4 Client Requirements**

11 Upon receiving a *FA_Revoke_Req* message from the FA for reasons such as DHCP initiated release or FA/HA
12 initiated release, the PMIP4 client SHALL clear the mobility binding and reply back with a *FA_Revoke_Rsp*
13 message.

14 **Table 4-90 – FA_Revoke_Req**

IE	Reference	M/O	Notes
FA Revoke Reason	Section 5.3.2.16	M	DHCP release, expiry, FA initiated release, HA initiated release

15 **Table 4-91 – FA_Revoke_Rsp**

IE	Reference	M/O	Notes
Result Code	Section 5.3.2.154	M	Result of Revoke, Success or failure indication

16 **4.8.2.4.4 FA Requirements**

17 There is no specific requirement on the FA for the termination process.

18 **4.8.2.4.5 HA Requirements**

19 The HA SHALL process the RRQ with Lifetime=0 and release the mobility binding for the user (NAI).

20 If accounting is enabled at the HA the HA SHALL send an Accounting-Request (Stop) packet with Acct-Terminate-
21 Action set to "Session-Timeout" or "User-Request" depending on whether or not the session was terminated due to
22 session time out (e.g. MIP lifetime timer expiry) or due to user request.

23 **4.8.2.4.6 AAA Server Requirements**

24 Upon receiving the Accounting-Request (Stop) message the AAA server SHALL signal the KeyHolder to delete all
25 the keys and all other session information stored for this session.

1   **4.8.2.4.7   PMIP4 Session Release Procedure**

2   **4.8.2.4.7.1   PMIP4 Session Release**

3   **4.8.2.4.7.1.1   MS Initiated PMIP4 Session Release**
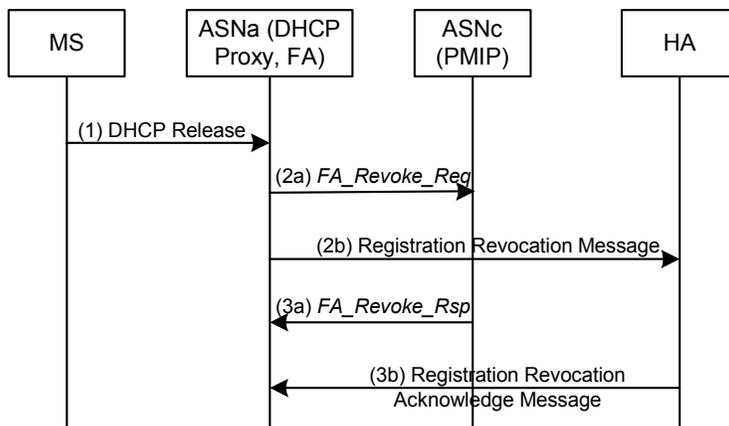
5   **Figure 4-62 – PMIP4 Session Release Triggered by MS, DHCP Proxy or FA**

6   **STEP 1**

7   The trigger can be MS sending DHCP-Release message to the ASNa where the DHCP proxy and FA reside or
8   DHCP proxy has expired on lease time or FA initiated session release.

9   **STEP 2 a, b**

10   The ASNa initiates the session release with PMIP4 client and HA concurrently by sending *FA_Revoke_Req* and
11   Registration Revocation Message respectively. At this point, ASNa starts a timer $T_{FA\_Revoke\_Req}$ to wait for
12   *FA_Revoke_Rsp*[13].

13   **STEP 3 a, b**

14   *FA_Revoke_Rsp* and Registration Revocation Acknowledgement Message are received from PMIP4 client and HA
15   respectively. After ASNa has received *FA_Revoke_Rsp* messages, $T_{FA\_Revoke\_Req}$ is stopped.

16   **4.8.2.4.7.1.1.1   MS Initiated PMIP4 Session Release Timer and Timing Consideration**

17   This section identifies the timer used during MS Initiated PMIP4 Session Release procedure.

18   • $T_{FA\_Revoke\_Req}$: is started by AnchorDPF ASNa, where DHCP proxy and FA are located, upon sending an
19   *FA_Revoke_Req* message and a Registration Revocation message. It is stopped upon receiving both
20   corresponding *FA_Revoke_Rsp* and Registration Revocation ACK message.

21   Table 4-92 shows the default value of timers and also indicates the range of the recommended duration of these
22   timers.

---

[13] The timer for Registration Revocation Message sent to the HA and retransmission behavior should be per [26]

1 **Table 4-92 – Timer Values for MS Initiated PMIP4 Session Release Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T $_{FA\_Revoke\_Req}$	TBD		TBD

2 **4.8.2.4.7.1.1.2   MS Initiated PMIP4 Session Release Error Conditions**

3 This section describes error conditions associated with the MS Initiated PMIP4 Session Release procedure.

4 **4.8.2.4.7.1.1.2.1   Timer Expiry**

5 Table 4-93 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
6 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
7 should be performed as indicated in Table 4-45.

8 **Table 4-93 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T $_{FA\_Revoke\_Req}$	AnchorDPF ASN	Behave as if both *FA_Revoke_Rsp* are received. The Context information remained on PMIP4 and HA is released based on their time-out mechanism, which is implementation dependent.

9 **4.8.2.4.7.1.2   R3 Session Release – Initiated by Authenticator or AAA**
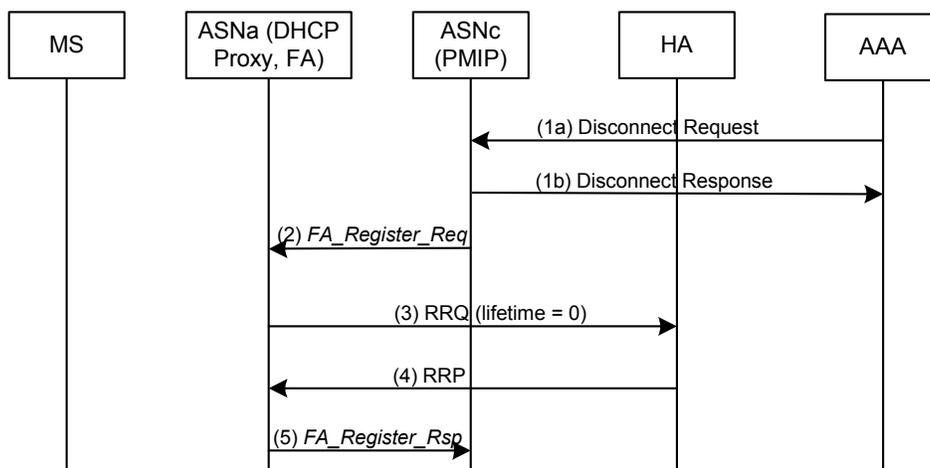
10

11 **Figure 4-63 – PMIP4 Session Release triggered by Authenticator or AAA**

12 **STEP 1**

13 The trigger can be Authenticator timeout on re-authentication or AAA initiated Disconnect.

1 **STEP 2**

2 The ASNb where the PMIP4 client resides, sends a *FA_Register_Req* with the encapsulated RRQ of lifetime=0 to
3 the ASNa where the FA resides, and a timer $T_{FA\_Register\_Req}$ is started at this point by PMIP4 client to monitor
4 *FA_Register_Rsp* message.

5 **STEP 3**

6 FA sends the RRQ with lifetime=0 to the HA.

7 **STEP 4**

8 The HA removes the binding and replies with RRP.

9 **STEP 5**

10 ASNa sends a *FA_Register_Rsp* with the encapsulated RRP to the PMIP4 client, and PMIP4 client stops
11 $T_{FA\_Register\_Request}$ once it gets *FA_Register_Rsp*.

12 **4.8.2.4.7.1.2.1   Authenticator or AAA Initiated PMIP4 Session Release Timer and Timing Consideration**

13 This section identifies the timer used in the Authenticator or AAA Initiated PMIP4 Session Release procedure.

14   • $T_{FA\_Reg\_Req}$: this timer is defined in section 4.8.2.3.7.1.1.

15 **4.8.2.4.7.1.2.2   Authenticator or AAA Initiated PMIP4 Session Release Error Conditions**

16 This section describes error conditions associated with the Authenticator or AAA Initiated PMIP4 Session Release
17 procedure.

18 **4.8.2.4.7.1.2.2.1   Timer Expiry**

19 Table 4-94 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
20 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
21 should be performed as indicated in Table 4-94.

22 **Table 4-94 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{FA\_Register\_Req}$	PMIP4 client	Behaves as if PMIP4 session has been released.

23 ## 4.8.3   Client MIPv4 R3 Mobility Management

24 The basic client MIPv4 operation SHALL be as per Mobile IP standard [15]. The following sections describe the
25 detailed stage-3 node requirements for each phase of the user's session via CMIP4.

26 The CMIP4 behavior for interworking with 3GPP2 is described in the Stage 3 Annex, WiMAX – 3GPP2
27 Interworking.

28 ### 4.8.3.1   Client MIPv4 Connection Setup Procedure

29 The basic connection setup procedure using CMIP4 is shown in stage-2, section 7.8.1.9.1. The node requirements to
30 support the connection setup are described as follows.

31 #### 4.8.3.1.1 MS Requirements

32 The Mobile IPv4 Client behavior assumes that the Mobility Stack in the MS conform to IETF standards such as
33 [15].

34 Due to the EAP based method of bootstrapping Mobility Keys, after successful Device/User Network Access
35 authentication and authorization, the Mobile IP Client SHALL have access to all the mobility keys that it requires,

such as MN-HA key to be used for CMIP4 and CMIP6 (designated MN-HA-CMIP4), associated value of SPI (SPI-CMIP4 or SPI-CMIP6 accordingly, depending on the version of MIP protocol used), and the outer NAI used during authentication.

A CMIP4 capable MS SHALL send a Mobile IPv4 RRQ to the FA after it receives an Agent Advertisement (that is received solicited or unsolicited) from the FA containing a new FA-CoA if the MS did not already request for an IP address using DHCP. Otherwise, the MS SHALL not initiate CMIP4 registration procedure once it has received an IP address from the network via DHCP. In the RRQ, the MS SHALL include an NAI extension that consists of the pseudoIdentity@realm that was used as the outer NAI during EAP based Device/User Network Access Authentication and Authorization.

The RRQ SHALL contain the MN-HA AE and MAY contain MN-FA AE. For bootstrapping of the MN-HA and MN-FA key material, refer to section 4.3.5. The Mobile IPv4 Client SHALL use MN-HA SPI set to the value of SPI-CMIP4 associated with the CMIP MN-HA Key computed from the EMSK at the successful completion of the EAP based Device/User Network Access Authentication and Authorization.

In the HoA field in the RRQ, if the MS desires a dynamic address allocation by the home agent, it SHALL include 0.0.0.0.

If MS requests for a dynamic home agent assignment, it SHALL set the HA field to either 255.255.255.255 or 0.0.0.0 (termed as ALL-ZERO-ONE-ADDR). "MS requesting dynamic home agent assignment SHALL use the MN-HA key that is derived based on ALL-ZERO-ONE-ADDR or a particular HA IPv4 address it wishes to connect for calculation of MN-HA authentication extension in the RRQ and use the MN-HA key that is derived based on assigned HA IP address in the RRP for validation of MN-HA authentication extension once the RRP with success code is received.

The Mobile IP Client MAY have access to the address of the Home Agent, the Mobile IPv4 Client SHALL set the HA field in the RRQ to this address.

Upon receiving a RRP in response to the RRQ with reply code = 0 (success), the MS SHALL use the HoA contained in the RRP as the HoA for the mobility session. In this case, the HA address contained in the RRP SHALL be treated as the assigned home agent for the session (if dynamic home agent assignment was requested).

Support for the MN-FA Challenge Extension as specified in [36] is optional.

The error handling and retransmission behavior of the MS SHALL be governed by the Mobile IPv4 standard [15].

When connected to a WiMAX network, if the MS wants to use MIPv4 it SHALL NOT invoke DHCP for IPv4 address acquisition before and after starting the Mobile IP procedures.

The scenario when the MS performs CMIP4 registration after the network performs PMIP4 procedures is not in the scope of Release 1.0.0. In other words, in Release1.0.0 once the MS sends DHCPREQUEST, it is not expected to follow it later on with MIP RRQ.

4.8.3.1.2 FA Requirements

FA and anchor DPF are always collocated. As soon as the FA (collocated with the DPF) determines that the data path (i.e., R6 for profiles A and C) is connected for a new MS for which no mobile IPv4 session exists, the FA SHALL send a series of Agent Advertisement over that data path (i.e., R6 for profiles A and C) to the MS after a configurable time period (to allow the MS to initiate either Simple IPv4 or CMIP4). The Agent Advertisement SHALL contain the FA-CoA and the supported lifetime. The FA SHALL set the MIP lifetime < RADIUS session time attribute value that the FA is configured to support. The Agent Advertisement SHALL be formatted as per [15] The FA SHALL support MIPv4 registration revocation as per [26] and the FA SHALL set the appropriate fields in the Agent Advertisement message.

The FA SHALL send Agent Advertisement under the following conditions:

   a. The DPF notifies the FA that the data path (i.e., R6 for profiles A and C) is up and the FA determines that the MS is authorized for only CMIP4 from the subscriber profile cached in the NAS (received during user/device authentication from the HAAA).

   b. The DPF in the target ASN forwards the Anchor DPF *HO_Req* received over R4 to the target FA. Note that the currently serving ASN is responsible for ensuring that the MS is a CMIP4 authorized MS and the MS

1   has an active CMIP4 session. The target FA does not perform additional MS capability checks before
2   sending Agent Advertisement.

3   c.   When solicited by the MS unless the MS has an existing IPv4 session.

4   Upon receiving the RRQ from the MS, the FA SHALL follow the [15] specification to process it.

5   If MIPv4 registration revocation is supported and if there is no alternative way to secure FA-HA communication
6   other than FA-HA AE, the FA SHALL extract the FA-HA key from the security context and append the FA-HA AE
7   in the relayed RRQ.

8   If GRE tunneling is used between the FA and the HA, the FA MAY include the GRE key extension CVSE carrying
9   its GRE-key as defined in draft-yegani-gre-key-extension-02.txt.

10   Upon receiving the RRP back from the HA, the FA SHALL forward the RRP to the MS if FA-HA AE validation is
11   successful (if FA-HA AE is used). If FA-HA AE is not used, the FA SHALL forward the RRP back to the MS.

12   In order to allow the termination of sessions by the home or visited network, the HA and the ASN SHALL support
13   MIP4 Registration Revocation ([26]) and [28].

14   The Registration Revocation message shall be either protected using an FA-HA Authentication Extension as per
15   [26] or by using another security mechanism at least as secure, and agreed upon by the home and visited domains,
16   e.g., IPsec. If an FA-HA security association is not available, or in the absence of another appropriate security
17   mechanism, the FA and HA shall silently discard any Registration Revocation messages received.

18   **4.8.3.1.3   HA Requirements**

19   The HA SHALL process Mobile IPv4 message as per [15]. Upon receiving an RRQ if the HA does not have a
20   security association for the MN, the HA SHALL issue a RADIUS Access-Request with User-Name attribute set to
21   the contents of the NAI extension received in the RRQ. After successful processing of the Access-Request, the
22   HAAA responds back to the HA with the set of attributes including the mobility keys (MN-HA, FA-HA) and
23   associated SPI values, so that the HA can validate the corresponding Authentication Extensions in the RRQ. The
24   same SPI value and the MN-HA key are used for both verifying incoming RRQs and signing outgoing RRPs by the
25   HA.

26   If the Mobile requested Dynamic HA assignment by setting the HA-IP address in the RRQ to the ALL-ZERO-ONE-
27   ADDR (NO S), then the FA simply forwards the RRQ to the HA address that it received during Device/User
28   Network Access Authentication and Authorization. In this case the HA receives the RRQ with the HA-IP address
29   set to ALL-ZERO-ONE-ADDR (NO S) in the message body and the packet is destined to its IP address. "The HA
30   SHALL indicate this to the HAAA by including the RRQ-HA-IP attribute set to the Home Agent field of the RRQ
31   in Access Request. In response to Access Request, HA will receive Access Accept with RRQ-MN-HA-KEY from
32   the HAAA that is calculated based on RRQ-HA-IP address as well as MN-HA-CMIP4 key that is calculated based
33   on HA-IP-MIP4 address. The HA SHALL use the RRQ-MN-HA-KEY for validation of MN-HA authentication
34   extension in the received RRQ and the MN-HA-CMIP4 key for deriving MN-HA authentication extension in the
35   RRP it sends to the MS. For MIP re-registration, the HA SHALL use only MN-HA-CMIP4 key for validation of
36   RRQ and deriving MN-HA authentication extension in RRP. The HAAA MAY also send to the HA the HA-IP
37   address that it sent to the FA for this MN. In this case if this address matches the HA's HA-IP address then the HA
38   SHALL process the RRQ and respond back to the MS with an RRP as normal – that is, providing the MN-HA AE
39   validation and the RRQ processing is successful.

40   If the FA-HA AE (if required) and MN-HA AE (required) validations are successful, the HA SHALL assign an HoA
41   to the MS if dynamic HoA assignment is requested (i.e. RRQ contains the HoA=0.0.0.0) and respond back to the
42   MS with a RRP indicating success. In this case, if the HoA is statically assigned for the user (NAI), the HA SHALL
43   register the mobility binding with that HoA. Authorization of the static HoA MAY require AAA transaction.

44   If the RRQ contains the GRE key extension CVSE the HA SHALL respond back to the FA with GRE key extension
45   CVSE carrying its GRE-key in the RRP.

46   If registration revocation is supported, the HA SHALL exchange the revocation support extension with the FA as
47   defined in [26]. The generic error handling requirements for the HA are as per [15].

1 **4.8.3.1.4 AAA Server Requirements**

2 "In addition to the requirements listed in section 4.8.2.1.6, if the Access Request from HA contains a RRQ-HA-IP
3 field, the HAAA SHALL derive an additional key RRQ-MN-HA-KEY using the key derivation formula for MN-
4 HA-CMIP4 in section 4.3.5.1 but with RRQ-HA-IP as the HA-IPv4 address. The HAAA SHALL send back both
5 RRQ-MN-HA-KEY and MN-HA-CMIP4 key to the HA in the Access Accept.".

6 **4.8.3.2   Client MIPv4 Session Renewal**

7 The Mobile IPv4 session SHALL be renewed by the MS based on the registration lifetime value in the RRP. The
8 processing requirements for the resulting RRQ and RRP are the same as defined in section 4.8.2.1.3.

9 **4.8.3.2.1 CMIP4 Session Renewal Procedure**

10 Same as the CMIP4 session establishment procedure described in section 4.8.3.1.

11 **4.8.3.3   Client MIPv4 CSN Anchored Mobility Handover**

12 The CSN anchored mobility event MAY be triggered by two different events:

13 • The MS incurring a handover to a target BS which requires a relocation of the FA function (CoA) due to
14 network boundary crossing or network configuration.

15 • Due to resource management decision in the ASN-GW the ASN-GW MAY force a relocation of the MIPv4
16 service to a different FA.

17 **4.8.3.3.1 MS Requirements**

18 A CMIP4 capable MS SHALL send a Mobile IPv4 RRQ to the FA after it receives an Agent Advertisement from
19 the FA containing a new FA-CoA after incurring inter BS handover. The mobile IPv4 registration requirements are
20 as per section 4.8.2.1.3.

21 **4.8.3.3.2 FA Requirements**

22 Upon receiving an Anchor DPF *HO_Req* message from the ASN Functional Entity in the serving ASN, the Target
23 FA SHALL send an Agent Advertisement to the MS as soon as the data path to the MS is established..

24 **Table 4-95 – Anchor DPF HO_Req Message**

IE	Reference	M/O	Notes
Anchor MM context	Section 5.3.2.11	M	DHCP Proxy Info, DHCP Server Info, MIPv4 Info etc

25 In response to the Anchor DPF *HO_Req* message the target FA SHALL respond to the ASN functional entity with
26 an Anchor DPF *HO_Rsp* message. The further processing of the resulting RRQ and RRP at the target FA for the
27 MS is as per section 4.8.2.1.4

28 **Table 4-96 – Anchor DPF HO_Rsp Message**

IE	Reference	M/O	Notes
R3 Operation Status	Section 5.3.2.167	M	Success or failure indication

29 After the CSN anchored handover is successfully completed the target FA function SHALL send the Context_Rpt
30 message to the anchor authenticator function. The Context_Rpt message must contain the address of the new anchor
31 DPF function. Upon receipt of the Context_Rpt message containing the address of the new anchor DPF the anchor
32 authenticator must update its notion of the location of the anchor DPF function for this MS. The anchor
33 authenticator SHALL confirm the receipt of the Context_Rpt message by sending the Context_Ack message.

4.8.3.3.3 HA Requirements

The HA SHALL process the RRQ from the MS to register its new CoA as per section 4.8.2.1.5. If registration revocation was supported and the HA exchanged revocation support extension with the FA during initial MIPv4 session setup, the HA SHALL remove the binding with CoA of the Anchor FA when it receives a registration revocation message ([26]) from the FA.

4.8.3.3.4 AAA Server Requirements

Same as section 4.8.2.1.6.

4.8.3.3.5 MS Mobility Triggered

For CMIP4 based CSN anchored Mobility Management, the MS performs Mobile IPv4 registration upon receiving an Agent Advertisement from an FA in the ASN.

4.8.3.3.6 Network Resource Optimization Triggered

When the MS disappears from the coverage area w/o performing a graceful termination of the Mobile IPv4 session at the FA and the HA, the FA MAY initiate release of zombie resources by using Registration Revocation methods as described in [26].

4.8.3.4 Client MIPv4 Session Termination

The ongoing MIPv4 session of a CMIP4 MS MAY be either terminated by the MS itself or MAY be terminated by the network based on some events happening in the network that necessitates such an action. This section defines the requirements to support the termination case.

4.8.3.4.1 MS Requirements

A CMIP4 capable MS SHALL send a Mobile IPv4 RRQ with lifetime set to 0 when it wishes to terminate the ongoing Mobile IPv4 session with the network.

Upon receiving an Agent Advertisement from the FA (with which the MS has an ongoing Mobile IPv4 session) containing sequence number = 0, the MS SHALL consider its Mobile Ipv4 session terminated by the network. Moreover, if the Agent Advertisement has the B-bit set, the MS SHALL NOT attempt to register with that FA until a later time when it receives an Agent Advertisement from that FA with B-bit unset.

4.8.3.4.2 FA Requirements

Upon receiving RRQ with lifetime set to 0, the FA SHALL relay the message to the HA. When the FA receives the corresponding RRP, indicating successful de-registration, it SHALL clear the mobility binding state for the MS. The FA SHALL forward the RRP back to the MS if the corresponding R6/R4 still exists.

The FA implementations compliant to this document SHALL support and use Mobile IPv4 Registration Revocation ([26]).

Based on what the I-bit setting in the Revocation Support Extension (sec 3.2, [26]) and the availability of R6 after registration revocation messages are exchanged with the HA, the FA MAY send an Agent Advertisement to the MS with sequence field set to 0. The FA MAY also set the B-bit in this Agent Advertisement message.

If MIP lifetime expires, FA may trigger ASN network resource release through the normal data path release procedure per policy.

4.8.3.4.3 HA Requirements

Upon receiving a RRQ with lifetime set to 0 from a registered MS, the HA SHALL remove the mobility binding for the MS and reply with a RRP as per the behavior defined in [15].

The HA implementations compliant to this document SHALL support and use Mobile IPv4 Registration Revocation ([26]).

Upon receiving a Registration Revocation from the FA for an MS, the HA SHALL tear down the mobility binding state for the MS (considering FA-HA AE validation is successful) and reply back to the FA with a Registration Revocation Acknowledgment message.

4.8.3.4.4 AAA Server Requirements

When the MS' mobility session is terminated Accounting Stop messages are received from both the HA and the NAS. In this case the Accounting Stop message SHALL contain the Terminate-Cause attribute set to TBD indicating that the session has terminated as opposed to a handover. In this case, the HAAA SHALL signal the release of all state information and in particular the Key Generator/ Key Holder SHOULD be cleared of all the keys associated with the MS.

4.8.4 Client MIP6 Mobility Management

Mobile IPv6 (MIP6) operation is specified by the IETF. The base specifications for MIP6 include RFCs [29] and [30]. As per [29] the client/host is involved in the mobility management and hence the term client MIP6 mobility is used in the context of this specification. Authentication of the MS (Mobile Station) to the HA is via the Authentication protocol ([21]) and support for hosts that use IPsec to secure the MIP6 signaling as per [30] is optional.

The MS establishes an IPv6 Initial service flow (ISF) and either acquires or auto-configures a global scope IPv6 address from the ASN [Reference ISF establishment process] .

The following sections describe the operating details of Client MIP6.

The CMIP6 implementations compliant to this specification SHALL implement the following RFCs/Drafts:

- [29]: Base MIP6 protocol
- [21]: Authentication Protocol for MIP6
- [32]: Identification Option for MIP6
- draft-ietf-mip6-hiopt-02.txt

Support for hosts complying to [30] for securing the CMIP6 messages is optional.

4.8.4.1 Client MIP6 Connection Setup Procedure

After acquiring or auto-configuring a global scope IPv6 address from the ASN, the Mobile IPv6 Client in the MS triggers the registration procedure (connection setup) with the home agent. The decision to initiate MIP6 signaling by an MS to an HA is based on local policy at the host. The following sections define the node behavior of a MIP6 MS.

The MIP6 capable MS needs information about the Home agent or Home link and/or its Home Address (HoA) in order to initiate MIP6 signaling towards the HA. The MIP6 client in the MS has to be bootstrapped with this information. The MS acquires the information required for establishing a MIP6 session via DHCPv6. Prior to the MS initiating DHCPv6, it has authenticated itself to the network via EAP. As part of the EAP transaction, the home AAA determines that the MS/user is authorized for MIP6 service and hence includes the information required to bootstrap MIP6 in the Access-Accept message which is sent to the visited AAA at the conclusion of the EAP transaction. The call flow for MIP6 bootstrapping is as shown in Figure 4-64:

1
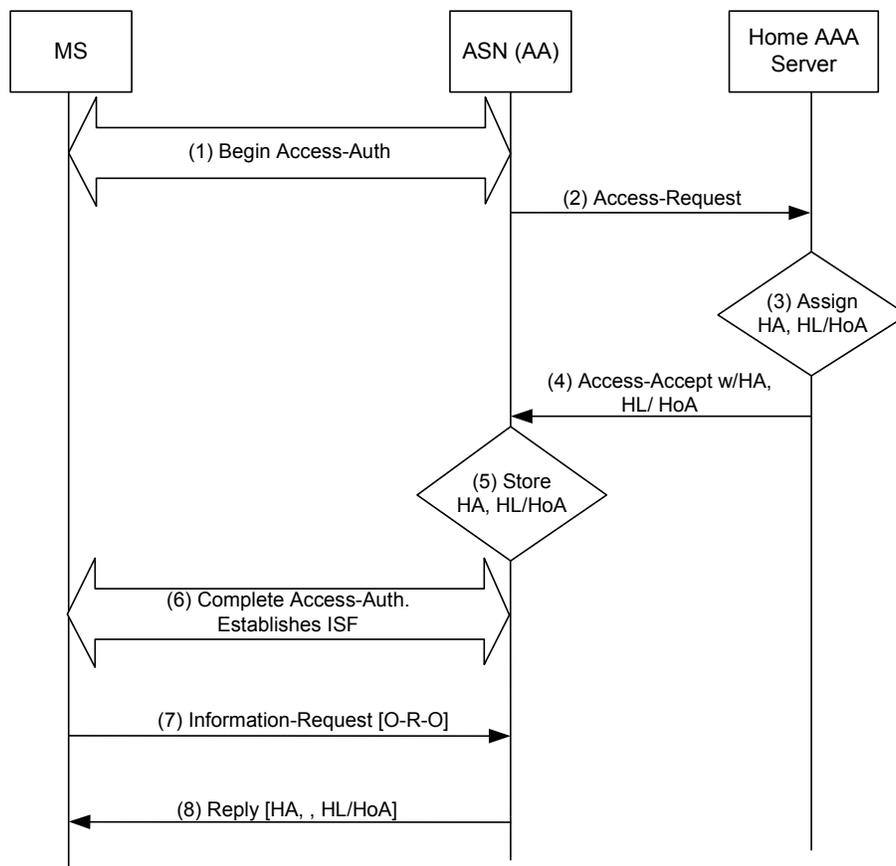
2   **Figure 4-64 – Client MIP6 Connection Setup Procedure**

3   **STEP 1**

4   The MS performs Access Authentication procedure via EAP-PKMv2.

5   **STEP 2**

6   The NAS (which is the Anchor Authenticator (AA) in the ASN) sends an Access-Request to the Home AAA server.

7   **STEP 3**

8   While performing EAP authentication and authorization the Home AAA server notes that the user is authorized for
9   MIP6 service by verifying the user's profile. The Home AAA server assigns an HA and either a HL prefix or a HoA
10   to the MS.

11   **STEP 4**

12   The Home AAA server includes this information in the following RADIUS VSA: The Assigned Home Agent info
13   in the MIP6-Home-Agent Address VSA, if HL prefix is assigned, HL prefix info in the MIP6-Home-Link Prefix
14   VSA, if the HoA is assigned, HoA info in the MIP6-Home-Address VSA.

15   **STEP 5**

16   The Anchor Authenticator in the ASN receives these MIP6 bootstrap parameters via the related VSAs from the
17   Home AAA server and stores them in the local DHCPv6 server.

1 **STEP 6**

2 The Access Authentication procedure completes successfully. The Initial Service Flow (ISF) gets established. The
3 MS configures its IPv6 stack with a link local and global address as per the basic IPv6 connection setup procedure.

4 **STEP 7**

5 The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [3736] sent to
6 the ASN.

7 **STEP 8**

8 The ASN looks up the appropriate cached record based on the Path_ID over which the DHCPv6 information request
9 is received and replies back to the MS [RFC 3736] with the options that were requested and attaches the MIP6
10 bootstrap information options as per draft-ietf-mip6-hiopt-02.txt.

11 ### 4.8.4.1.1 MS/CMIP6 Client Operation

12 MIP6 is an integral part of the IPv6 stack in the MS. The terms MS and CMIP6 Client are used interchangeably in
13 this document. The CMIP6 Client SHALL initiate the Mobile IPv6 registration procedure as part of the connection
14 setup as soon as the MS configures (either via DHCPv6 or via auto-configuration) a global scope IPv6 address when
15 attached to the ASN. Local policy at the MS acts as the trigger for initiating the MIP6 binding update following the
16 care-of-address configuration. The CMIP6 Client SHALL use the address obtained or auto-configured in the
17 attached ASN as the Care-of Address (CoA) in the MIP6 Binding Update.

18 The MS discovers the address of the HA, its own HoA or HL prefix by including the option codes defined in [draft-
19 jang-mip6-hiopt-02.txt] in the DHCP Information-Request message which is sent by the MS to the DHCPv6 server
20 in the ASN. In the DHCP Information Request, the MS may include the Home Network Identifier Option to identify
21 the home network from which it wants to receive the bootstrap info. If used, the MS SHALL set the id-type to 1 in
22 this option and include the @realm part of it's NAI in the Home Network Identifier field.

23 After obtaining the HA address, via the DHCP response the CMIP6 Client SHALL send a BU (Binding Update) to
24 the HA to register it's binding with the CoA. The BU SHALL be protected by the Mobility Message Authentication
25 Option as defined in [21]. The MS implementations conformant to this specification SHALL only require and use
26 the MN-HA Mobility Message Authentication Option in all messages. An even-valued MN-HA SPI SHALL be
27 used. The procedure to derive the MN-HA key to compute MN-HA Mobility Message Authentication Option is
28 described in section 4.3.5.2. The MS SHALL include Mobile Node Identifier Option for Mobile IPv6 ([32]) in all
29 BUs. The Mobile Node SHALL use the same pseudoIdentity, i.e. pseudoIdentity@Realm that was used during
30 Device/User Network Access Authentication and Authorization procedure at the ASN.

31 Note: Even-valued SPIs are also used for CMIP6. The reason for this is to avoid backwards-compatibility issues
32   in future releases where, in addition to PMIP4, PMIP6 may be supported.

33 An MS may establish an IPsec SA with its HA as per [30] and send the Binding update via this SA. Securing
34 binding update/Ack messages with an IPsec SA is optional in this release. It should be noted that an MS uses either
35 [21] or [30] for securing the MIP6 messages and not both.

36 If the MS also received the HoA in the DHCP Reply message, the MS SHALL set the HoA field in the BU to the
37 received HoA.

38 If the MS did not receive the HoA in the DHCP Reply message but it received the HL prefix info, the MS can
39 perform stateless address auto-configuration of the HoA from the received HL prefix as per the autoconfiguration
40 process described in [34]. In this case, the MS SHALL set the HoA field in the BU to the auto-configured HoA.

41 If the MS did not receive the HoA and HL prefix in the DHCP Reply message, the MS SHALL either set the HoA
42 field to 0::0 (unspecified address) if it wishes that the HA assign it the whole 128-bit address or it can include a /64
43 Interface ID (IID) in the HoA field. In the latter case, the MS is requesting the HA to assign a HoA using the IID
44 supplied by the MS. The MS SHALL perform BAck processing as per [21]. The MIP6 Route optimization feature
45 requires the existence of an IPsec SA between the MS and the HA. If the Authentication protocol ([21]) is used for
46 securing the registration messages, then route optimization as described in [29]   cannot be performed. Route

1 optimization, in the scenario when the MS is using [21] for securing the CMIP6 registration messages, is for further
2 study.

4.8.4.1.2 NAS and DHCPv6 Proxy Requirements

4 The NAS in the ASN, is also the Anchor Authenticator and should cache the Mobile IPv6 bootstrap parameters that
5 are received from the Home AAA server at the time of Device/User Network Access Authentication and
6 Authorization procedure. Upon receiving DHCPv6 information request from the MS the DHCPv6 proxy SHALL
7 reply to the MS with the Home Network Information option with the MIP6 bootstrap info that was received from the
8 AAA server. To identify the set of information to convey to the MS, the DHCPv6 proxy SHALL use the R6
9 Path_ID to determine the set of cached parameters that is relevant to the MS. The DHCPv6 proxy may also receive
10 the Home Network Identifier Option [ref: draft-jang-mip6-hiopt-02.txt] in the DHCPv6 Information Request.
11 However, the DHCPv6 proxy is not required to process this information. To convey the Home Agent address to the
12 MS, the DHCPv6 proxy SHALL set the hainfo-type to 1 and the Home Network Information field to the Complete
13 IPv6 address of the home agent in the Home Network Information Option. To indicate the received HL prefix, the
14 DHCPv6 proxy SHALL set the hainfo-type to 0 and the Home Network Information field to Home subnet prefix in
15 the Home Network Information Option. If both HA and HL prefix information need to be conveyed to the MS, the
16 DHCPv6 proxy SHALL include two Home Network Information Options with fields set as described above.

4.8.4.1.3 HA Requirements

18 The HA SHALL support Mobile IPv6 operation with Base Mobile IPv6 ([29]) and Authentication Protocol for
19 Mobile IPv6 ([21]). The HA should also support the hosts that use IPsec to secure the binding update/Ack messages
20 as per [30]. Upon receiving a BU from a MS, the HA SHALL perform validation of MN-HA Mobility Message
21 Authentication Option based on the identification of the user from the NAI contained in the BU in the Mobile Node
22 Identifier Option ([32]) and the corresponding MN-HA key. The HA acquires the MN-HA key from the AAA by
23 sending a RADIUS Access Request as shown in *Table X1*. The User-Name attribute value is obtained from the NAI
24 contained in the BU in the Mobile Identifier Option ([32]). This NAI SHALL be the same NAI used as the outer
25 NAI during Device/User Network Access Authentication and Authorization procedures. The HA SHALL also
26 include the following attributes: the IPv6 address of the HA so that the HAAA can validate that the correct values
27 have been used. The HA SHALL sign the packet using Message-Authenticator as specified in [8].

28 If the HA requires the Chargeable User Identity (CUI) attribute, it SHALL include the CUI attribute set to NULL in
29 the Access-Request packets.

30 The HA SHALL include the WiMAX capability attribute indicating its capabilities to the HAAA.

31 Upon successful processing by the HAAA, the HA receives a RADIUS Access-Accept packet as shown in Table
32 5-6. The HA SHALL validate the Message Authenticator as per the procedures defined in [8]. If the packet does not
33 contain the Message-Authenticator, the HA SHALL silently discard the packet. If the packet contains the Message
34 Authenticator but the computed value does not match the Message Authenticator, then the HA SHALL silently
35 discard the packet. If the HA discards the RADIUS Access-Accept packet it should also discard the BU message. If
36 the validation is successful, then the HA should decrypt the MN-HA attribute using the procedures defined in [35]
37 section 3.5.

38 Once the MN-HA key is decrypted, the HA can validated the MN-HA Auth-AE. If the MN-HA Auth-AE is verified
39 successfully, the HA SHALL create a security association with the MN storing the MN-HA key locally. The HA
40 SHALL use the MN-HA key to compute MN-HA AE for all subsequent messages. Once the MN-HA AE is
41 validated the HA SHALL continue to process the BU as prescribed below:

42 • If the MN-HA Auth-AE fails authentication, the HA SHALL silently discard the BU.

43 • If the RADIUS Access-Accept message contains MIP-Authorization-Status set to False, then MIP6 service
44 is not authorized for the subscriber. The HA SHALL construct a BA with status set to Administratively
45 prohibited (129). The BA SHALL include the MN-HA Auth-AE which is signed by the MN-HA key
46 received in the RADIUS Access-Accept.

47 • If the HA receives the CUI attribute in the Access-Accept packet, it SHALL include it in all RADIUS
48 accounting packets only if it supports accounting message as indicated by the WiMAX Capability attribute
49 sent in the Access-Request message, and if accounting messages were selected by the RADIUS server in

1 the WIMAX-Capability attribute. Similarly, if accounting is enabled and the Class attribute is received in
2 the Access-Accept message, the HA SHALL include the Class attribute in all accounting messages.

3 • If the HoA contained in the BU is unknown to the HA but the prefix of the HoA matches one of the
4 prefixes that the HA supports for HoA construction, the HA will assume that the MS discovered the HL
5 prefix info via bootstrapping. In this case, the HA may perform a local check in the local repository of
6 Binding Cache Entries (BCEs) to make sure that the address (HoA) does not clash with that of another
7 mobility binding. The HA SHALL perform the uniqueness validation of the assigned or requested HoA as
8 per [29]. If the uniqueness of the HoA validation succeeds, the HA admits the binding and replies to the
9 MS with a BA. The BA is protected by the MN-HA Mobility Message Authentication Option.

10 • If the HoA contained in the BU contains 0::0 (unspecified address) or EUI-64/IID the HA SHALL
11 consider this as a request for a dynamic HoA assignment request from the MS. In the former case, the HA
12 SHALL assign a 128-bit IPv6 address (HoA) from its local repository for the MS. In the latter case, the HA
13 SHALL auto-configure a HoA with the received IID and a shared /64 prefix. In this document it is assumed
14 that the /64 prefix is solely owned by the HA (i.e. no other HA owns and uses that prefix). HA SHALL
15 make sure by checking in the local repository of BCEs that the auto-configured HoA does not clash with
16 another HoA that is being used by some other user. If for some reason the HA finds a clash, the HA
17 SHALL use either a globally unique /64 prefix to auto-configure the HoA or it SHALL use a shared /64
18 prefix to do the same. In the latter case, the HA SHALL again perform the BCE check to detect any clash.
19 When the HA determines that the HoA assigned or auto-configured for the MS is unique, the HA SHALL
20 admit the mobility binding for the MS with that HoA.

21 • If the HA receives Prepaid attributes in the RADIUS Access-Accept packet then it SHALL proceed to
22 perform the prepaid procedures as specified in section 4.4.3.3.

23 • If the HA receives Hot-lining attributes in the RADIUS Access-Accept packet then it SHALL proceed to
24 perform the hot-lining procedures as specified in section 4.4.3.5.

25 • If the HA supports accounting and the RADIUS server requested accounting for this user, the HA SHALL
26 send a RADIUS Accounting-Request Start with Session Begin set to TRUE as described in the Accounting
27 session indicating that the Session has started.

28 Given the particular (HA) deployment assumptions for WiMAX Rel.1 the MS is always away from its home IP link
29 and hence the HA is in a virtual home.

4.8.4.1.4 AAA Requirements and Behavior

31 The HA interfaces with the HAAA server in the CSN.

32 During Device/User Network Access Authentication and Authorization procedures, the HAAA sends MIP6
33 bootstrap information to the ASN (NAS and DHCPv6 Proxy) as specified in (REF Network entry procedure)

34 When the HA receives a BU from the MS, the HA constructs a RADIUS Access Request message to fetch the MN-
35 HA key which is needed for authenticating the BU. The Access-Request packet is shown in Table 5-6.

36 The HAAA should validate the Message-Authenticator in the RADIUS Access-Request packet as per procedures
37 defined in [8]. If the message does not contain the Message Authenticator, or if the Message-Authenticator
38 validation fails, then the HAAA SHALL silently discard the packet.

39 The User-Name AVP SHALL contain the PseudoIdentity@realm that was used during Device/User Network
40 Access Authentication and Authorization procedures. The AAA SHALL locate the PseudoIdentity and ensure that
41 it matches an internal identity. If PseudoIdentity cannot be found then the HAAA SHALL reply back with an
42 Access-Reject with the error code indicating missing User-Name AVP.

43 If the pseudo Identity is found then the HAAA SHALL reply with an Access-Accept packet as shown in *Table xx2*
44 containing the MN-HA encrypted using the procedures defined in [35]] section 3.5. The HAAA SHALL include the
45 Message-Authenticator computed according to [8].

46 If the HAAA determines that the user is not authorized for MIP6 then it SHALL set the value of the MIP-
47 Authorization-Status to False. Otherwise if the user is authorized for MIP6 service, the HAAA SHALL set the MIP-
48 Authorization-Status to True.

1 If the Access-Request packet contains the CUI attribute set to NULL, then the HAAA SHALL also include the CUI
2 computed using the procedures defined in section 4.4.3 in the Access-Accept packet.

3 If the User is a prepaid user and prepaid is to be performed at the HA (providing the HA indicated it supports
4 Prepaid Capabilities in the WiMAX Capability Attribute), then the HAAA SHALL include prepaid attributes in the
5 Access-Accept packet as specified in section 4.4.3.3.

6 If the MS is to be hot-lined, and the hot-lining is to be performed at the HA (provided the HA is capable of
7 supporting hot-lining as indicated in the WiMAX Capabilities Attribute), then the HAAA SHALL include the hot-
8 lining attributes as specified in section 4.4.3.5.

9 **4.8.4.2   MIP6 Inter Access Router (AR) Handovers**

10 An ongoing session by an MS that is using CMIP6 may incur an inter Access Router (NAS) handover. This may
11 happen due to the MS incurring handover to a BS that has connectivity to a new Access Router or the serving ASN
12 Functional Entity may decide to force a handover due to resource management reason or administrative reasons. The
13 following sections detail the operation of such handovers.

14 **4.8.4.2.1 MS/ CMIP6 Client Operation**

15 The MS/ CMIP6 Client SHALL reset its MIP6 binding with a CoA as soon as the MS receives a new Router
16 Advertisement from a new Access Router containing a prefix other than the one received in the router advertisement
17 which was used for address autoconfiguration. This may either happen over an existing over-the-air link (resource
18 management case) or it may happen due to change of the over-the-air link (handover). In either case, the MS
19 SHALL perform IPv6 connectivity negotiation as defined in section 4.11.3. In case of stateful IPv6 address
20 configuration scenario for CoA with DHCPv6, the MS won't be able to send and receive any data unless it
21 reconfigures the IPv6 stack with a new CoA via DHCPv6. This is because the target AR may not be able to support
22 the CoA that the MS received while being served by the old AR. DHCPv6 based forced handover is not supported in
23 this document.

24 Upon configuring a new CoA, the MS SHALL perform Mobile IPv6 BU/BA procedures. However, since it is an
25 ongoing Mobile IPv6 session, the MS does not need to acquire the MIP6 bootstrap information from the target NAS.
26 Also, the MS SHALL use the existing HoA and HA in the BU to update the CoA with the HA.

27 **4.8.4.2.2 AR/NAS and DHCPv6 Proxy Operation**

28 The target AR (target ASN) may receive *Anchor_DPF_HO_Req* from an ASN Functional Entity to trigger a forced
29 or regular handover.

30 Subsequently, the target AR SHALL send a RA to the MS to re-configure its CoA (if stateless auto-configuration of
31 CoA is used in the ASN). It is assumed that the target AR has received the MIP6 bootstrap information from the
32 Serving AR along with other state information via the context transfer procedure. The Target AR SHALL perform
33 the same functions as described in section 5.6.3.1.2 to help the MS bootstrap the MIP6 parameters in case, the MS'
34 DHCPv6 Client requests for such info.

35 Upon successful completion of MIP6 registration, the target AR SHALL send an *Anchor_DPF_HO_Rsp* message to
36 the ASN functional entity to complete the handover procedure and update the ASN functional entity with new
37 mobility information.

38 After the CSN anchored handover is successfully completed the target AR function SHALL send the Context_Rpt
39 message to the anchor authenticator function. The Context_Rpt message must contain the address of the new anchor
40 DPF function. Upon receipt of the Context_Rpt message containing the address of the new anchor DPF the
41 authenticator must update its notion of the location of the anchor DPF function for this MS. The anchor
42 authenticator SHALL confirm the receipt of the Context_Rpt message by sending the Context_Ack message.

43 **4.8.4.2.3 HA Behavior**

44 The HA SHALL process the BU from the MS with a new CoA when the associated mobility binding with the old
45 CoA has not expired. The HA SHALL perform the BU validation as per section 5.6.3.1.3. If the BU processing is
46 successful, the HA SHALL update the mobility binding with the new CoA information. Note that in this case, the
47 HoA remains the same as the ongoing MIP6 session. The HA may adjust the MIP6 session lifetime to a different

1 value (i.e. HA may consider this as a MIP6 session renewal) or the HA may respond back to the MS with remaining
2 lifetime of the ongoing MIP6 session. .

3 If the HA supports accounting and the RADIUS server requested accounting for this user, the HA SHALL send a
4 RADIUS Accounting-Request Stop with Session–Continue set to True followed by an RADIUS Accounting-
5 Request Start Session Begin set to False indicating that the Session has started, as described in section 4.4.3.4.

6 **4.8.4.2.4 AAA Requirements**

7 None.

8 **4.8.4.3 MIP6 Session Renewal**

9 The MIP6 MS performs Mobile IPv6 session renewal before expiry of the session lifetime if it wishes to continue
10 the mobility session by sending a binding update to its HA.

11 **4.8.4.3.1 MS/ CMIP6 Client Requirements**

12 The MS SHALL send a Binding Update to the HA if it wishes to continue the IPv6 mobility session. The MS
13 SHALL construct the Binding Update as per the details described in 5.6.3.2.1

14 **4.8.4.3.2 AR/ and DHCPv6 Proxy Requirements**

15 The AR (ASN) has no requirements on session renewal.

16 **4.8.4.3.3 HA Requirements**

17 The HA SHALL renew the mobility session upon successful processing of the Binding Update received from the
18 MS before expiry of the mobility session lifetime. In response, the HA SHALL send back a BA to the MS following
19 the procedure described in 5.6.3.2.3.

20 **4.8.4.3.4 AAA Requirements**

21 None.

22 **4.8.4.4 MIP6 Session Termination**

23 The IPv6 mobility session can be terminated as follows:

24   a. By the MS by sending a Binding Update with lifetime set to 0.

25   b. By the ASN functional entity upon detection of loss of radio link.

26 The following sections describe the requirements for each node for MIP6 session termination.

27 **4.8.4.4.1 MS/ CMIP6 Client Requirements**

28 The MS SHALL send a BU to the HA with lifetime set to 0 if it wishes to terminate the IPv6 mobility session. The
29 MS SHALL construct the BU as per the details described in 5.6.3.2.1. After receiving the corresponding BA, the
30 MS SHALL tear down the IPv6 session if MIP6 was the only session for the MS.

31 **4.8.4.4.2 AR/NAS and DHCPv6 Proxy Requirements**

32 Upon receiving an R3 *Session_Release_Req* from an ASN Functional Entity, the AR (the Serving DPF) SHALL
33 initiate termination of the corresponding link (R6) for the MS. The AR (the serving DPF) may be able to inspect the
34 BU/BAs that the MS exchanges with the HA.

35 In this case, the AR SHALL send a R3 *Session_Release_Req* to the ASN-functional entity and initiate teardown of
36 R6 for a MS if the MS received a BA with lifetime 0 and a R6 still exists after a configurable amount of time has
37 elapsed.

38 **4.8.4.4.3 HA Requirements**

39 The HA SHALL teardown the mobility session upon successful processing of the BU received from the MS with
40 lifetime = 0. In response, the HA SHALL send back a BA to the MS following the procedure described in 5.6.3.2.3.
41 In the BA the HA SHALL set the lifetime to 0.

1 If the HA supports accounting and the RADIUS server requested accounting for this user, the HA SHALL send a
2 RADIUS Accounting-Request Stop with Session-Continue set to FALSE and RADIUS Terminate-Cause set to TBD
3 indicating that the Session has started, as described in section 4.4.3.4.

4 #### 4.8.4.4.4 AAA Requirements

5 Upon receiving Accounting Request Stop for MIP6, the HAAA SHALL clear the MIP6 state of the user.

6 ## 4.9 Radio Resource Management

7 ### 4.9.1 Introduction

8 RRM is a function performed by the ASNs in a WiMAX Network, aiming at increasing the radio resource usage
9 efficiency. RRM introduces a concept of Radio Resource Agent (RRA) and Radio Resource Controller (RRC)
10 functional elements and signaling between RRA and RRC and between RRC and RRC (see [stage 2] section 7.7 for
11 more details on RRA and RRC functional entities and their respective responsibilities).

12 If RRM is supported, then ASN SHALL have at least one RRC. Depending on ASN Profile, an RRC may be located
13 in an ASN GW (as in Profile A) or in a BS (as in Profile C). In Profile B, the RRC location in the ASN is not
14 specified. The RRA is always located in the BS. See section 4.9.2 and Stage 2 Part 2 section 7.9 for details on RRM
15 reference model.

16 Implementation of RRM is optional. This is possible because

17 • Many RRM tasks, e.g. providing assistance for Service Flow Admission Control, are executed
18   autonomously and locally in each BS without any interaction to other RRM Functional Entities in the ASN.

19 • Some RRM related signaling is implicitly included in signaling between other ASN functions, as for
20   example:

21   − Handover function, e.g. using *HO_Req* and *HO_Rsp* to evaluate the spare capacity of candidate Target
22   BSs, and

23   − QoS Function, e.g. SF handling using *RR_Req* and *RR-Rsp*.

24 When RRC is not implemented, then also RRA concept and requirements do not apply, i.e. are informative only.

25 ### 4.9.2 RRM Primitives and their Mapping to Reference Points

26 As specified in Stage 2 section 7.9, there are four RRM procedures, involving seven RRM primitives. These
27 primitives MAY be used on references points R6 or R4. The mapping of these primitives to R6 or R4 depends on
28 the applicable ASN Profile.

29 In Profile A, RRC is in ASN-GW and controls its associated RRAs in the BSs.
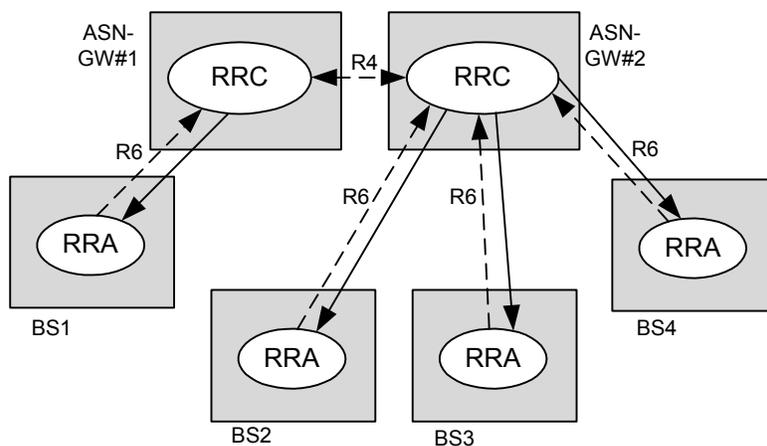
30

31 **Figure 4-65 – RRAs Resident in BS and RRC Resident in ASN-GW**

1 Profile B is a closed system and can be described as an ASN where R6 interface is not exposed for interoperability.
2 The RRM procedures mentioned between two neighboring Profile B ASNs are used over R4 reference point. For a
3 Profile B, any required inter-working with a neighboring BS belonging to profile A or C can only be facilitated over
4 the R4 reference point.

5 In Profile C, each BS has its own RRC function which controls its local RRA function as well as communicates to
6 its neighboring RRCs in other BSs. Since for this release this RRC-RRC communication can't go directly from BS
7 to BS, it SHALL be relayed via the ASN-GW (or ASN-GWs). For that purpose, it SHALL be assumed that there is
8 an "RRC Relay" function in the ASN-GW (see [stage 2] section 7.7 for more details on RRC Relay). Use of the
9 RRC Relay function allows for inter-profile RRM signaling communication between ASNs of all Profiles A, B and
10 C.

11
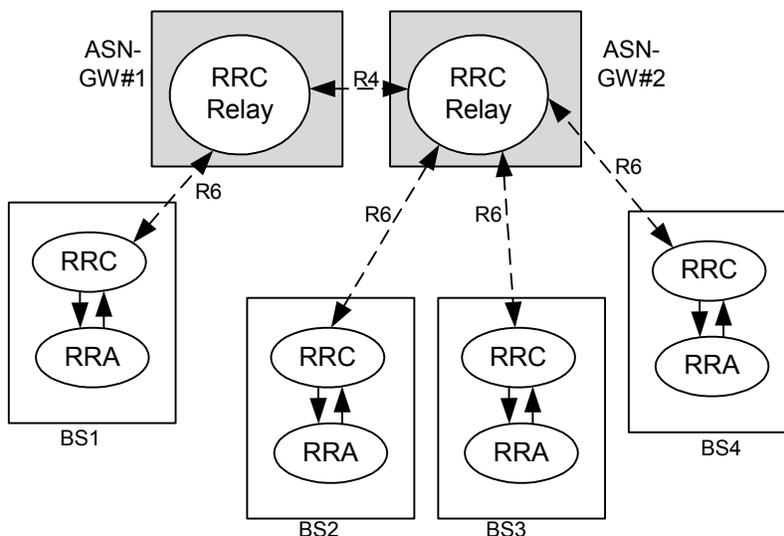
12 **Figure 4-66 – RRC-RRC Communication on R6 in Profile C**

13 The mapping of RRM primitives to R6 and R4 is shown in Table 4-97.

14 **Table 4-97 – RRM Procedures, Messages, Mapping to Reference Points**

RRM Primitives	Communication Peers	Profile A	Profile B	Profile C	Inter-ASN (profile independent)
R4/R6 Per-BS *Spare_Capacity_Req* and *Spare_Capacity_Rpt*	RRC – RRC	R4	R4	R4 and R6	R4
	RRC – RRA	R6	Not exposed for intra ASN. Mapped over R4 for inter ASN	None (BS internal)	None (RRC-RRA is ASN internal)
R6 *Neighbor_BS_Resource_Status_Update*	RRC – RRA	R6	Not exposed for intra ASN. Mapped	None (BS internal)	None (RRC-RRA is ASN internal)

RRM Primitives	Communication Peers	Profile A	Profile B	Profile C	Inter-ASN (profile independent)
			over R4 for inter ASN		
R6 Per-MS *PHY_Parameters_Req* and *PHY_Parameters_Report*	RRC – RRA	R6	Not exposed for intra ASN. Mapped over R4 for inter ASN	None (BS internal)	None (RRC-RRA is ASN internal)
R4/R6 Per-BS *Radio_Config_Update_Req* and *Radio_Config_Update_Rpt*	RRC – RRC	R4	R4	R4 and R6	R4
	RRC – RRA	R6	Not exposed	None (BS internal)	None (RRC-RRA is ASN internal)

1 Table 4-97 reveals:

2 • RRC- RRA communication (which involves all RRM primitives) becomes visible only in Profile A where
3 RRC is in ASN GW, so RRC-RRA goes over R6. In Profiles B and C this communication is either internal
4 or not over an exposed R6 interface.

5 • RRC-RRC communication (which involves two RRM primitives: Per-BS Spare Capacity req/report only)
6 exists on R4 in Profiles A, B and C; so this allows for inter-ASN RRM communication in a profile
7 independent way, where the involved ASNs MAY be any Profile, A, B, or C. - Note that in Profile C, there
8 is not a full RRC in ASN GW but just an "RRC Relay" function.

9 R6 signaling is specified in sections 7.1.1 for Profile A and 7.3.2 for Profile C respectively.

10 R4 signaling is specified in the sequel.

11 Note: For support of Association levels 1 and 2 as specified in [802.16e-2005], section 6.3.22.1.3, additional RRM
12 procedures – or HO preparation procedures - may be required in subsequent releases.

13 4.9.3 Inter-ASN RRM Signaling (profile independent)

14 This is signaling on R4. As can be seen from Table 4-97 above, R4 signaling involves RRC-RRC communication.
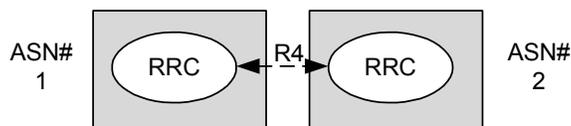
15

16 Figure 4-67 – Inter-ASN RRM Communication is RRC to RRC Communication

17 Note: A similar figure occurs for intra-ASN R4 communication; two ASN GWs within a single ASN communicate
18 via R4; from RRM view, this is RRC-RRC communication like on inter-ASN R4.

19 As shown Table 4-97, R4 RRM signaling includes the Per-BS Spare Capacity Reporting procedure and the Per-BS
20 Radio Configuration Reporting procedure.

21 Any other RRM procedures and primitives are not applicable on R4.

1 **4.9.3.1   Per-BS Spare Capacity Reporting Procedure**

2 On the R4 reference point between two ASNs, this procedure MAY be used by a Serving ASN to retrieve
3 information from a neighboring ASN about the current spare capacity of any Base Station in the neighboring ASN.
4 This information can be used by Serving ASN for any purpose, in particular for helping in decisions on:

5 • Triggering a network initiated HO for the purpose of load balancing between the Base Stations within a
6 network involving more than one ASN;

7 • Processing an MS initiated *HO_Req*: Modifying (pruning or extending) the set of candidate Target BSs
8 (TBSs) to which to forward the *HO_Req*.

9
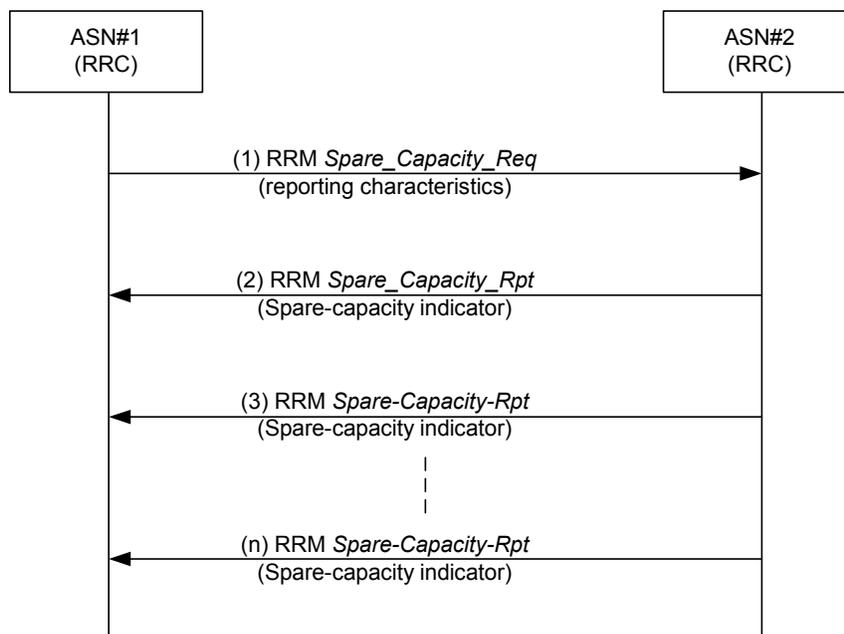
10 **Figure 4-68 – Per-BS Spare Capacity Reporting Procedure**

11 **STEP 1**

12 ASN#1 sends an RRM R4 *Spare_Capacity_Req* to ASN#2, requesting it to indicate the available radio resources of
13 a specific BS once, or periodically, or event driven.

14 If the optional reporting characteristics field is not included, then the *Spare_Capacity_Rpt* SHALL be sent only once
15 by the reporting entity.

16 In the *Spare_Capacity_Req* message, more than one of the bits in the "Reporting characteristics" field may be set to
17 1; in this case, the *Spare_Capacity_Rpt* SHALL be sent whenever any of the corresponding multiple event occurs.

18 **STEP 2, 3, …, n**

19 Reporting RRC sends RRM R4 *Spare_Capacity_Rpt* to Requesting RRC, either in direct response to the Request, or
20 subsequently in response to predefined events.

21 If the *Spare_Capacity_Req* includes multiple events in the reporting characteristics, then the *Spare_Capacity_Rpt*
22 can include this attribute to indicate which event triggered the report by setting the corresponding bit position in the
23 attribute.

24 **4.9.3.1.1 R4 Messages for Per-BS Capacity Reporting Procedures**

25 This section provides the message definitions for the R4 messages in support of the Per-BS Spare Capacity
26 Reporting Procedure. See also sections 5.2.6.6 and 5.3 for message and TLV definitions.

1   **Table 4-98 – RRM R4 Spare_Capacity_Req**

IE	Reference	M/O	Notes
RRM Spare Capacity Report Type	Section 5.3.2.164	M	
BS ID (one or more)	Section 5.3.2.25	M	Identifier of the BS whose Spare Capacity SHALL be reported. Multiple BS ID TLVs MAY be included.
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. If the optional reporting characteristics field is not included, then the *Spare_Capacity_Report* SHALL be sent only once by the reporting entity. – TLV may be included based on local RRC policy. Decision to include this TLV is implementation specific.
RRM Averaging Time T	Section 5.3.2.162	O	The Time T is used by BS (RRA) as the measurement interval for producing the information requested by RRC. – If omitted, the BS SHALL apply a default value.
RRM Reporting Period P	Section 5.3.2.163	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
RRM Absolute Threshold Value J	Section 5.3.2.163	O	The threshold value J is used by BS (RRA) as the absolute threshold for reporting.
RRM Relative Threshold RT	Section 5.3.2.161	O	The threshold value RT is used by BS (RRA) to keep track of the threshold from the last measurement period.

2   **Table 4-99 – RRM R4 Spare_Capacity_Rpt**

IE	Reference	M/O	Notes
RRM Spare Capacity Report Type	Section 5.3.2.164	M	
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates the reason for this report.
RRM BS Info	Section 5.3.2.159	M	
>BS ID	Section 5.3.2.25	M	
>Available Radio Resource DL	Section 5.3.2.22	M	This TLV SHALL be omitted if the Failure Indication TLV is included.

IE	Reference	M/O	Notes
>Total Slots DL	Section 5.3.2.191	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Available Radio Resource UL	Section 5.3.2.23	M	This TLV SHALL be omitted if the Failure Indication TLV is included.
>Total Slots UL	Section 5.3.2.192	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Radio Resource Fluctuation	Section 5.3.2.142	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>DCD Configuration Change Count	Section 5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>UCD Configuration Change Count	Section 5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
Failure Indication	Section 5.3.2.69	O	"Failure Indication" is to be used for exceptional cases; e.g., the indicated BS ID does not exist, RRC cannot route the request to the indicated BS ID, the indicated BS is out of service for the time being. Error Code 33 = BS out of service.

1

2   **4.9.3.2   Per-BS Radio Configuration Update Procedure**

3   On the R4 reference point between two ASNs, this procedure MAY be used by an ASN#1(RRC) to request a report
4   on some critical radio resource configuration parameters from ASN#2(RRC), such as DCD, UCD burst profile
5   changes at a specific BS.
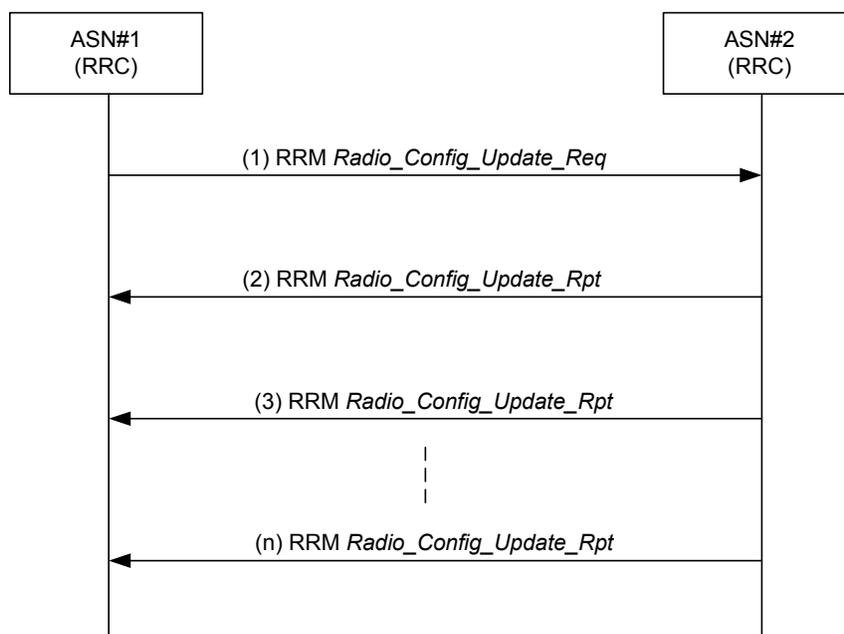
6

7   **Figure 4-69 – Per-BS Radio Configuration Reporting Procedure**

1   **STEP 1**

2   ASN#1 sends an RRM R4 *Radio_Config_Update_Req* to ASN#2, requesting it to indicate the DCD/UCD settings of
3   a specific BS once, or periodically, or event driven.

4   **STEP 2, 3, …, n**

5   ASN#2 sends RRM R4 *Radio_Config_Update_Rpt* to ASN#1, either in direct response to the Request, or
6   subsequently in response to predefined events.

7   **4.9.3.2.1 R4 Messages for Per-BS Radio Configuration Update Procedure**

8   This section provides the message definitions for the R4 messages in support of the Per-BS Radio Configuration
9   Update Procedure. See also section 5 for message and TLV definitions.

10   **Table 4-100 – R4 RRM Radio_Config_Update_Req**

IE	Reference	M/O	Notes
BS ID (one or more)	Section 5.3.2.25	M	Identifier of the BSs whose configuration parameters SHALL be reported. Multiple BS ID TLVs MAY be included.
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. In this message, only Bit#0 (periodic reporting) and Bit#1 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset. If *Radio_Config_Update_Rpt* needs to be sent based on multiple events, then the corresponding bits have to be set to 1. If the optional reporting characteristics field is not specified, then the *Radio_Config_Update_Rpt* SHALL be sent only once. – This TLV is included based on local RRC policy. Decision to include this TLV is implementation specific.
RRM Reporting Period P	Section 5.3.2.163	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.

11

12   **Table 4-101 – R4 RRM Radio_Config_Update_Rpt**

IE	Reference	M/O	Notes
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates the reason for this report. If the *Radio_Config_Update_Req* includes multiple events in the reporting characteristics, then the *Radio_Config_Update_Rpt* can include this attribute to indicate which event triggered the report by

IE	Reference	M/O	Notes
			setting the corresponding bit position in the attribute. In this message, only Bit#0 (periodic reporting) and Bit#1 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset.
RRM BS Info	Section 5.3.2.159	M	Composed TLV including BS related parameters. At least one of the optional parameters within "RRM BS Info" SHALL be included in the message.
>BS ID	Section 5.3.2.25	M	
>DCD Configuration Change Count	Section 5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>UCD Configuration Change Count	Section 5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Full DCD Setting	Section 5.3.2.72	O	This TLV may be used only while DCD configuration change count is presented. The DCD_settings is a TLV value that encapsulates the DCD message (excluding the generic MAC header and CRC) that the BS will send out in R1 with the new DCD change count.
>Full UCD Setting	Section 5.3.2.73	O	This TLV may be used only while UCD configuration change count is presented. The UCD_settings is a TLV value that encapsulates the UCD message (excluding the generic MAC header and CRC) that the BS will send out in R1 with the new UCD change count.
Failure Indication	Section 5.3.2.69	O	"Failure Indication" is to be used for exceptional cases; e.g., the indicated BS ID does not exist, RRC cannot route the request to the indicated BS ID, the indicated BS is out of service for the time being.

4.10 Paging and Idle-Mode MS Operation

4.10.1 Introduction

The control plane protocols and procedures for Idle mode and paging are described in section 7.10 of the Stage 2 specification.

The key operations and procedures are:

- Location update
- Paging operation
- Exit Idle mode
- Enter Idle mode

In this section we describe the details of the call flows and the associated messages. For detailed message and TLV formats refer to sections 5.2 and 5.3.

4.10.2 Location Update

The MS SHALL perform the Location Update procedure when it meets the LU conditions as specified in the IEEE STd 802.16e specification. The MS SHALL use one of two processes for Location Update: Secure Location Update or Unsecure Location Update. An Un-Secure Location Update process is performed when MS and BS do not share a

1   valid security context (means that BS is not able to receive a valid AK (e.g., MS crossed Mobility Domain
2   boundaries or PMK has expired) or when the BS otherwise elects to direct the MS to proceed with network re-entry.
3   Un-Secure Location Update results in MS network re-entry. It is performed in the same way as a regular MS
4   network entry process. Anchor PC relocation may occur during Location Update procedure. Anchor PC relocation
5   during location update is an optional procedure. For Location Update with Power Down, refer to section 4.5.2.2.1.

6   ### 4.10.2.1 Successful Location Update - No Paging Controller Relocation

7   Figure 4-70 describes a MS initiated successful location update procedure with no paging controller relocation.
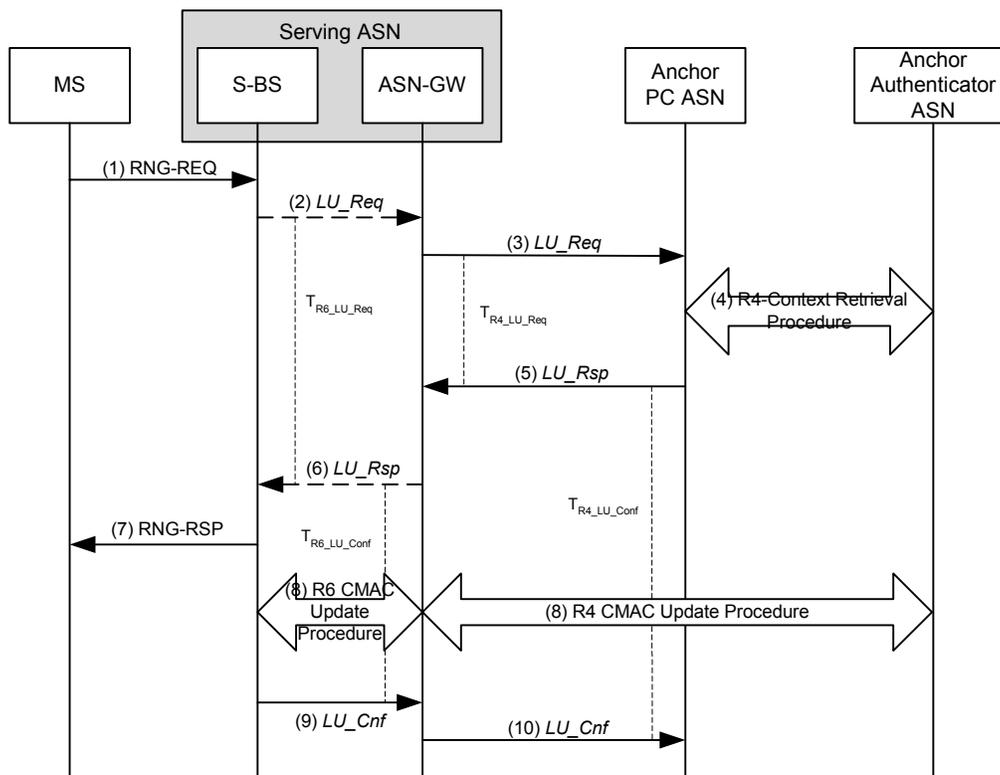
8

9   **Figure 4-70 – Secure Location Update - No Paging Controller Relocation**

10 **STEP 1**

11 The MS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e
12 specification are met. The MS sends a RNG-REQ message, which includes the Ranging Purpose Indication TLV set
13 to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor PC ASN acting as the Anchor
14 PC function for the MS, and the HMAC/CMAC tuple.

15 **STEP 2**

16 The serving BS sends an R6 *LU_Req* message to the serving ASN-GW and starts timer $T_{R6\_LU\_Req}$. The message may
17 include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS proposes an update to these parameters.

18 **STEP 3**

19 The Serving ASN (associated with the serving BS and local PC) sends an R4 *LU_Req* message to the Anchor PC
20 ASN associated and starts timer $T_{R6\_LU\_Req}$. The message may include the PG ID, Paging Offset, and Paging Cycle
21 TLVs if the Serving ASN proposes an update to these parameters. Note that this message may be relayed by several
22 intermittent ASNs before reaching the Anchor PC ASN.

1   **STEP 4**

2   If the Anchor PC ASN retains context information for the MS including its Authenticator ID, the Anchor PC ASN
3   initiates a Context Request procedure with the Anchor Authenticator ASN. Refer to section 4.13 for the call flow. If
4   the Anchor Authenticator ASN has valid key material for the MS, it returns AK context for the MS to the Anchor
5   PC ASN.

6   **STEP 5**

7   Upon successful retrieval of the AK context, the Anchor PC ASN sends an R4 *LU_Rsp* message back to the Serving
8   ASN and starts timer $T_{R4\_LU\_Conf}$. The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging
9   Offset, Paging Cycle, Anchor PC ID TLVs, and Location Update Status TLV set to 'Accept'. Upon receipt of the
10   R4 *LU_Rsp* message, Serving ASN stops timer $T_{R4\_LU\_Req}$.

11   **STEP 6**

12   Upon receipt of the R4 *LU_Rsp* message, the Serving ASN-GW stops timer $T_{R4\_LU\_Req}$, sends an R6 *LU_Rsp*
13   message to the S-BS, and starts timer $T_{R6\_LU\_Conf}$. The message includes the Location Update Status TLV set to
14   'Accept', AK Context TLVs, as well as the assigned Paging Information TLV if they were included in the
15   corresponding R4 message..

16   **STEP 7**

17   Based on the AK and AK context received from the Anchor PC, the Serving BS (associated with Local PC/Relay
18   PC) successfully authenticates the RNG_REQ message received from the MS and sends a RNG_RSP message with
19   HMAC/CMAC and Successful *LU_Rsp* indication, as specified in the IEEE Std 802.16 specification, to the MS.

20   **STEP 8**

21   The Serving BS initiates an R6 CMAC Key Count Update procedure with the ASN-GW. The Serving ASN initiates
22   an R4 CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key
23   Count. Refer to section 4.13 for the call flow.

24   **STEP 9**

25   The Serving BS sends an R6 *LU_Cnf* message to the serving ASN-GW with Location Update TLV indicating
26   'success'. Upon receipt of the message, the serving ASN-GW stops timer $T_{R6\_LU\_Conf.}$

27   **STEP 10**

28   The Serving ASN sends an R4 *LU_Cnf* message with a successful LU indication to the Anchor PC ASN and stops
29   timer $T_{R6\_LU\_Req}$. Upon receipt of the message, The Anchor PC ASN updates the LR with MS Idle Mode information
30   and stops timer $T_{R4\_LU\_Conf.}$

1   **4.10.2.2 Successful Secure Location Update with PC Relocation**
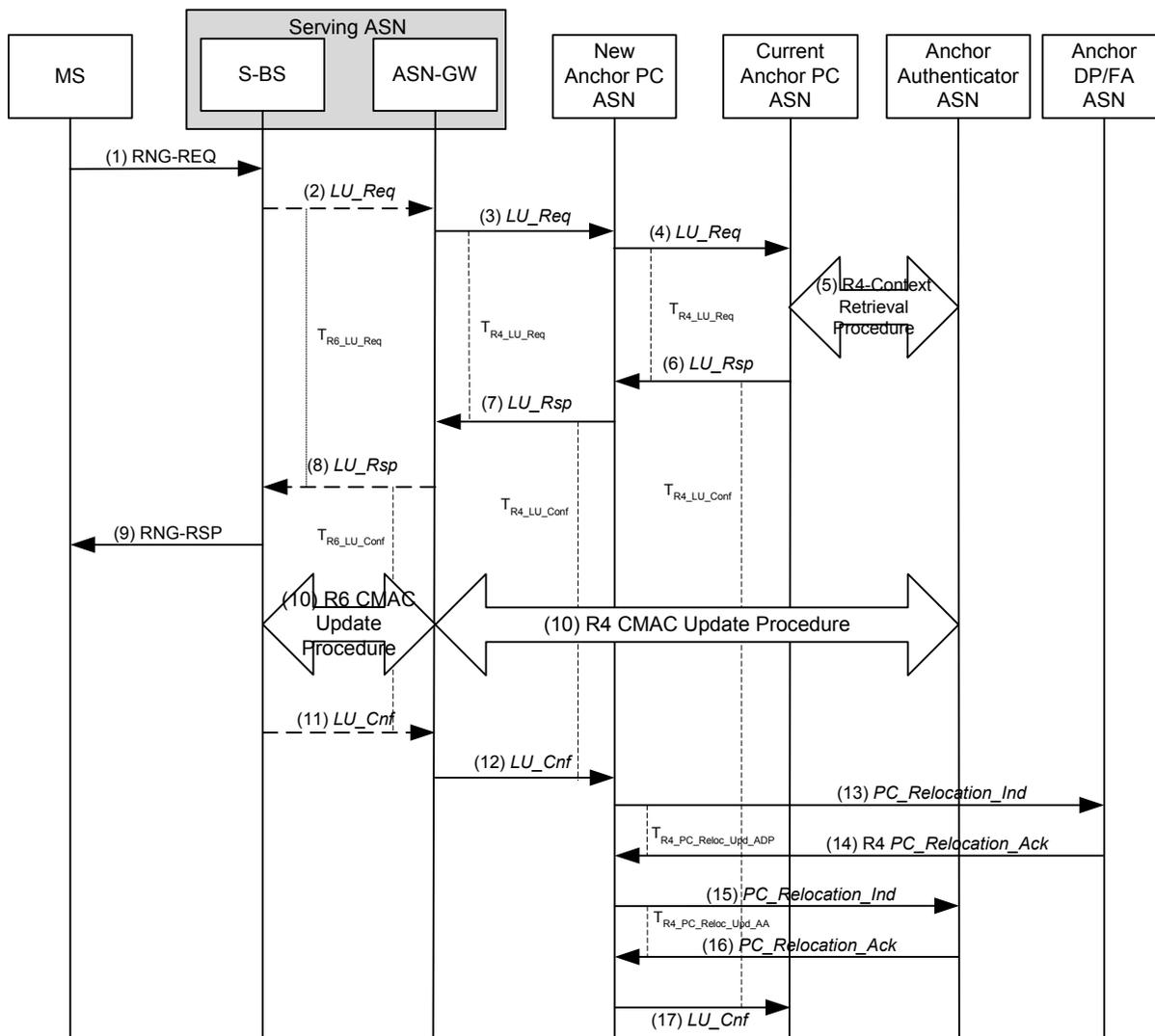
2

3   **Figure 4-71 – Secure Location Update With PC Relocation**

4   **STEP 1**

5   The MS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e
6   specification are met. The MS sends a RNG-REQ message, which includes the Ranging Purpose Indication TLV set
7   to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor PC ASN acting as the Anchor
8   PC function for the MS, and the HMAC/CMAC tuple.

9   **STEP 2**

10   The serving BS sends an R6 *LU_Req* message to the serving ASN-GW and starts timer $T_{R6\_LU\_Req}$. The message may
11   include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS proposes an update to these parameters.

12   **STEP 3**

13   The Serving ASN (associated with the serving BS and local PC) sends an R4 *LU_Req* message to the Anchor PC
14   ASN associated and starts timer $T_{R6\_LU\_Req}$. The message may include the PG ID, Paging Offset, and Paging Cycle

1 TLVs if the Serving ASN proposes an update to these parameters. Note that this message may be relayed by several
2 intermittent ASNs before reaching the Current Anchor PC ASN. The Serving ASN or any intermittent ASN along
3 the path may request PC relocation.

STEP 4

5 Upon receipt of the R4 *LU_Req* message, a relay PC ASN adds the Anchor PC Relocation Destination TLV to
6 initiate PC relocation to it as part of the location update procedure, and forwards the message on to the Anchor PC
7 ASN. New Anchor PC ASN starts timer $T_{R4\_LU\_Request}$.

STEP 5

9 Refer to section 4.13 for the call flow. If the Current Anchor PC ASN retains context information for the MS
10 including its Authenticator ID, the Current Anchor PC ASN initiates a Context Request procedure with the Anchor
11 Authenticator ASN. If the Anchor Authenticator ASN has valid key material for the MS, it returns AK context for
12 the MS to the Anchor PC ASN.

STEP 6

14 The Current Anchor PC ASN sends an R4 *LU_Rsp* message back to the New Anchor PC ASN and starts timer
15 $T_{R4\_LU\_Conf}$. The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle,
16 Anchor PC ID TLVs, and Location Update Status TLV set to 'Accept'. The Anchor PC Relocation Request
17 Response TLV is set to 'Accept' to indicate that the Current Anchor PC ASN accepted the *PC_Relocation_Req* and
18 the Anchor PC ID TLV is set to the identifier of New Anchor PC ASN ID which was received in the Anchor PC
19 Relocation Destination TLV in the R4 *LU_Req* message. The R4 *LU_Rsp* message also includes MS Info TLV
20 containing MS context for transfer to the New Anchor PC ASN.

21 If the New Anchor PC ASN doesn't request PC Relocation, the CurrentAnchor PC MAY still request to perform
22 such procedure by including also the PC Relocation Indication TLV. If the New Anchor PC doesn't accept the
23 relocation it will report Failure in step 17.

STEP 7

25 Upon receipt of the R4 *LU_Rsp* message from Current Anchor PC ASN, New Anchor PC ASN stops timer
26 $T_{R4\_LU\_Req}$, stores the MS context received from Current Anchor PC ASN, updates the Paging Information (Paging
27 Group ID, Paging Cycle, Paging Offset), forwards the R4 *LU_Rsp* message on to the Serving ASN, and starts
28 timer$T_{R4\_LU\_Conf}$.

STEP 8

30 Upon receipt of the R4 *LU_Rsp* message, the Serving ASN-GW stops timer $T_{R4\_LU\_Req}$, sends an R6 *LU_Rsp*
31 message to the S-BS, and starts timer$T_{R6\_LU\_Conf}$. The message includes the Location Update Status TLV set to
32 'Accept', MS Info, AK Context, Anchor PC ID, and Old Anchor PC ID TLV. The message may include the Paging
33 Information TLV if they were included in the corresponding R4 message.

STEP 9

35 Based on the AK and AK context received from the Current Anchor PC, the Serving BS (associated with Local
36 PC/Relay PC) successfully authenticates the RNG_REQ message received from the MS and sends a RNG_RSP
37 message with HMAC/CMAC and Successful Location Update Response indication, as specified in the IEEE Std
38 802.16 specification, to the MS.

STEP 10

40 The Serving BS initiates an R6 CMAC Key Count Update procedure with the ASN-GW. The Serving ASN initiates
41 a CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key Count.
42 Refer to section 4.13 for the call flow.

STEP 11

The Serving BS sends an R6 *LU_Cnf* message to the serving ASN-GW with Location Update TLV indicating 'success'. Upon receipt of the message, the serving ASN-GW stops timer $T_{R6\_LU\_Conf.}$

STEP 12

The Serving ASN sends an R4 *LU_Cnf* message with a successful LU indication to New Anchor PC ASN (as indicated by the Anchor PC ID received from the BS) and stops timer $T_{R6\_LU\_Req}$. Alternatively the a Relay PC ASN forwards *LU_Cnf* to the ASN associated with New Anchor PC with the result indication reassigned by Relay PC. Upon receipt of the message, New Anchor PC ASN stops timer $T_{R4\_LU\_Conf}$.

STEP 13

Upon receipt of the *LU_Cnf* message indicating successful PC relocation, the 'old' Current Anchor PC clears the LR context for this MS, stops timer $T_{R4\_LU\_Conf,}$ sends an R4 *PC_Relocation_Ind* to the Anchor DP/FA ASN, and starts timer $T_{R4\_PC\_Reloc\_Upd\_ADP.}$

STEP 14

The Anchor DP/FA ASN updates the Anchor PC for the MS with the New Anchor PC ASN ID and responds with an R4 *PC_Relocation_Ack* message confirming the Anchor PC update. Upon receipt of the message, the Current Anchor ASN stops timer $T_{R4\_PC\_Reloc\_Upd\_ADP}$. At this point, New Anchor PC ASN hosts the Anchor PC function and becomes the 'new' Current Anchor PC ASN for the MS and the Anchor PC is de-allocated from the 'old' Current Anchor PC ASN.

STEP 15

And the same time of sending *PC_Relocation_Ind* to Anchor DP/FA, the 'old' Current Anchor PC sends an R4 PC Relocation Indication to Anchor Authenticator ASN to inform the change of the Anchor PC, and starts timer $T_{R4\text{-}PC\_Reloc\_Upd\_AA.}$

STEP 16

The Anchor Authenticator ASN updates the Anchor PC for the MS with the New Anchor PC ASN ID and responds with an R4 *PC_Relocation_Ack* message confirming the Anchor PC update. Upon receipt of the message, the Current Anchor ASN stops timer $T_{R4\text{-}PC\_Reloc\_Upd\_AA}$. At this point, New Anchor PC ASN hosts the Anchor PC function and becomes the 'new' Current Anchor PC ASN for the MS and the Anchor PC is de-allocated from the 'old' Current Anchor PC ASN.

STEP 17

The New Anchor PC ASN sends an R4 *LU_Cnf* message with a successful LU indication to the Current Anchor PC ASN and stops timer $T_{R4\_LU\_Conf}$.

4.10.2.3 Location Update Timers and Considerations

The following timers are used to support Idle Mode Location Updates:

- $T_{R4\_LU\_Req}$: This timer is started by a Serving or Relay ASN upon transmission of an R4 *LU_Req* message from a source ASN to a target ASN. This timer is stopped upon reception of an R4 *LU_Rsp* from the target ASN.

- $T_{R4\_LU\_Conf}$: This timer is started upon transmission of an R4 *LU_Rsp* message by a source AN to a target ASN. This timer is stopped upon reception of an R4 *LU_Cnf* message from the target ASN.

- $T_{R4\_PC\_Reloc\_Upd\_ADP}$: This timer is started by an Anchor PC ASN upon transmission of a R4 *PC_Relocation_Ind* message to an Anchor DP/FA ASN. This timer is stopped upon reception of a R4 *PC RelocationAck* message from an Anchor DP/FA ASN.

1   • T$_{R4\text{-}PC\_Reloc\_Upd\_AA}$: This timer is started by an Anchor PC ASN upon transmission of a R4
2   *PC_Relocation_Ind* message to an Anchor Authenticator ASN. This timer is stopped upon reception of a
3   R4 *PC_Relocation_Ack* message from an Anchor Authenticator ASN

4   • T$_{R6\_LU\_Req}$: This timer is started by a Serving BS upon transmission of an R6 *LU_Req* message from a
5   Serving BS to a Serving ASN-GW. This timer is stopped upon reception of an R6 *LU_Rsp* message from
6   the Serving ASN-GW.

7   • T$_{R6\_LU\_Conf}$: This timer is started by a Serving ASN-GW upon transmission of an R6 *LU_Rsp* message to a
8   Serving BS. This timer is stopped upon reception of an R6 *LU_Cnf* message from the Serving BS.

9 Table 4-102 describes the default value and recommended range and duration for these timers.

10

Table 4-102 – Location Update Timer Values

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T$_{R4\_LU\_Req}$	TBD		TBD
T$_{R4\_LU\_Conf}$	TBD		TBD
T$_{R4\_PC\_Reloc\_Upd\_ADP}$	TBD		TBD
T$_{R4\_PC\_Reloc\_Upd\_AA}$	TBD		TBD
T$_{R6\_LU\_Req}$	TBD		TBD
T$_{R6\_LU\_Conf}$	TBD		TBD

11 **4.10.2.4 Location Update Error Procedures**

12 **4.10.2.4.1 Timer MAX Retries**

13 Table 4-103 describes timer expiry causes, reset triggers and corresponding actions. Upon timer expiry, if the
14 maximum number of retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s) should
15 be performed as indicated in Table 4-103.

16

Table 4-103 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T$_{R4\_LU\_Req}$	Source/Relay ASN	Notify Serving ASN of failure. Serving ASN notifies MS.
T$_{R4\_LU\_Conf}$	Anchor PC ASN/Relay ASN	Anchor PC ASN refrains from updating LR with MS Idle Mode info.
T$_{R4\_PC\_Reloc\_Upd}$	Old Anchor PC ASN	Old Anchor PC ASN notifies Relay Serving ASN of PC relocation. Serving ASN notifies MS.
T$_{R6\_LU\_Req}$	Serving BS	Serving BS notifies MS or Location Update failure.
T$_{R6\_LU\_Conf}$	Serving ASN-GW	Anchor PC refrains from updating LR with MS Idle Mode info.

17 **4.10.2.4.2 Authenticator Context Retrieval failure**

18 Whenever the RNG-REQ authentication fails either because the CMAC is determined to be invalid or the Anchor
19 Authenticator could not provide complete AK context, the ASN of the Relay PC SHALL instruct the MS to begin

1   the "Un-secure Location Update". Just as with failure of Secure Location Update, Unsecure Location Update is
2   performed as MS network re-entry from Idle Mode process (see 4.10.2.4.4).

4.10.2.4.3 PC Relocation Failure

4   PC Failure may occur if the Current Anchor PC ASN rejects PC relocation or a candidate Anchor PC rejects the
5   *Relocation_Req*. PC relocation may also fail if the Anchor DP/FA ASN could not be updated of the pending PC
6   relocation. If PC relocation failure occurs for any reason, the current Anchor PC ASN shall continue to support the
7   Anchor PC function and the serving ASN shall be notified by means of the R4 *LU_Rsp* message.

8   If PC relocation requested by the Current Anchor PC ASN is refused because of failure or policy, then the Current
9   Anchor PC MAY still release the context of the user due, for example, to overflowing of the LR database

10 If PC relocation requested by the New Anchor PC ASN is refused, then the New Anchor PC MAY still decide to
11 enforce a new PC-ID to the MS as a local decision or the New Anchor PC MAY force the MS to perform Unsecure
12 LU.

4.10.2.4.4 Secure Location Update Failure

14 The Anchor PC receiving *LU_Cnf* message including LU Result Indicator with a value of Failure should keep the
15 MS information unchanged as if the LU Update procedure had not occurred.

16 MS receiving RNG-RSP message with "Failure of Idle Mode Location Update" should perform a network re-entry
17 process (see 4.10.4). The network will re-authenticate the MS during network re-entry from Idle Mode. If the re-
18 authentication still fails, any entity of the network which has kept any information related to the MS should not be
19 changed.

20 If MS performs a network re-entry process caused by un-secure LU, not power down, after successful re-
21 authentication with complete or optimized network re-entry, the Idle Mode Entry procedure may be initiated by MS
22 or network as described in section 4.10.5.

23 If MS performs a network re-entry process caused by un-secure LU, power down request, after successful re-
24 authentication with complete or optimized network re-entry, the MS or network should send DREG REQ/CMD to
25 finish its power down process.

4.10.2.5 Location Update Messages

27 Note: *Context_Req* and *Context_Rpt* messages should be specified in the generic utility section of the document.
28 MS Info Request Response messages have been renamed.

29   **Table 4-104 – R6 LU_Req Primitive Structure**

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the BS where MS performs location update.
Anchor PC ID	Anchor Paging Controller Identification	M	"PC ID" field in DREG_REQ on R1 points to MS's anchor Paging Controller
Authentication Indication	Indicates whether or not the S_BS has security information (Cached AK and AK context or Authenticator ID for this MS) for verifying authenticated RNG-REQ	M	0: No Authentication Information 1: Authentication Information present
Anchor PC Relocation Destination	Requested new Anchor PC	O	Identifier for destination Anchor PC in the event of Anchor PC relocation
Paging Information	Paging Information	O	Paging Information TLV contains

IE	Description	M/O	Notes
			PAGING_CYCLE, PAGING OFFSET, and Paging Group ID. The BS may make a suggestion for Paging Cycle and Paging Offset for the MS performing LU
Network Exit Indicator	This Information Element indicates the MS is currently attempting to switch power off, regardless of value	O	This is in case the LU is caused by Power Down Update

Table 4-105 – R6 LU_Rsp Primitive Structure

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the BS where MS performs location update.
Old Anchor PC ID	Paging Controller Identification	O	This TLV is included in the event of PC relocation
Authenticator ID	The ID of Anchor Authenticator	O	
AK Context	AK and AK context	O	Security context required for BS to validate the received RNG-REQ message from MS and respond with RNG-RSP signed by a valid H/CMAC digest
Paging Information	Paging Information	O	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, and Paging Group ID. The BS may make a suggestion for Paging Cycle and Paging Offset for the MS performing LU
Anchor PC ID	Identifier of Anchor PC	O	This TLV is included in the event of PC relocation
Anchor PC Relocation Request Response	Response to the relocation request	O	"Accept" or "Refuse"
MS Info	The information that needs to be transferred form the old Anchor PC to new Anchor PC	O	MS Info to be included in the event of PC relocation
Location Update Status	indicates that whether the LU procedure SHOULD be continued; if refused the S_BS SHALL require MS to conduct unsecured Location Update (Network Re-entry from Idle Mode)	M	"Accept" or "Refuse"

1   **Table 4-106 – R6 LU_Cnf Primitive Structure**

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the BS where MS performs location update.
LU Result Indicator	Indicates the success/failure of the LU procedure	M	• 1 = Failure • 0 = Success
Anchor PC ID	Identifier of the Anchor PC	O	Included if PC relocation was requested earlier
Relocation Success Indicator	(Boolean) Indicates confirmation of whether the Relocation was accepted and completed by the Relocation Destination	O	Success if Relocation was accepted by destination and completed.

2   **Table 4-107 – R4 LU_Req Primitive Structure**

IE	Reference	M/O	Notes
BS ID	Section 5.3.2.25	M	BS ID indicating the BS where MS performs location update.
Anchor PC Relocation Destination	Section 5.3.2.13	O	Identifier for destination Anchor PC
Paging Information	Section 5.3.2.119	O	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, and Paging Group ID. The BS may make a suggestion for Paging Cycle and Paging Offset for the MS performing LU
Network Exit Indicator	Section 5.3.2.109	O	Included when LU is caused by Power Down Update

3   **Table 4-108 – R4 Context_Req Primitive Structure**

IE	Reference	M/O	Notes
BS ID	Section 5.3.2.25	M	The current Serving BS ID MS is registered in
Anchor PC Relocation Destination	Section 5.3.2.13	O	Identifier for destination Anchor PC, included in the event of Anchor PC relocation

4   **Table 4-109 – R4 Context_Rpt Primitive Structure**

IE	Reference	M/O	Notes
BS ID	Section 5.3.2.25	M	The current Serving BS ID MS is registered in
AK Context	Section 5.3.2.6	M	

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Provide failure indication for this message

1 **Table 4-110 – R4 LU_Rsp Primitive Structure**

IE	Reference	M/O	Notes
BS ID	Section 5.3.2.25	M	BS ID indicating the BS where MS performs location update.
Old Anchor PC ID	Section 5.3.2.113	O	This TLV is included in the event of PC relocation.
Authenticator ID	Section 5.3.2.19	O	
AK Context	Section 5.3.2.6	O	AK Context SHALL not be provided in the case where Location Update Status is set to "Refuse"
Paging Information	Section 5.3.2.119	M	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, and Paging Group ID.
Anchor PC ID	Section 5.3.2.12	O	This TLV is included in the event of PC relocation.
Anchor PC Relocation Request Response	Section 5.3.2.14	O	"Accept" or "Refuse"
PC Relocation Indication	Section 5.3.2.122	O	Included by the Current Anchor PC to request PC relocation
MS Info	Section 5.3.2.103	O	MS Info to be included in the event of PC relocation.
Location Update Status	Section 5.3.2.88	M	"Accept" or "Refuse"

2 **Table 4-111 – R4 LU_Cnf Primitive Structure**

IE	Reference	M/O	Notes
BS ID	Section 5.3.2.25	M	BS ID indicating the BS where MS performs location update.
LU Result Indicator	Section 5.3.2.90Omdocatopm	M	0 = Success 1 = Failure
Relocation Success Indicator	Section 5.3.2.149	O	Success if Relocation was accepted by destination and completed.

3 **Table 4-112 – R4 PC_Relocation_Indication_Ack Primitive Structure**

IE	Description	M/O	Notes
BS ID	Section 5.3.2.25	M	BS ID indicating the BS where MS performs location update.

IE	Description	M/O	Notes
Anchor PC ID	Section 5.3.2.12	M	Indicating the new Anchor PC ID
LU Result Indicator	Section 5.3.2.90	M	0 = Success 1 = Failure

1 **Table 4-113 – R4 PC_Relocation_Ind Primitive Structure**

IE	Reference	M/O	Notes
PC ID	Section 5.3.2.117	M	

2 **Table 4-114 – R4 PC_Relocation_Ack Primitive Structure**

IE	Reference	M/O	Notes
VOID			

3 ## 4.10.3 Paging Procedure

4 Paging procedures i.e. the sending of the *Paging_Announce* messages occur under several scenarios which include:

5 • Incoming data for the MS

6 • Location update forced by the network for this MS

7 • Network initiated MS network re-entry

8 • Cancel *Paging_Announce* once the MS has exited IDLE state.

9 Paging procedures may include topological aware and unaware schemes.

10 Call flows described in this section may only occure when functional entities such as Relay PC, FA/ADPF, Anchor
11 PC, and authenticator are located in different ASNs per each MS. If two functional entities shown are co-located in a
12 single ASN the corresponding R4 signaling described are not exposed. For example, if the PC and Authenticator are
13 collocated for an MS, R4 signaling between the PC and Authenticator are not exposed. Another example is that if
14 the PC and FA/ADPF is located within a single ASN, the corresponding R4 signaling between the PC and FA is not
15 exposed.

16 ### 4.10.3.1 Topologically Aware Paging

17 In the topologically aware paging scheme, the Anchor PC is aware of the Paging group's structure and contains the
18 addresses of of all the Relay-PC identities. In addition the PC may keep track of the BSID where the MS last
19 performed a location update, and also neighboring BS topology to allow for multi-step paging. The Anchor PC
20 directly sends R4 *Paging_Announce* messages to only the Relay PCs associated with the MSs current PGID (see
21 Figure 4-72). The Relay PC in turn will do single or multi-step paging based on the information contained in the
22 received *Paging_Announce* message. Topologically aware paging is an optional procedure for WiMAX networks.

1
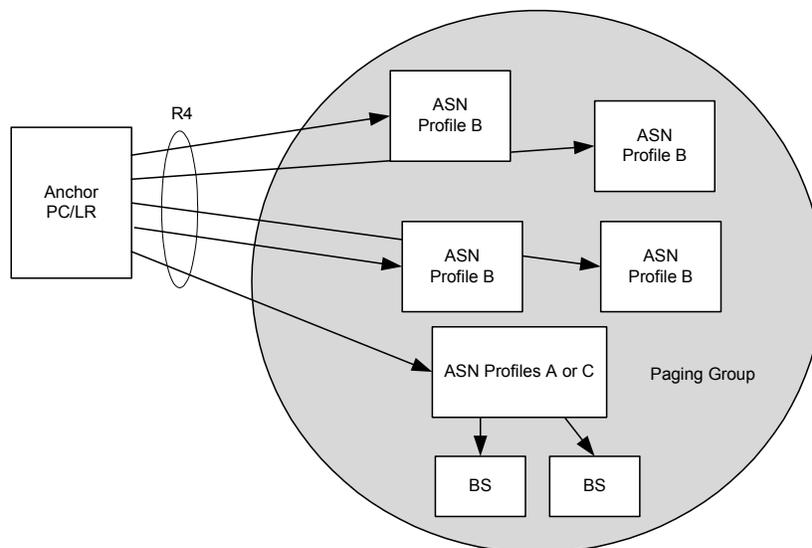
2   **Figure 4-72 – Topologically Aware Paging Announce Scheme**

3 **4.10.3.2 Topologically Unaware Paging Scheme**

4   In the topologically unaware paging scheme the Anchor PC is unaware of the topology or structure of the paging
5   groups and has no knowledge of the paging group members associated with the PC-Relays that manage the various
6   paging groups. As such several vendor specific paging scehmes can be supported (e.g. flood paging where the
7   Anchor PC sends a message to all associated Relay PC's). The following describes an example of a topologically
8   unaware paging procedure (see Figure 4-73). The Anchor PC keeps track of the Relay PC ID, reported by the last
9   Location Update message received from the MS. As the MS in Idle Mode traverses the network, it performs location
10 updates as it passes through different paging groups. The Anchor PC/LR keeps updating the last reported Relay PC
11 ID so that a *Paging_Announce* message can be forwarded to it when the MS is paged. The last reported Relay PC
12 (i.e. the local PC), is topologically aware and maintains the list of its local neighboring ASNs and additional Relay
13 PCs that are part of the Paging group and forwards the *Paging_Announce* message to the paging group members as
14 well as the BSs under its control. The additional Relay PC will in turn forward the *Paging_Announce* message to the
15 BS their control. The topologically unaware Anchor PC relies on the last reported Relay PC, to contain the list of
16 pertinent Base Stations and/or Relay PCs that need to be paged. This list is defined by the network operator and is
17 based on the local topology of a group of neighboring Base Stations within the same paging group. Note that for
18 optimization, the member list may also include neighboring Base Stations that belong to adjacent page groups that
19 may be deemed appropriate for paging as well. Topologically unaware paging is a mandatory procedure for
20 WiMAX networks.

1
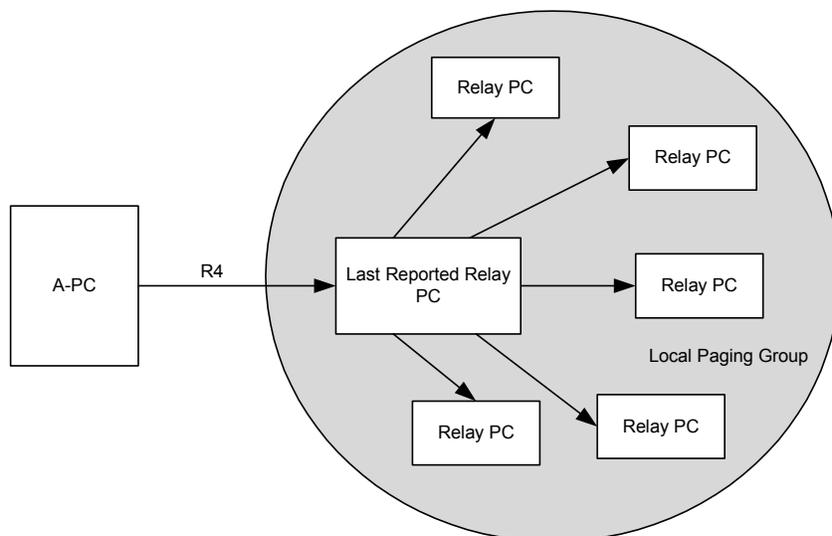
Figure 4-73 – Topologically Unaware Paging Announce Scheme

4.10.3.3 Single-step vs Multi-step Paging Operations

For efficiency and flexibility in the implementation of paging operation, paging may be performed in a single step or multiple steps. The following provides illustrative examples of single and multi-step Paging Announce algorithm.

Single-step Operation:

In a single step paging operation, when a MS is to be paged, the PC/LR directly sends *Paging_Announce* messages to each Relay PC in the list defined for the paging group last reported by the MS. The Local/Relay PC directly sends *Paging_Announce* messages to each Base Station in the BS ID IE if received from the Anchor PC. If the BS ID IE is not present, the local PC sends the *Paging_Announce* message to all BSs under its domain.

Multi-step Operation:

In a multi step paging operation, rather than flooding the entire group members with a paging messages over the air in one instance, this method is flexible and allows the expansion of the paging area in a step by step manner, provided the paging group can be organized in such fashion. Paging in a multi-step fashion allows for conservation of RF resources. Hence in this method, when the PC/LR starts paging the MS it sends the *Paging_Announce* message to a subset of the paging group members that are defined for the last Paging group reported by the MS, and additionally it includes a BS ID(s) TLV indicating the BSs to be paged in each Paging Announce step. If there is no answer to the paging message after a pre-defined timeout, the PC/LR expands the coverage area to the next defined subgroup. In this fashion the entire page group is covered in a multi-step manner. Alternatively, the Anchor PC may include the Last reported BSID (this can be stored at the PC/LR) when could be used by the Local PC to identify a subgroup of BSs to be paged. The MS MAY still be located around the coverage area of the last BS that performed the last Location Update.
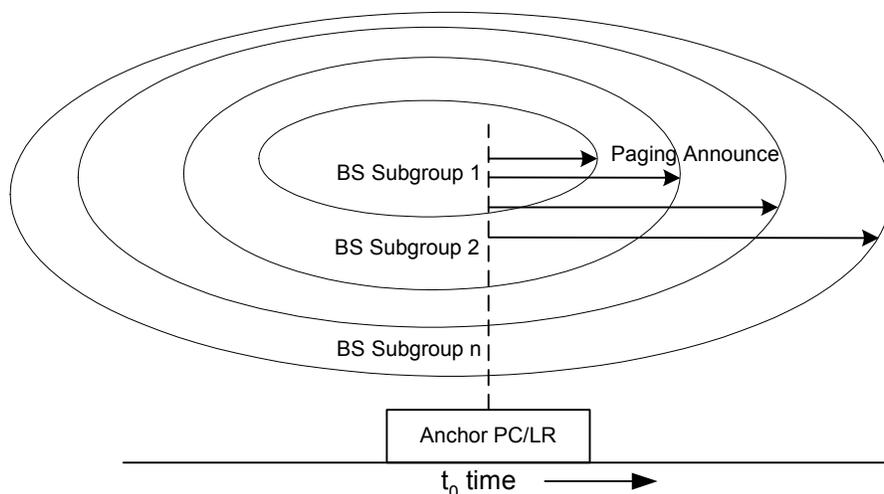
1

2 **Figure 4-74 – Single-step Paging**
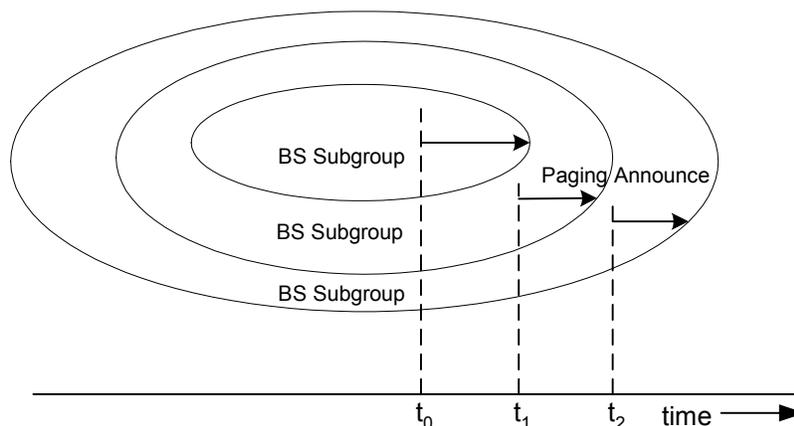
3

4 **Figure 4-75 – Multi-step Paging**

5 **4.10.3.4 IP Multicasting Support for Paging_Announce**

6 IP Multicasting [16] MAY be used for announcing the paging information for an Idle Mode MS or a set of Idle
7 Mode MS's via the *Paging_Announce* message.

8 Multicast groups may be created as as described in [16]. Each multicast group contains some set of the BSs – the
9 exact grouping being implementation dependent.

10 Each multicast group is assigned a multicast IP address, which is used as the destination address in the IP header of
11 the *Paging_Announce* message.

12 In general, non-members of the group can also receive the message sent using multicast IP address. However, only
13 the members of the group can be recipients of the messages sent to the group

14 **4.10.3.5 Paging Procedure Message Flow**

15 The following call flow illustrates the paging procedure. The paging operation can be triggered by several actions,
16 but the paging procedure for each trigger is similar. Figure 4-76 illustrates the paging procedure triggered by DL
17 data arrival for a MS when the MS is in Idle Mode.

1
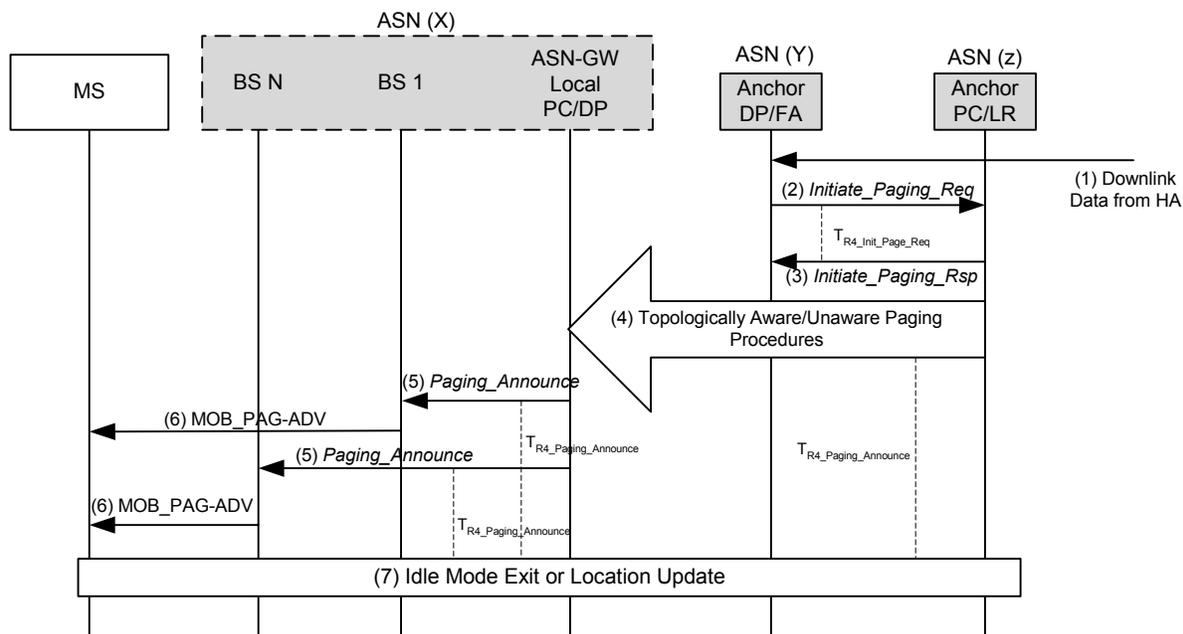
2 **Figure 4-76 – Paging Procedure**

3 **STEP 1**

4 Data from HA arrives through the tunnel at the FA and its associated DPF. The Anchor DPF buffers the data.

5 **STEP 2**

6 The Anchor Data Path Function determines that MS is in Idle Mode and SHALL activate it before the received data
7 can be delivered. Anchor DPF sends an R4 *Initiate_Paging_Req* message to Anchor PC/LR to request paging.
8 Optionally the R4 *Initiate_Paging_Req* message contains the QoS parameters of the flow for which the data arrived
9 at the Anchor DPF. This helps set priority treatment of the Paging operation based on the QoS parameters and flow
10 types. The Anchor DPF may have policies for triggering paging based on the QoS parameters for the data received.
11 The Anchor DP Function starts timer $T_{Init\_Page\_Req}$.

12 Note: When MS is in Idle Mode, if data not belonging to any saved SF of the MS arrives, the decision to initiate
13 paging or not is left for operator's setting.

14 **STEP 3**

15 Anchor PC/LR retrieves the information related to the MS, And ends an R4 *Initiate_Paging_Rsp* to Anchor Data
16 Path function. This message is used to indicate whether the MS context as contained in the PC/LR is correct and the
17 requested paging action is authorized. Exclusion of the Response Code TLV indicates intent to page the MS. Upon
18 receipt of this message the Anchor DP Function starts timer $T_{Init\_Page\_Req}$ if running.

19 **STEP 4**

20 If paging action is authorized, Anchor PC retrieves the MS paging information and constructs *Paging_Announce*
21 message. The Anchor PC MAY issue one or more *Paging_Announce* messages based on its knowledge of the
22 Paging Region topology as shown in sections 4.10.3.1 and 4.10.3.2. The Anchor PC MAY issue *Paging_Announce*
23 message(s) to the appropriate Relay PC(s) or directly to BS(s), according to its knowledge of the Paging Region
24 topology. The Anchor PC SHOULD start a timer $T_{R4\_Paging\_Announce}$ when it sends out the first *Paging_Announce*
25 message and SHOULD wait for the paging response. The Anchor PC MAY set a paging re-transmission counter N
26 and—until exhausting the re-transmission counter, and when the Anchor PC does not receive a paging response—
27 may retransmit the *Paging_Announce* message prior to the expiration of the timer $T_{R4\_Paging\_Announce}$. If re-

1 transmitted, the *Paging_Announce* message SHALL be sent no more than N times before the expiration of timer
2 $T_{R4\_Paging\_Announce}$..

3 If the Anchor PC is topologically aware of the defined Paging Group (PG), including the last BS from which the MS
4 performed location update, the Anchor PC SHALL directly issue *Paging_Announce* messages to all, or some subset,
5 of the Paging Group members consisting of BSs and/or relay PCs in the region.

6 If the Anchor PC is topologically unaware of the Paging region, or the BSs defined in the Paging group, but rather
7 one or more Relay PCs, the *Paging_Announce* messages are sent to the known Relay PC(s). The Relay PC(s) then
8 appropriately forwards the announce message to all the one or more BSs in the Paging region.

9 **STEP 5**

10 The ASN-GW that contains the local/relay PC function for the MS initiates the paging operation and sends the R6
11 *Paging_Announce* message to the relevant BS(s) associated with the PGID received in R4 *Paging_Announce*. The
12 ASN GW may perform single step or multi-step paging as described in section 5.10.3.3 based on if BS ID TLV or
13 the L-BSID TLV is present. Associated with each R4 *Paging_Announce* message the ASN-GW starts timer
14 $T_{R6\_Paging\_Announce}$.

15 **STEP 6**

16 Once the Paging Agent (PA) at the BS receives the *Paging_Announce* message with the requested action set to
17 "Start" it extracts the relevant paging parameters for the MS (Paging Cycle, Paging Offset) and initiates the paging
18 action requested by sending out MOB-PAG_ADV message over the airlink as per the indicated paging cycle and the
19 paging offset. The optional SF Flow info in the message helps the BS implement a paging priority scheme for faster
20 call setup when bandwidth is constrained or for resource allocation. The PA will continue to page the MS for the
21 duration specified by the Paging Announce Timer TLV or until the appropriate response is received from the MS or
22 a stop page indication is received from the Local PC.

23 **STEP 7**

24 Upon being successfully paged the MS will perform a Idle Mode Exit or a Location Update procedure. If any Paging
25 Agent (PA) receives a successful reply from the paged MS, the Paging Agent will notify the Local PC by sending a
26 R6 *LU_Req* message in the case of Network Initiated location update or R6 *IM_Exit_State_Change_Req* message in
27 the case of data delivery to MS in idle mode, Upon receipt of a such a message the Local PC will stop timer
28 $T_{R6\_Paging\_Announce}$ if running, and in turn will send the appropriate R4 *LU_Req* or R4 *IM_Exit_State_Change_Req*
29 message to the Anchor PC. Upon receipt of such a message, the Anchor PC will stop timer $T_{R4\_Paging\_Announce}$, if
30 running. The Anchor PC may also initiate stop paging procedures (see xxxx).

31 **4.10.3.6 Stop Paging Procedure**

32 The Paging stop operation is illustrated in Figure 4-77. It is assumed that the MS is being paged over multiple BSs
33 (this could be triggered for example either in response to incoming data to be delivered to the MS or network
34 initiated location update. See section 4.10.3 for detail on the paging process). Upon the PC detecting a response
35 from the MS (e.g. receipt of an authenticated Location Update, or an authenticated Re-entry from Idle Mode), the
36 Anchor PC may send a *Paging_Announce* message with paging start/stop=0 to alert all BSs to stop the paging
37 procedure. This Stop Paging process is a method to prematurely end the normally timed Paging Advertisement
38 method. The support of the Stop Paging procedure is optional.
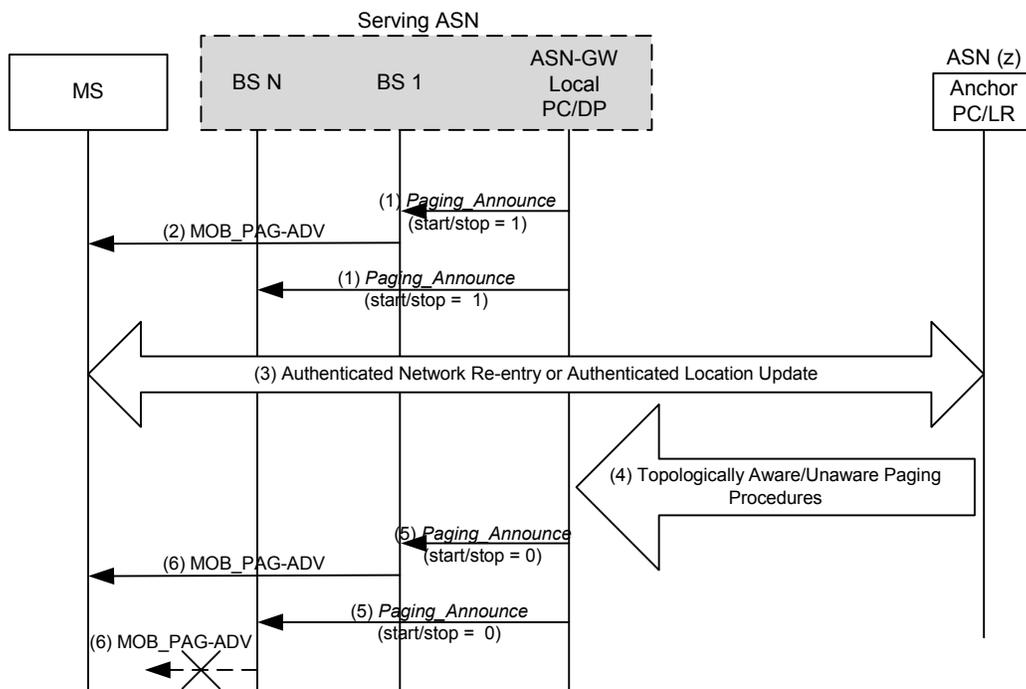
Figure 4-77 – Stop Paging Procedure

STEP 1

The Local PC send R6 *Paging_Announce* message to the BS to initiate paging procedures for the MS. The R6 *Paging_Announce* message has the Paging Start/Stop TLV set to 1. Refer to section 5.10.3 for a description of paging start process.

STEP 2

Upon receipt of the R6 *Paging_Announce* the BS sends a MOB_PAG-ADV message to the MS. Refer to section 4.10.3 for a description of paging start process.

STEP 3

Depending on the action solicited by the MOB_PAG-ADV, the MS performs a Network Re-entry or a Location Update.

STEP 4

Upon receipt of a response from the MS, the Anchor PC sends a R4 *Paging_Announce* message to all BSs in the PG. The R4 *Paging_Announce* message has the Paging Start/Stop TLV set to 0.

STEP 5

The Local PC sends a R6 *Paging_Announce* message to the BSs. The R6 *Paging_Announce* message has the Paging Start/Stop TLV set to 0.

STEP 6

Upon receipt of the R6 *Paging_Announce* message with Paging Start/Stop = 0, the BS may terminate/cease a MOB_PAG-ADV messages over the air. The decision by the BS to terminate or continue its paging procedure is implementation dependent.

1 **4.10.3.7 Paging Timers and Timing Considerations**

2 This section identifies the timer entities participating in the Paging procedure. The following timers are defined over
3 R4 and R6:

4 • $T_{R4\_Paging\_Announce}$: is started by the Anchor PC/Relay upon sending a R4 *Paging_Announce* message. It is
5 stopped upon receiving R4 *LU_Req* or R4 *IM_Exit_State_Change_Req* message.

6 • $T_{R6\_Paging\_Announce}$: is started by the Local PC/Relay PC upon sending a R6 *Paging_Announce* message. It is
7 stopped upon receiving R6 *LU_Req* or R6 *IM_Exit_State_Change_Req* message.

8 • $T_{R4\_Init\_Page\_Req}$: is started by the Anchor DP function upon sending the R4 *Initiate_Paging_Req* message to
9 the Anchor PC, and is stopped upon receiving a corresponding the R4 *Initiate_Paging_Rsp* message.

10 Table 4-115 shows the default value of timers and also indicates the range of the recommended duration of these
11 timers. Note that these values are provisioned in Release 1.0.0.

12 **Table 4-115 – Paging Timer Values for R4 and R6**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R4\_Paging\_Announce}$	TBD		TBD
$T_{R6\_Paging\_Announce}$	TBD		TBD
$T_{R4\_Init\_Page\_Req}$	TBD		TBD

13 **4.10.3.8 Paging Error Conditions**

14 This section describes error conditions associated with the Paging Procedure.

15 **4.10.3.8.1 Timer Expiry**

16 Table 4-116 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
17 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
18 should be performed as indicated in Table 7-5.

19 **Table 4-116 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R4\_Paging\_Announce}$	Anchor PC / Relay PC	The Anchor PC SHALL consider the MS unavailable and stop paging. The Relay PC has no action.
$T_{R6\_Paging\_Announce}$	Relay PC / Local PC	No action
$T_{R4\_Init\_Page\_Req}$	Anchor DP Function	Anchor DP Function SHALL discard the stored data for the MS. The Anchor DP function MAY additionally send some indication to the upstream noted to indicate data delivery failures. Specification of such behavior is implementation specific and outside the scope of this document

20 **4.10.3.8.2 R4 Initiate_Paging_Rsp**

21 Upon receipt of the R4 *Initiate_Paging_Req* message, if the Anchor PC is unable to initiate paging procedures for
22 the MS, it SHALL send a R4 *Initiate_Paging_Rsp* message and include the Response Code TLV with suitable error
23 code value. Upon receipt of R4 *Initiate_Paging_Rsp* message indicating that paging cannot be initiated for the MS,
24 the Anchor DP function MAY resend the R4 *Initiate_Paging_Req* message. If the Anchor DP function does not
25 resend the R4 *Initiate_Paging_Req* message or if the subsequent attempts are also unsuccessful, then Anchor DP
26 Function SHALL discard the stored data for the MS. The Anchor DP function MAY additionally send some

1   indication to the upstream noted to indicate data delivery failures. Specification of such behavior is implementation
2   specific and outside the scope of this document.

3   **4.10.3.9   Messages for Paging Procedure**

4   This section provides the message definitions for the R4 and R6 messages in support of the Paging procedure. See
5   also sections 5.2 and 5.3 for message and TLV definitions respectively.

6
Table 4-117 – R4 Initiate_Paging_Req

IE	Reference	M/O	Notes
SF Info	5.3.2.185	O	Optional QoS type and parameters of the flow to perform preferential Paging and resource reservation. Included if the Anchor DPF has this information and based on local DPF policy. Decision to include this TLV is implementation specific.

7
Table 4-118 – R4 Initiate_Paging_Rsp

IE	Reference	M/O	Notes
Response Code	5.3.2.153	O	Included in paging not allowed. Valid values: • 0x00 = Not allowed - Paging Reference is zero • 0x01 = Not allowed - No such SF
Failure Indication	5.3.2.69		

8
Table 4-119 – R4 Paging_Announce

IE	Reference	M/O	Notes
Paging Information	5.3.2.119	O	Paging Information TLV obtained from the MS containing PAGING_CYCLE, PAGING OFFSET, and Paging Group ID. This IE is included for Paging (start) operation; however it is not required for Paging stop
BS ID(s)	5.3.2.25	O	Included for multi-step paging procedure. If this TLV is not included, then, it is assumed to be a single step paging operation Decision to include this TLV is implementation specific. This is not included for paging stop operation.
L-BSID	5.3.2.87	O	Last reported BS included to identify a Paging subgroup Decision to include this TLV is implementation specific. This is not included for paging stop operation.
SF Info	5.3.2.185	O	Service Flow type and parameters to do prioritized paging based on the QoS type of calls and resource reservation Decision to include this TLV is implementation specific. This is not included for paging stop operation.
Paging Start/Stop	5.3.2.121	M	1 = start Paging Operation 0 = stop Paging Operation

IE	Reference	M/O	Notes
Paging Announce Timer	5.3.2.115	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.
Authenticator ID	5.3.2.19	O	Included as an optimization for reducing the Network entry latency
Paging Cause	5.3.2.116	O	This IE is included for Paging (start) operation; however it is not required for Paging stop When included the following values are valid: • 01 = Location Update • 02 = Network Re-Entry, Incoming Data for Idle MS • 03 = Network Re-entry, required TEK re-authorization • 04 = Network Re-entry, required full security re-authorization • 05 = Network Re-entry, other network management

1 **Table 4-120 – R6 Paging_Announce**

IE	Reference	M/O	Notes
Paging Information	5.3.2.119	O	This compound TLV contains Paging Cycle, Paging Offset and PG ID. This IE is included for Paging (start) operation; however it is not required for Paging stop
PCID	5.3.2.119	O	Used for topologically unaware paging This is not included for paging stop operation.
Anchor PCID	5.3.2.12	O	Included if received in the R4 *Paging_Announce* message.
SF Info	5.3.2.184	O	SF Flow Info for preferential treatment for paging and call origination This is not included for paging stop operation.
Paging Start/Stop	5.3.2.184	M	
Paging Announce Timer	5.3.2.115	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.
Authenticator ID	5.3.2.19	O	Included if received in the R4 *Paging_Announce* message
Paging Cause	5.3.2.116	O	This IE is included for Paging (start) operation; however it is not required for Paging stop When included the following values are valid: • 01= Location Update • 02 = Network Re-Entry, Incoming Data for Idle MS • 03 = Network Re-entry, required TEK re-authorization • 04 = Network Re-entry, required full security re-authorization • 05 = Network Re-entry, other network management

1 ## 4.10.4 Idle Mode Exit

2 ### 4.10.4.1 Idle Mode Exit – Serving ASN Does Not Have MS Context

3 The call flow for a typical scenario for the MS exiting idle mode is shown below. Here it is assumed that when the
4 MS is trying to re-enter the network from idle mode, (i.e. exit the idle mode), the serving ASN does not have any
5 context for this MS – hence, the entire context has to be retrieved from the Anchor PC. In other words the MS tries
6 to re-enter the network when the "management resource holding timer" has expired in the network. Section 4.10.4.1
7 describes the idle mode exit procedure before the expiry of the Resource Retain Timer.
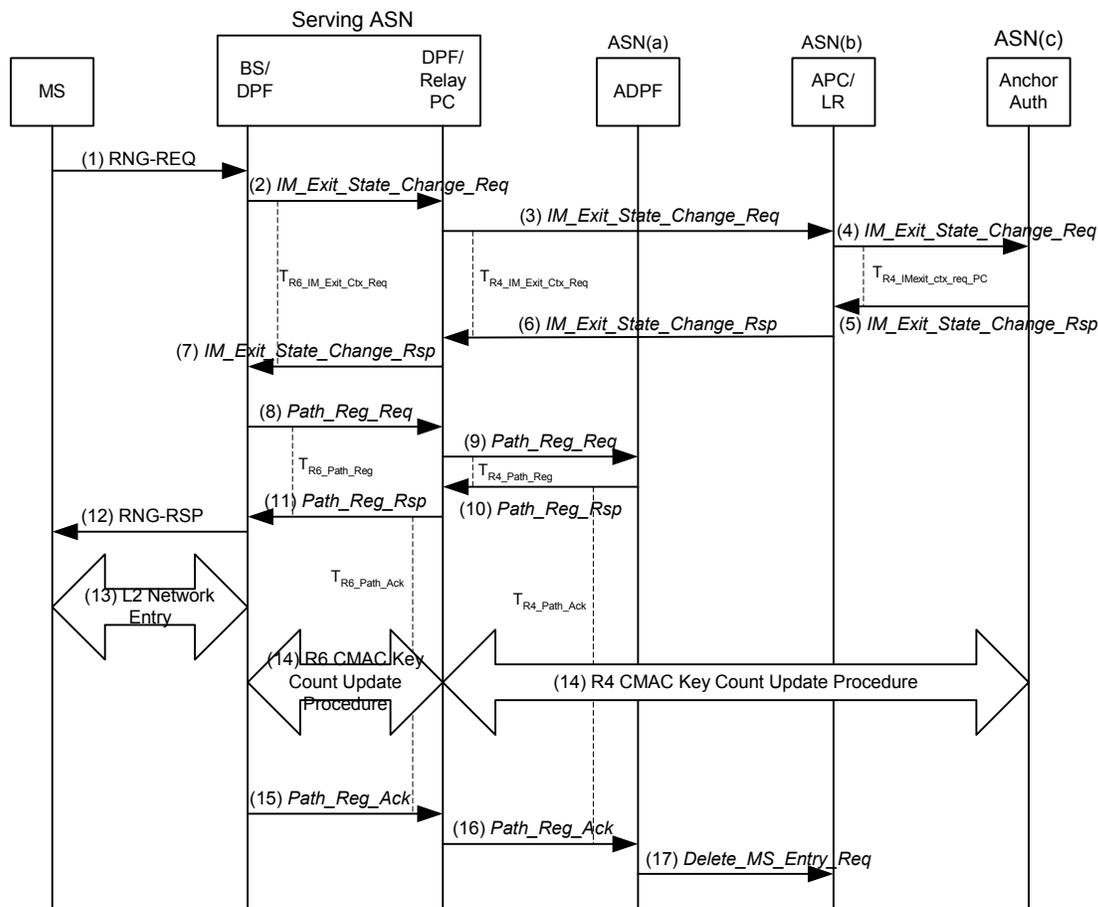
8

9 **Figure 4-78 – Idle Mode Exit Procedure**

10 **Flow Description**

11 MS CAN exit Idle mode in two ways, initiated by the network through Paging or on its own becomes active so that
12 it can communicate. Though the steps in the two scenarios are the same, the sequences are different and some of the
13 steps could be optional.

14 **Case a: Network initiated Idle mode exit (in response to a page)**

15 When MS exits Idle mode in response to a prior Page message, it performs Ranging (RNG_REQ). The MS context
16 may already be available at the BS, as part of the Page initiation, from the *Paging_Announce* message as described
17 in section 4.10.3. If the MS context is available at the BS, this will eliminate steps 2-7 in Figure 4-78

1 **Case b: MS initiated Idle mode exit**

2 When MS on its own wants to become active to initiate communication, it performs the steps given below.

3 **STEP 1**

4 MS initiates exit procedure from IDLE mode and sends RNG_REQ as described in IEEE 802.16 specification. The
5 Ranging Purpose Indication TLV is set to one and PC ID TLV is included, thus indicating that the MS intends to
6 Re-Entry from Idle Mode.

7 **STEP 2**

8 The BS receives the RNG_REQ message from MS indicating Idle mode exit and sends R6
9 *IM_Exit_State_Change_Req* to the Relay PC in the ASN-GW, indicating that the MS wants to become active. Timer
10 $T_{R6\_IM\_Exit\_Ctx\_Req}$ is started at this point by the BS to monitor the response for this message.

11 **STEP 3**

12 The Relay PC in the Serving ASN receives the R6 *IM_Exit_State_Change_Req* from the BS indicating Idle mode
13 exit and sends R4 *IM_Exit_State_Change_Req* to the Anchor PC/LR in ASN(b), indicating that the MS wants to
14 become active. Timer $T_{R4\_IM\_Exit\_Ctx\_Req}$ is started at this point by the ASN-GW to monitor the response for this
15 messageIn the event that the relay PC is the anchor PC, this step is not required.

16 **STEP 4**

17 On receiving the R4 *IM_Exit_State_Change_Req*, the Anchor PC/LR proceeds to request the security context from
18 the Anchor Authenticator in ASN(c) using the R4 *IM_Exit_State_Change_Req*. Timer $T_{R4\_IMexit\_ctx\_req\_PC}$ is started at
19 this point by the Anchor PC to monitor the response for this message. This step is optional if the Anchor
20 Authenticator and Anchor PC/LR are co-located in the same gateway.

21 **STEP 5**

22 Anchor Authenticator responds with the security context back to the Anchor PC/LR with R4
23 *IM_Exit_State_Change_Rsp* message. Once the Anchor PC receives this message, Timer $T_{IM\_Exit\_Ctx\_Req\_PC}$ is
24 stopped. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN.

25 **STEP 6**

26 Anchor PC/LR, sends R4 *IM_Exit_State_Change_Rsp* to the Relay PC. Once the relay PC receives this message,
27 Timer $T_{R4\_IM\_Exit\_Ctx\_Req}$ is stopped. R4 *IM_Exit_State_Change_Rsp* contains the stored information for the MS at the
28 Anchor PC.

29 **STEP 7**

30 Serving ASN retrieves the MS context from Anchor PC ASN and forwards the MS context to the BS on the R6
31 interface. Once the BS receives this message, Timer $T_{R6\_IM\_Exit\_Ctx\_Req}$ is stopped. The message is defined in section
32 5.2. The AK fetched from the authenticator is used to verify the RNG-REQ.

33 **STEP 8**

34 After successful authentication, the BS starts data path establishment – it sends R6 *Path_Reg_Req* to the DPF in the
35 serving ASN. Timer $T_{R6\_Path\_Reg}$ is started at this point by the BS to monitor the response for this message.

36 **STEP 9**

37 The Serving ASN extends the data path establishment to the FA or Anchor DPF in ASN(a) across the R4 interfaces.
38 Timer $T_{R4\_Path\_Reg}$ is started at this point by the serving DPF to monitor the response for this message.

1 **STEP 10**

2 The Data Path Function associated with FA or A_DPF in ASN(a) confirms data path establishment and sends R4
3 *Path_Reg_Rsp* back to the Serving ASN. Timer $T_{R4\_Path\_Ack}$ is started at this point by the Anchor DPF to monitor the
4 ACK for this message. Also, once the serving ASN receives this message, Timer $T_{R4\_Path\_Reg}$ is stopped.

5 **STEP 11**

6 The DPF in the serving ASN confirms data path establishment - sends R6 *Path_Reg_Rsp* to the Serving BS). Timer
7 $T_{R6\_Path\_Ack}$ is started at this point by the serving ASN DPF to monitor the ACK for this message. Also, once the BS
8 receives this message, Timer $T_{R6\_Path\_Reg}$ is stopped

9 **STEP 12**

10 The BS will use MS service and operational information indicated by IDLE Mode Retain Info obtained by Step 7 to
11 construct HO Process Optimization TLV (802.16e parameter) settings in the RNG-RSP based on local policy; then
12 sends RNG_RSP message to the MS formatted according to IEEE 802.16e specification. This message delivers all
13 the required information to resume service in accordance with Idle Mode Retain Information.

14 **STEP 13**

15 The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification. Acknowledge
16 to the Data Path function in the serving ASN confirming intra-ASN data path establishment completion and service
17 flows establishment.

18 **STEP 14**

19 The BS updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN. The
20 procedure for this operation is described in section 4.13. The Anchor Authenticator acknowledges the CMAC update
21 for the MS.

22 **STEP 15**

23 Upon the MS Network Re-Entry completion the BS sends R6 *Path_Reg_Ack* to the data path function in the serving
24 ASN. Timer $T_{R6\_Path\_Ack}$ is stopped at the serving ASN-GW.

25 **STEP 16**

26 The Data Path function in serving ASN sends an inter-ASN R4 *Path_Reg_Ack* to the Data Path function associated
27 with Anchor DPF/FA. Timer $T_{R4\_Path\_Ack}$ is stopped at the anchor DPF.

28 **STEP 17**

29 When R4 *Path_Reg_Ack* is received at Anchor DPF, the Data Path function associated with FA sends a
30 *Delete_MS_Entry_Req* message to PC/LR in order to delete the Idle mode entry associated with the MS. If MS is
31 exiting Idle mode due to a network initiated Idle mode exit, the PC/LR will cease all Paging Announce operations.

32 **4.10.4.1.1 Timers and Timing Considerations**

33 This section identifies the timer entities participating in the IM exit procedure. The IM exit procedure definition
34 shown in Table 4-121 employs the following timers:

35 • $T_{R6\_IM\_Exit\_Ctx\_Req}$: is started by a BS upon sending the R6 *IM_Exit_State_Change_Req* message to the relay
36   PC in the ASN-GW. It is stopped upon receiving a corresponding response.

37 • $T_{R4\_IM\_Exit\_Ctx\_Req}$: is started by a relay PC entity in the ASN upon sending the R4
38   *IM_Exit_State_Change_Req* message to the anchor PC. It is stopped upon receiving a corresponding
39   response.

40 • $T_{R4\_IM\_Exit\_Ctx\_Req\_PC}$: is started by an anchor PC entity upon sending the R4 *IM_Exit_State_Change_Req*
41   message to the anchor authenticator. It is stopped upon receiving a corresponding response.

1 • $T_{R6\_Path\_Reg}$: is started by the BS upon sending the "R6 Path Registration REQ" message to the serving ASN
2   DPF. It is stopped upon receiving a corresponding response.

3 • $T_{R4\_Path\_Reg}$: is started by the serving DPF upon sending the "R4 Path Registration REQ" message to the
4   anchor DPF/FA. It is stopped upon receiving a corresponding response.

5 • $T_{R4\_Path\_Ack}$: is started by an R4 DPF entity upon sending the R4 *Path_Reg_Rsp* message to another DPF in
6   the ASN. It is stopped upon receiving the R4 *Path_Reg_Ack*.

7 • $T_{R6\_Path\_Ack}$: is started by an R4 DPF entity upon sending the R6 *Path_Reg_Rsp* message to the BS. It is
8   stopped upon receiving the R6 *Path_Reg_Ack*.

9 Table 4-121 shows the default value of timers and also indicates the range of the recommended duration of these
10 timers. Note that these values are provisioned in Release 1.0.0.

11 **Table 4-121 – Timer Values for IM Exit Messages over R4**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_IM\_Exit\_Ctx\_Req}$	TBD		TBD
$T_{R4\_IM\_Exit\_Ctx\_Req}$	TBD		TBD
$T_{R4\_IM\_Exit\_Ctx\_Req\_PC}$	TBD		TBD
$T_{R6\_Path\_Reg}$	TBD		TBD
$T_{R4\_Path\_Reg}$	TBD		TBD
$T_{R4\_Path\_Ack}$	TBD		TBD
$T_{R6\_Path\_Ack}$	TBD		TBD

12 **4.10.4.1.2 Idle Mode Exit Error Conditions**

13 This section describes error conditions associated with the IM exit procedure.

14 **4.10.4.1.2.1   Timer Max Retries**

15 Table 4-122 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
16 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
17 should be performed as indicated in Table 7-5.

18 **Table 4-122 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Exit\_Ctx\_Req}$	BS	RNG-RSP message indicating that IM Exit is not possible is sent to the MS on the air interface.
$T_{R4\_IM\_Exit\_Ctx\_Req}$	Relay PC	Relay PC indicates to the BS, failure of context retrieval for the MS in the *IM_Exit_State_Change_Rsp* message
$T_{R4\_IM\_Exit\_Ctx\_Req\_PC}$	Anchor PC	Anchor PC indicates to the Relay PC, failure of context retrieval for the MS in the *IM_Exit_State_Change_Rsp* message

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Reg}$	BS DPF	RNG-RSP message indicating that IM Exit is not possible is sent to the MS on the air interface.
$T_{R4\_Path\_Reg}$	ASN DPF	ASN DPF indicates to the downstream DPF (ASN-GW or BS), the failure of data path setup for the MS in the "R4 and R6 *Path_Reg_Rsp* messages.
$T_{R4\_Path\_Ack}$	ASN DPF	ASN DPF indicates to the downstream ASN DPF, the failure of data path setup for the MS in the R4 *Path_Reg_Rsp* message.
$T_{R6\_Path\_Ack}$	Serving ASN DPF	Serving ASN DPF indicates to the BS, the failure of data path setup for the MS in the R6 *Path_Reg_Rsp* message

4.10.4.1.2.2   AK Context Generation Error

The Anchor Authenticator generates AK and AK Context information upon receipt of the R4 *IM_Exit_State_Change_Req*. If the Anchor Authenticator is unable to generate this information, it sends the AK Response with failure code to the Anchor PC. This is done by explicitly including the Failure Indication TLV in the response message. Upon receipt of the response with failure indication at the Anchor PC, the timer $T_{IM\_Exit\_Ctx\_Req\_PC}$ is stopped and the IM exit state change Response is sent to the relay PC with the inclusion of the failure indication – thereby indicating to the relay PC that there has been an AK Context generation error. This is further propagated to the BS which sends the appropriate failure code to the MS on R1 via RNG-RSP message.

4.10.4.1.2.3   R6 Data Path Establishment Error

This error refers to the inability of establishing the data path on the R6 interface. When this error occurs, the DPF where the error occurs includes a Failure indication TLV in the R6 *Path_Reg_Rsp* message back to the BS. The BS, upon receipt of the message, sends the appropriate failure code to the MS on R1 via RNG-RSP message

4.10.4.1.2.4   R4 Data Path Establishment Error

This error refers to the inability of establishing the data path on the R4 interface. When this error occurs, the DPF where the error occurs includes a Failure indication TLV in the R4 *Path_Reg_Rsp* message back to the downstream ASN DPF. When the downstream DPF receives this message with the failure indication, the error is propagated further downstream to the BS which sends the appropriate failure code to the MS on R1 via RNG-RSP message

4.10.4.2   Idle Mode Exit – Serving ASN Has MS Context

As per IEEE 802.16e, when the MS enters idle mode, the BS in the serving ASN starts a timer – "Management Resource Holding Timer". The BS retains all of the R1 context and the R4, R6 data paths for this MS until the timer has expired or until the context is revoked by the Anchor PC. The Anchor PC SHALL send a control message – *Delete_MS_Entry_Req* to the serving BS to revoke the MS context if the MS has entered the network at a different BS before the management resource holding timer at the serving BS expires. How the anchor PC determines whether the management resource holding timer has expired at the serving BS is an implementation issue.

If the context in the serving BS is not revoked before the management resource holding timer expires, the serving BS SHALL release the MS context and the data paths for this MS only at the expiry of this timer.

In certain cases the MS may decide to exit idle mode before this timer expires and/or before the MS context is revoked from the serving BS. In such a case, the procedure for the MS to exit idle mode can be further simplified and is illustrated in Figure 4-79.

1
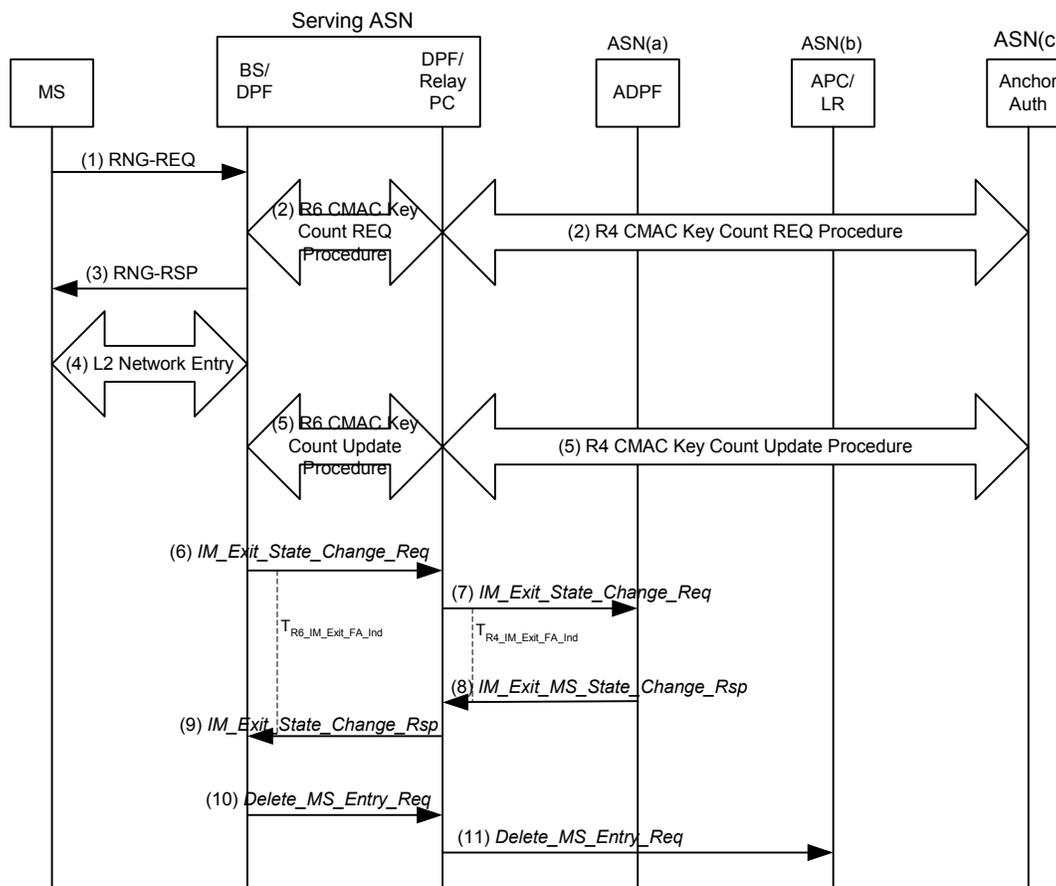
Figure 4-79 – Idle Mode Exit Procedure when the Management Resource Holding Timer has not Expired and when the MS State Stored at the BS is not Revoked by the Anchor PC

The steps in the above procedure are detailed below:

STEP 1

The MS sends a RNG-REQ to enter back into the network from Idle mode before the timer expires.

STEP 2

The BS sends R4 and R6 messages to the Anchor Authenticator in ASN(c) via the serving ASN, to retrieve the CMAC Key count for the MS. The procedure for this operation is described in section 4.13. The Anchor Authenticator responds back with the CMAC key count.

STEP 3

The BS has the required context now and the data paths retained for this MS since Resource Retain Timer is not expired. Hence it authenticates the MS and sends RNG-RSP back to the MS.

STEP 4

The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification.

STEP 5

The BS updates the Anchor Authenticator in ASN(c) with the CMAC Key count for the MS via the serving ASN. The procedure for this operation is described in section 4.13. The Anchor Authenticator acknowlegdes the update.

1 **STEP 6**

2 The BS SHALL send R6 *IM_Exit_State_Change_Req* to the DPF in the serving ASN-GW to indicate the MS
3 exiting the idle mode before the timer expiry. Timer $T_{R6\_IM\_Exit\_FA\_Ind}$ is started at this point by the BS to monitor the
4 response for this message.

5 **STEP 7**

6 The DPF in the serving ASN SHALL send the coresponding R4 *IM_Exit_State_Change_Req* to the Anchor DPF in
7 ASN(a) to indicate the MS exiting the idle mode before the Resource Retain Timer expiry. Timer $T_{R4\_IM\_Exit\_FA\_Ind}$ is
8 started at this point by the serving ASN DPF to monitor the response for this message.

9 **STEP 8**

10 The Anchor DPF in ASN(a) SHALL respond with R4 *IM_Exit_State_Change_Rsp* to the DPF in the serving ASN.
11 Once the serving ASN DPF receives this message, timer $T_{R4\_IM\_Exit\_FA\_Ind}$ is stopped.

12 **STEP 9**

13 The DPF in the serving ASN-GW SHALL forward the recieved message as R6 *IM_Exit_State_Change_Rsp* to the
14 BS. Once the BS receives this message, timer $T_{R6\_IM\_Exit\_FA\_Ind}$ is stopped.

15 **STEP 10**

16 The BS SHALL send the R6 *Delete_MS_Entry_Req* to the relay PC in the serving ASN-GW, to remove the entry of
17 this MS from the LR database in the anchor PC.

18 **STEP 11**

19 The relay PC in the serving ASN SHALL send the R4 *Delete_MS_Entry_Req* to the Anchor PC/LR in ASN(b) to
20 remove the entry of this MS from the LR database in the anchor PC.

21 **4.10.4.2.1 Timers and Timing Considerations**

22 This section identifies the timer entities participating in the IM exit procedure. The IM exit procedure definition
23 shown in Table 4-123 employs the following timers:

24 • $T_{R6\_IM\_Exit\_FA\_Ind}$: is started by a BS upon sending the R6 *IM_Exit_State_Change_Req* message to the
25 serving DPF in the ASN-GW. It is stopped upon receiving a corresponding response.

26 • $T_{R4\_IM\_Exit\_FA\_Ind}$: is started by a serving DPF entity in the ASN upon sending the R4
27 *IM_Exit_State_Change_Req* message to the anchor DPF. It is stopped upon receiving a corresponding
28 response.

29 Table 4-123 shows the default value of timers and also indicates the range of the recommended duration of these
30 timers. Note that these values are provisioned in Release 1.0.0.

31 **Table 4-123 – Timer Values for IM Exit Messages over R4**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_IM\_Exit\_FA\_Ind}$	TBD		TBD
$T_{R4\_IM\_Exit\_FA\_Ind}$	TBD		TBD

32 **4.10.4.2.2 Fast Idle Mode Exit Error Conditions**
33 This section describes error conditions associated with the IM exit procedure.

1   **4.10.4.2.2.1   Timer Max Retries**

2   Table 4-124 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
3   expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
4   should be performed as indicated in Table 4-124:

5   **Table 4-124 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Exit\_FA\_Ind}$	BS	RNG-RSP message indicating that IM Exit is not possible is sent to the MS on the air interface.
$T_{R4\_IM\_Exit\_FA\_Ind}$	Serving ASN DPF	The Serving ASN DPF sends the appropriate failure code downstream to the BS in the R6 *IM_Exit_State_Change_Rsp* message

6   **4.10.4.3   IM Exit Message Tables**

7   **Table 4-125 – Delete_MS_Entry_Req**

IE	Description	M/O	Notes

8   **Table 4-126 – R6 IM_Exit_State_Change_Req**

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	ID of the BS from which MS is initiating Idle mode Exit.
Anchor PCID	Paging Controller Identification	M	PC ID points to MS's anchor Paging Controller, as obtained from the RNG-REQ message

9   **Table 4-127 – R6 Path_Reg_Req**

IE	Description	M/O	Notes
Anchor DPF ID		M	
SFInfo	Contains ServiceFlow information in the nested IEs	O	One or more of the SF Info are optional based on whether they were stored as part of the Idle mode retain information for the MS

10   **Table 4-128 – R6 Path_Reg_Rsp**

IE	Description	M/O	Notes
DataPath Info		M	
SFInfo	Contains ServiceFlow information in the nested IEs	O	One or more of the SF Info are optional based on whether they were stored as part of the Idle mode retain information for the

IE	Description	M/O	Notes
			MS
Tunnel Parameters	Tunnel parameters for the MS	M	Tunnel parameters for the MS
Failure Indication	Transaction Failure	O	Data path not established. Code value = 5.

1

Table 4-129 – R6 Path_Reg_Ack

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the Serving BS performing operation

2

3

Table 4-130 – R4 IM_Exit_State_Change_Req

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	ID of the BS from which MS is initiating Idle mode Exit.

4

Table 4-131 – R4 IM_Exit_State_Change_Rsp

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	ID of the BS from which MS is initiating Idle mode Exit.
Anchor DPF/FA ID	Anchor DPF/FA of the MS	M	Anchor DPF/FA of the MS
IDLE Mode Retain Info	IDLE Mode Retain Info	M	IDLE Mode Retain Info
SBC context	Related context with SBC_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005
REG context	Related context with REG_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005
PKM context	Related context with PKM_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005
Authenticator ID	Anchor Authenticator of the MS	M	Anchor Authenticator of the MS.
MS SF context	MS SF info	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005
AK Context	AK and AK Context	M	AK, AKID, Lifetime, AK Sequence, EIK
CMAC Key count	CMAC Key count	M	CMAC Key count for the MS
Failure Indication	Requested context	O	Code value = 32. Included in the event of

IE	Description	M/O	Notes
	unavailable		failure

1 **Table 4-132 – R4 Path_Reg_Req**

IE	Description	M/O	Notes
SFInfo	Contains Service Flow information in the nested IEs	O	One or more of the SF Info are optional based on whether they were stored as part of the Idle mode retain information for the MS

2 **Table 4-133 – R4 Path_Reg_Rsp**

IE	Description	M/O	Notes
SFInfo	Contains Service Flow information in the nested IEs	O	One or more of the SF Info are optional based on whether they were stored as part of the Idle mode retain information for the MS
Tunnel Parameters	Tunnel parameters for the MS	M	Tunnel parameters for the MS
Failure Indication	Transaction Failure	O	Data path not established. Code value = 5.

3 **4.10.5 Idle Mode Entry**

4 Both MS and the network may initiate the procedure of entering Idle Mode.

1 **4.10.5.1 MS Initiated Idle Mode Entry**
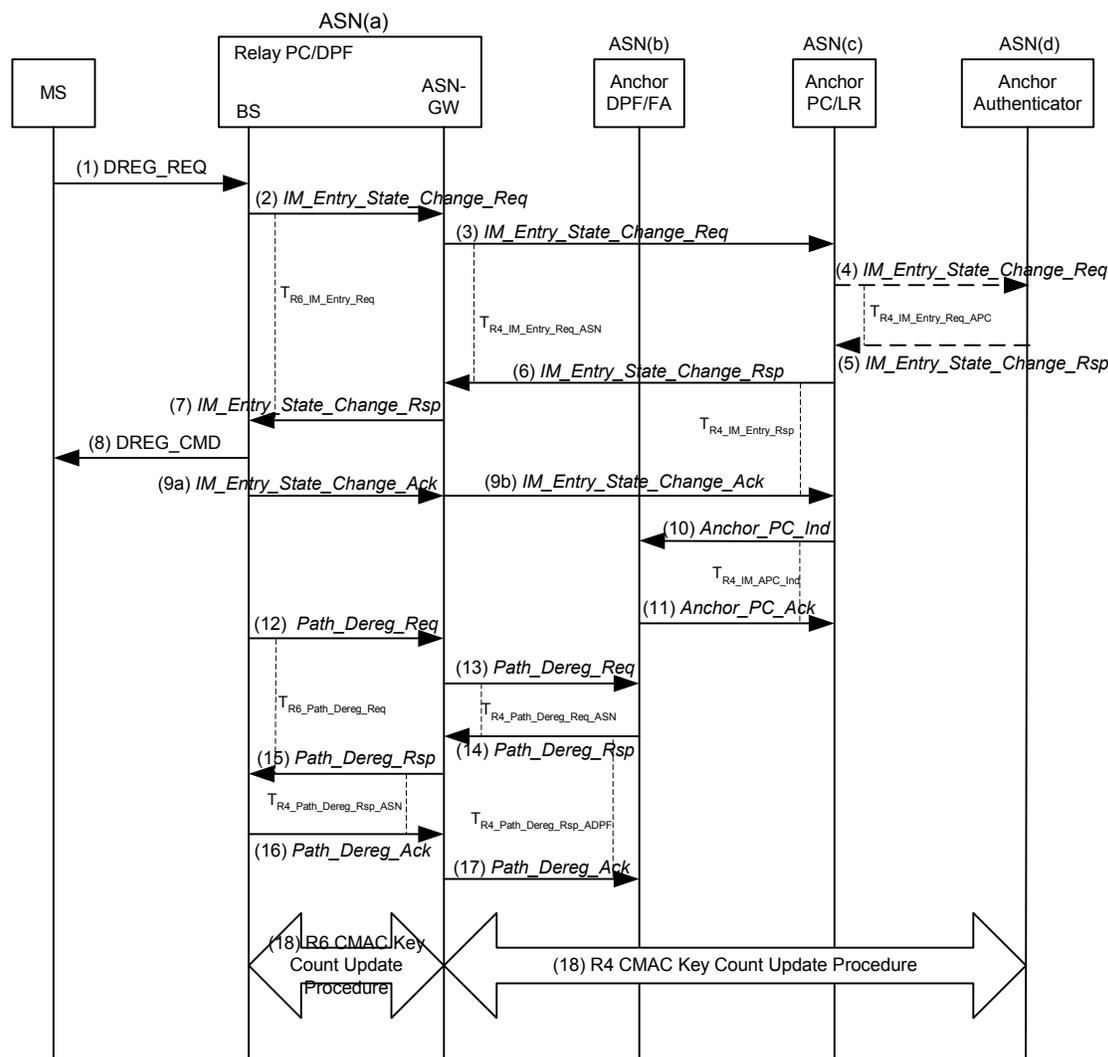
2

3 **Figure 4-80 – MS Initiated Idle Mode Entry**

4 **STEP 1**

5 MS decides to enter Idle Mode and sends DREG_REQ formatted as described in IEEE 802.16e. The De-
6 Registration Request code is set to 0x01 indicating that the MS intends to enter Idle Mode

7 **STEP 2**

8 Based on the MS's request, the BS(PA) in ASN(a) sends an R6 *IM_Entry_State_Change_Req* message to its ASN-
9 GW. Timer $T_{R4\_IM\_Entry\_Req}$ is started to monitor R6 *IM_Entry_State_Change_Rsp* at the BS(PA).

10 **STEP 3**

11 The local Relay PC in ASN(a) chooses an Anchor PC for the MS and sends inter-ASN R4
12 *IM_Entry_State_Change_Req* message to the ASN(c) associated with the chosen Anchor PC. Timer
13 $T_{R4\_IM\_Entry\_Req\_ASN}$ is started to monitor the R4 *IM_Entry_State_Change_Rsp*.

STEP 4

ASN(c), which includes the Anchor PC/LR, sends R4 *IM_Entry_State_Change_Req* to ASN(d) associated with Anchor Authenticator to verify whether MS is allowed to go in to Idle mode. Timer $T_{R4\_IM\_Entry\_Req\_APC}$ is started at this time to monitor the R4 *IM_Entry_State_Change_Rsp* from the Anchor Authenticator. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN.

STEP 5

ASN(d) associated with Anchor Authenticator checks if the MS is allowed to enter Idle Mode and saves necessary information if allowed, then sends back R4 *IM_Entry_State_Change_Rsp* to ASN(c) associated with Anchor PC/LR including MSID, IDLE mode authorization indication. If Anchor Authenticator rejects the Idle mode entry request, the Idle Mode Authorization TLV will contain the rejection code. When R4 *IM_Entry_State_Change_Rsp* for MS entering Idle Mode is send successfully, Anchor Authenticator stores Anchor PC ID for this MS. Upon reception of this message at Anchor PC, $T_{R4\_IM\_Entry\_Req\_APC}$ is stopped. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN.

STEP 6

According to the reported information in R4 *IM_Entry_State_Change_Rsp*, based on the content of Idle mode authorization indication IE, ASN(c) associated with Anchor PC updates the LR with current MS location information (PGID) and other parameters, and sends back R4 *IM_Entry_State_Change_Rsp* message to ASN(a). When this message is received at AN(a) timer $T_{R4\_IM\_Entry\_Req\_ASN}$ is stopped.

STEP 7

ASN(a) forwards the R6 *IM_Entry_State_Change_Rsp* to serving BS(PA) including IDLE Mode authorization indication and accepted Paging parameters. Upon reception of this message at the BS, timer $T_{R6\_IM\_Entry\_Req}$ is stopped.

STEP 8

BS sends DREG_CMD to the MS as specified in IEEE 802.16e. The DREG_CMD conveys "PC ID" field pointing to Anchor PC for the MS and allocated Idle mode parameters.

STEP 9

9a: After sending the DREG_CMD to the MS, the BS(PA) acknowledges the successful delivery of DREG_CMD to the local Relay PC in ASN(a) by sending R6 *IM_Entry_State_Change_Ack* .

9b: The local Relay PC in ASN(a) forwards the successful entry of MS in to Idlemode to the Anchor PC in ASN(c) by sending R4 *IM_Entry_State_Change_Ack*. Upon reception of this message at Anchor PC, timer $T_{R4\_IM\_Entry\_Rsp}$ is stopped.

STEP 10

ASN(c) associated with Anchor PC/LR updates the information of MS into LR database and SHALL send Anchor PC Indication message to ASN(b) associated with Anchor DPF/FA to reflect the success of MS entering Idle Mode. Timer $T_{R4\_APC\_Ind}$ is started at this time when Anchor PC Indication is send, to monitor the response.

STEP 11

The ASN(b) associated with Anchor DPF/FA finally updates the information of MS including the Anchor PC ID of this MS and acknowledges to the Anchor PC/LR by Anchor PC Ack message. When Anchor PC Ack is received at ASN(c) timer $T_{R4\_APC\_Ind}$ is stopped.

STEP 12

After the expiration of the Management Resource Holding Timer (an 802.16e parameter), BS initiates the related R6 data Path Dereg procedure by sending R6 *Path_Dereg_Req* to the ASN(a). After sending *Path_Dereg_Req* to the ASN(a) the BS starts timer $T_{R6\_Path\_Dereg\_Req}$ to monitor the reponse.

STEP 13

ASN-GW in ASN(a) forwards the message as R4 Path Dereg Req to the ASN(b) associated with the Anchor DPF/FA. Timer $T_{R4\_Path\_Dereg\_Req}$ is started in ASN(a) to monitor the reponse of this message.

STEP 14

ASN(b) completes the Path deregistration process for this MS and gives the response the message R4 Path Dereg Response to ASN(a). ASN(a) stops the timer $T_{R4\_Path\_Dereg\_Req}$ on receipt of this message.

STEP 15

ASN-GW in ASN(a) forwards the message to the BS(PA) as R6 Path Dereg Response. Upon reception of this message $T_{R6\_Path\_Dereg\_Req}$ is stopped. ASN(a) starts timer $T_{R4\_Path\_Dereg\_Rsp}$ to wait for the *Path_Dereg_Ack* message from the BS(PA).

STEP 16

The BS(PA) completes the Data Path Dereg process for this MS and acknowledges it by sending R6 *Path_Dereg_Ack* to the ASN(a). ASN(a) stops the timer $T_{R4\_Path\_Dereg\_Rsp.}$

STEP 17

ASN(a) completes the data path deregistration from its side and send R4 *Path_Dereg_Ack* to ASN(b) associated with Anchor DPF/FA. Upon reception of this message ASN(b) stops timer $T_{Path\_Dereg\_Rsp\_ADPF}$

STEP 18

The BS(PA) updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN as per the CMAC Key count update procedure in section 4.13. The Anchor Authenticator acknowledges the CMAC update for the MS. Optionally this procedure may be invoked anytime after step 11.

1 **4.10.5.2 Network Initiated Idle Mode Entry**
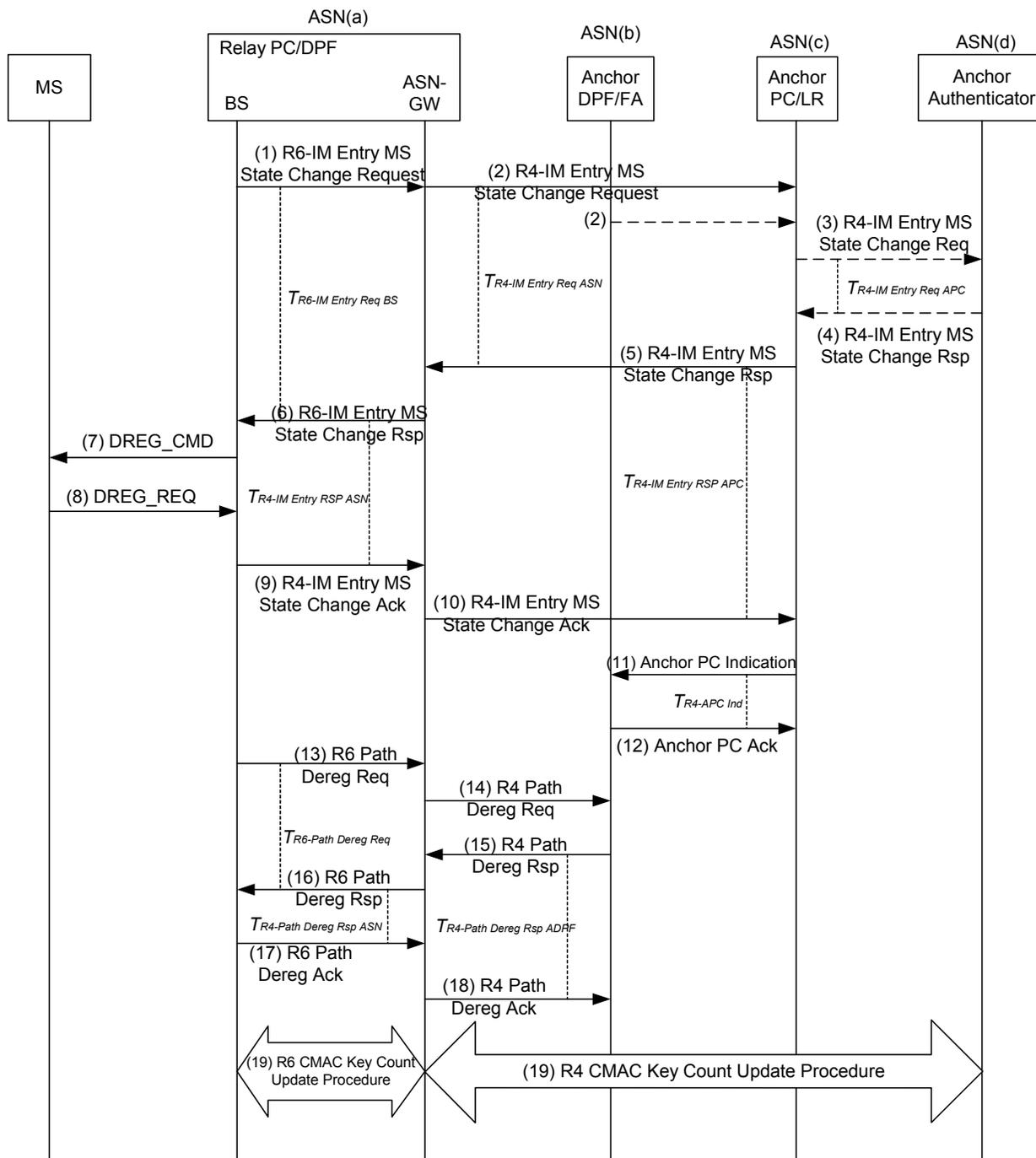
3 **Figure 4-81 – Network Initiated Idle Mode Entry**

4 Network may also initiate the MS Idle Mode Entry procedure. Network initiated Idle Mode entry is triggered by
5 Serving ASN. The exact trigger conditions are implementation specific and out of scope of this specification.

STEP 1

The Serving BS(PA) decides to trigger MS entering Idle Mode, and sends R6 *IM_Entry_State_Change_Req* to the serving ASN-GW in ASN(a). The timer $T_{R6\_IM\_Entry\_Req}$ is started by the BS(PA) to monitor the response message.

STEP 2

The Relay PC in ASN(a) associated with the Serving BS/PA will check the received message and recommends an Anchor PC and paging information for the MS. If the recommended Anchor PC is not itself, it forwards the message to the chosen Anchor PC as R4 *IM_Entry_State_Change_Req*. To help the Anchor PC to choose and confirm the paging parameters for the MS this message may include suggested parameters. Timer $T_{R4\_IM\_Entry\_Req\_ASN}$ is started in ASN(a) to monitor the R4 *IM_Entry_State_Change_Rsp*.

STEP 3

According to the reported info, the Anchor PC in ASN(c) will temporarily save current MS location information (BSID, Relay PC ID, PGID etc) and other parameters, and sends R4 *IM_Entry_State_Change_Req* message to the MS's Anchor authenticator to verify whether the MS is allowed to enter Idle mode. Timer $T_{R4\_IM\_Entry\_Req\_APC}$ is started to monitor the R4 *IM_Entry_State_Change_Rsp* from the Authenticator.

STEP 4

ASN(d) associated with Anchor Authenticator checks if the MS is allowed to enter Idle Mode and save necessary information if allowed, then sends back R4 *IM_Entry_State_Change_Rsp* to ASN(c) associated with Anchor PC/LR including MSID, Idle mode Authorization indication. If Idle mode entry is not allowed the Idle mode Authorization TLV will contain a rejection code. If the Authenticator fails to retrieve the security context or there is any other error with the message, the response message will contain an error code. Upon reception of this R4 *IM Entry_MS_State_Change_Rsp* message at Anchor PC, timer $T_{IM\_Entry\_Req\_APC}$ is stopped.

STEP 5

ASN(c) associated with Anchor PC/LR forwards the R4 *IM_Entry_State_Change_Rsp* message to ASN(a) associated with the local Relay PC. Upon reception of this message at ASN(a), timer $T_{R4\_IM\_Entry\_Req\_ASN}$ is stopped.

STEP 6

Relay PC in ASN(a) forwards the message as R6 *IM_Entry_State_Change_Rsp* message to related Serving BS(PA). To wait for the acknowledgement to this message ASN(c) starts $T_{R4-IM\ Entry\ Rsp\_ASN}$. When the serving BS(PA) receives this message it stops the timer $T_{R6\_IM\_Entry\_Req}$.

STEP 7

The serving BS(PA) sends DREG_CMD to the MS as specified in IEEE 802.16e, asking it to enter Idle mode. The "PC ID" field in DREG_CMD will contain the Anchor PC for the MS as well as other paging parameters for the MS operation in Idle mode.

STEP 8

MS sends DREG_REQ to the BS(PA) as specified in IEEE 802.16e., acknowledging the Idle mode entry.

STEP 9

Upon reception of DREG_REQ from MS, the BS(PA) sends R6 *IM_Entry_State_Change_Ack* to Relay PC in ASN(a) to notify that the MS has successfully entered Idle Mode. (Note: Here in this call flow a success scenario of MS agreement to Idle mode entry is assumed.)

1 **STEP 10**

2 The Relay PC in ASN(a) forwards the message as R4 *IM_Entry_State_Change_Ack* to the Anchor PC in ASN(c) to
3 indicate that the MS has successfully entered Idle mode and update the status. Upon reception of this message at
4 ASN(c) timer $T_{R4\_IM\_Entry\_Rsp\_APC}$ is stopped.

5 **STEP 11**

6 ASN(c) associated with Anchor PC/LR will update the Idle mode information of MS into LR database and SHALL
7 send R4 *Anchor_PC_Ind* message to ASN(b) associated with Anchor DPF/FA to confirm the success of MS
8 entering Idle Mode. ASN(c) starts timer $T_{R4\_APC\_Ind}$ to monitor the response from ASN(b).

9 **STEP 12**

10 The ASN(b) associated with Anchor DPF/FA finally updates the information of MS including the Anchor PC ID of
11 this MS and SHALL confirm the procedure by sending R4 *Anchor_PC_Ack* to the ASN(c). ASN(c) stops timer
12 $T_{R4\_APC\_Ind}$ at the receipt of this Anchor PC Ack.

13 **STEP 13**

14 After the expiration of the Management Resource Holding Timer (an 802.16e parameter), BS initiates the related
15 R6data Path Dereg procedure. by sending R6 Path Dereg Req to the ASN-GW in serving ASN(a). After sending
16 *Path_Dereg_Req* to the ASN(a) the BS starts timer $T_{R6\_Path\_Dereg\_Req}$ to monitor the reponse.

17 **STEP 14**

18 ASN-GW in ASN(a) forwards the message as R4 Path Dereg Req to the ASN(b) associated with the Anchor DPF/FA. Timer
19 $T_{R4\_Path\_Dereg\_Req\_ASN}$ is started in ASN-GW to monitor the reponse of this message.

20 **STEP 15**

21 ASN(b) completes the Path deregistration process for this MS and gives the response the message R4 Path Dereg Response to
22 ASN(a). ASN-GW in ASN(a) stops the timer $T_{R4\_Path\_Dereg\_Req\_ASN}$ on receipt of this message.

23 **STEP 16**

24 ASN(a) forwards the message to the BS as R6 Path Dereg Response. Upon reception of this message $T_{R6\text{-}Path\ Dereg\ Req}$
25 is stopped. ASN-GW in ASN(a) starts timer $T_{R4\_Path\_Dereg\_Rsp\_ASN}$ to wait for the *Path_Dereg_Ack* message from the
26 serving BS.

27 **STEP 17**

28 The BS completes the Data Path Dereg process for this MS and acknowledges it by sending R6 *Path_Dereg_Ack* to
29 the ASN-GW in ASN(a). ASN-GW stops the timer $T_{R4\_Path\_Dereg\_Rsp\_ASN}$ upon receipt of this message.

30 **STEP 18**

31 ASN-GW in ASN(a) completes the data path deregistration from its side and send R4 *Path_Dereg_Ack* to ASN(b)
32 associated with Anchor DPF/FA. Upon reception of this message ASN(b) stops timer $T_{R4\_Path\_Dereg\_Rsp\_ADPF}$

33 **STEP 19**

34 The BS(PA) updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN as per
35 the CMAC Key count update procedure in section 4.13. The Anchor Authenticator acknowledges the CMAC update
36 for the MS. Optionally this procedure may be invoked anytime after step 12,.

37 **4.10.5.3 Idle Mode Entry Timers and Timing Considerations:**

38 This section defines the timer entities defined for the Idle Mode entry procedure. The following timers are defined
39 over R4 and R6 interfaces.

1   • $T_{R6\_IM\_Entry\_Req}$: Started by the Serving BS when it sends R6 *IM_Entry_State_Change_Req* message to its
2   ASN-GW. This timer is stopped when ASN-GW response R6 *IM_Entry_State_Change_Rsp* is received.

3   • $T_{R4\_IM\_Entry\_Req\_ASN}$: Started by the Serving ASN when it sends R4 *IM_Entry_State_Change_Req* message.
4   This timer is stopped when ASN-GW response R4 *IM_Entry_State_Change_Rsp* is received.

5   • $T_{R4\_IM\_Entry\_Req\_APC}$: Started by the Anchor PC/LR when it sends R4 *IM_Entry_State_Change_Req* message
6   to the Authenticator. This timer is stopped when Authenticator responds with R4
7   *IM_Entry_State_Change_Rsp*.

8   • $T_{R4\_APC\_Ind}$: Started by the Anchor PC/LR when it sends R4 *Anchor_PC_Ind* to the Anchor DPF/FA. This
9   timer stopped when Anchor PC Ack is received.

10   • $T_{R4\_Path\_Dereg\_Req\_ASN}$: Started by the Serving ASN-GW when it sends R4 *Path_Dereg_Req* message to the
11   Anchor DPF/FA. This timer is stopped when Anchor DPF/FA response R4 *Path_Dereg_Rsp* is received.

12   • $T_{R6\_Path\_Dereg\_Req}$: Started by the Serving BS when it sends R4 *Path_Dereg_Req* message to the Anchor
13   DPF/FA. This timer is stopped when serving ASN-GW response R6 *Path_Dereg_Rsp* is received.

14   • $T_{R4\_Path\_Dereg\_Rsp\_ASN}$: Started by the Serving ASN when it sends R6 *Path_Dereg_Rsp* message to the serving
15   BS. This timer is stopped when serving BS response R6 *Path_Dereg_Ack* is received.

16   • $T_{R4\_Path\_Dereg\_Rsp\_ADPF}$: Started by the ADPF when it sends R4 *Path_Dereg_Rsp* message to the serving ASN.
17   This timer is stopped when serving ASN response R4 *Path_Dereg_Ack* is received.

18 Table 4-134 shows the default value of timers and also indicates the range of the recommended duration of these
19 timers. Note that these values are provisioned in Release 1.0.0.

20 **Table 4-134 – Idle Mode Entry Timer Values for R4 and R6**

Timer	Default Values (msec)	Criteria	Maximum Value
$T_{R6\_IM\_Entry\_Req}$	TBD		TBD
$T_{R4\_IM\_Entry\_Req\_ASN}$	TBD		TBD
$T_{R4\_APC\_Ind}$	TBD		TBD
$T_{R4\_IM\_Entry\_Req\_APC}$	TBD		TBD
$T_{R4\_APC\_Ind}$	TBD		TBD
$T_{R4\_Path\_Dereg\_Req\_ASN}$	TBD		TBD
$T_{R6\_Path\_Dereg\_Req}$	TBD		TBD
$T_{R4\_Path\_Dereg\_Rsp\_ASN}$	TBD		TBD
$T_{R4\_Path\_Dereg\_Rsp\_ADPF}$	TBD		TBD

21 **4.10.5.4 Idle Mode Entry Error Conditions**

22 This section describes error conditions associated with the Idle Mode entry procedure.

23 **4.10.5.5 Timer Max Retries**

24 Table 4-135 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
25 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
26 should be performed as indicated in Table 4-135.

1 **Table 4-135 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Entry\_Req}$	BS(PA)	Idle mode entry procedure is not progressing hence procedure is terminated, MS allowed to be Active. If initiated by MS, DREG_CMD with appropriate action code for either 'continue normal operation' or try after a time out is send out. If network initiated, the BS continues with the normal operation of the MS allowing the MS to be active.
$T_{R4\_IM\_Entry\_Req\_ASN}$	Local Relay PC	Sends R6 *IM_Entry_State_Change_Rsp* with failure indication code 32 to the BS. All actions taken at the ASN-GW/ Relay PC to put MS in Idle state is cancelled, MS allowed to continue in Active state.
$T_{R4\_IM\_Entry\_Req\_APC}$	Anchor PC	Sends R4 *IM_Entry_State_Change_Rsp* with failure indication code 32 to Serving ASN(a). All actions taken at Anchor PC to change the state of MS is cancelled. MS allowed to be Active
$T_{R4\_APC\_Ind}$	Anchor PC	Sends R4 *IM_Entry_State_Change_Req* to Anchor Authenticator to revert back the MS state to active. All actions taken at Anchor PC to change the state of MS is cancelled. MS allowed to be Active
$T_{R4\_IM\_Entry\_Rsp\_Asn}$		Failure indication sent downstream to the serving ASN.

2 **4.10.5.6   AK Context Generation Error**

3 Upon receiving the R4 *IM_Entry_State_Change_Req* message the Anchor Authenticator verfies the MS is allowed
4 to go idle and it is possible for network to support the this MS in Idle mode. If Authenticator makes a decision it is
5 possible and allowed to go idle mode, R4 *IM_Entry_State_Change_Rsp* is given to Anchor PC. generates. If the
6 Anchor Authenticator is unable to generate this information, it sends the AK Response with failure code to the
7 Anchor PC. This is done by explicitly including the Failure Indication TLV in the response message. Upon receipt
8 of the response with failure indication at the Anchor PC, the timer $T_{R4\_IM\_Entry\_Req\_APC}$ is stopped and the
9 *IM_Entry_State_Change_Rsp* is sent to the relay PC with the inclusion of the failure indication – thereby indicating
10 to the relay PC that there has been an AK Context generation error. This is further propagated to the serving BS and
11 ASN-GW which may drop the Idle mode entry procedures.

12 **4.10.5.7   R6 Data Path Deregistration Error**

13 This error refers to the inability of deregistering the data path on the R6 interface. When this error occurs, the DPF
14 where the error occurs includes a Failure indication TLV in the R6 Path Dereg Response message back to the
15 serving BS. The serving BS upon receipt of the message, takes appropriate failure recovery action on the R6
16 datapath which are beyond the scope of this specification.

17 **4.10.5.8   R4 Data Path Deregistration Error**

18 This error refers to the inability of deregistering the data path on the R4 interface. When this error occurs, the DPF
19 where the error occurs includes a Failure indication TLV in the R4 Path Dereg Response message back to the

1 serving ASN. The serving ASN upon receipt of the message, takes appropriate failure recovery action on the R4
2 datapath which are beyond the scope of this specification.

3 **4.10.5.9 IM Entry Message Tables**

4 **Table 4-136 – R6 IM_Entry_State_Change_Req**

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the Serving BS performing operation
IDLE Mode Retain Info	Suggested IDLE Mode Retain Info	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
SBC context	The related context with SBC/REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
REG context	The related context with REG_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
PKM context	The related context with PKM_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
Paging Cycle request	Paging Cycle requested by MS if MS initiated.	O	Included based on the Paging Cycle Request TLV received from MS and if cached in the BS apriori
Paging Information	Paging Information requested by MS	M	Included based on the Paging Information TLV received from MS and if cached in the BS(PA) apriori. If not cached in the BS(PA), the BS(PA) will set the Page Group ID part of the TLV may suggest by including suggested values for Paging cycle and Offset.
SA Context	AK and AK context, SA and SA context	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
SFInfo	Contains Service Flow information in the nested IEs	M	Service Flow Information of the MS
Authenticator ID	Authenticator IDentifier	M	ID of Anchor Authenticator
Anchor DPF/FA ID	Anchor DPF/FA Identifier	M	ID of Anchor DPF/FA

5 **Table 4-137 – R4 Anchor_PC_Ind**

IE	Description	M/O	Notes
IDLE Mode Authorization Indication	IDLE Mode authorization indication	M	Indicate to allow MS entering Idle Mode

IE	Description	M/O	Notes
Anchor PC ID		M	Confirmed Paging Controller ID for the MS entering Idle mode

1   **Table 4-138 – R4 Anchor_PC_Ack**

IE	Description	M/O	Notes
MSID	MS MAC address	O	MS Identification to point what is the required MS

2   **Table 4-139 – R4 IM_Entry_State_Change_Req**

IE	Description	M/O	Notes
BS ID	Base Station Identification	M	BS ID indicating the Serving BS performing operation
IDLE Mode Retain Info	Idle mode retain info defined in .16e	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005 . Optionally included in this R4 message if present in the corresponding R6 message.
SBC context	Related context with SBC_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005. Optionally included in this R4 message if present in the corresponding R6 message.
REG context	Related context with REG_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005. Optionally included in this R4 message if present in the corresponding R6 message.
PKM context	Related context with PKM_REQ/RSP	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005. Optionally included in this R4 message if present in the corresponding R6 message.
Paging Information	Paging Information	M	Paging Information TLV obtained from the MS containing PAGING_CYCLE, PAGING OFFSET, and Paging Group ID. The local Relay PC may make a suggestion for PAGING_CYCLE and OFFSET but the Paging Group ID part of the TLV is mandatory.
SA Context	SA and SA context	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005 .

IE	Description	M/O	Notes
			Optionally included in this R4 message if present in the corresponding R6 message.
SFInfo	Contains Service Flow information in the nested IEs	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005 . Optionally included in this R4 message if present in the corresponding R6 message.
Paging Cycle Request	Paging Cycle Request	O	Included based on the bits set in the Idle mode retain information TLV from the MS.See IEEE 802.16e-2005. Optionally included in this R4 message if present in the corresponding R6 message.
Anchor PC ID	Anchor Paging Controller Identifier	M	Recommended Anchor PC ID by the Relay PC.
Anchor DPF/FA ID	IP address of ASN-GW associated with Anchor DPF/FA	M	
Authenticator ID	Authenticator IDentifier	M	

1 **Table 4-140 – R4 IM_Entry_State_Change_Rsp**

IE	Description	M/O	Notes
BS ID	Identification of the serving BS	M	BS ID indicating the Serving BS performing operation. (To indicate destination BS for a relayed message, this IE is needed)
Paging Information	Paging Information	M	Paging Information TLV meant for the DREG-CMD to the MS containing PAGING_CYCLE, PAGINGOFFSET, and Paging Group ID Confirmed and stored by the Anchor PC.
Anchor PC ID	Anchor Paging Controller Identifier	O	Included if Paging Controller ID different than the APC received in R4 *IM_Entry_State_Change_Req* message
Idle Mode Authorization Indication	IDLE Mode authorization indication	M	Indicate whether MS is allowed enter Idle Mode. If Authenticator rejected the *IM_Entry_State_Change_Req*, TLV will contain reject code.
Failure Indication	Requested context unavailable	O	Optional TLV if there is a failure in retrieving the context. Code Value = 32

1 **Table 4-141 – IM_Entry_State_Change_Ack**

IE	Description	M/O	Notes
MSID	MS MAC address	O	MS Identification to point what is the required MS
BS ID	Base Station Identification	M	BS ID indicating the Serving BS performing operation
Anchor PC ID	Anchor Paging Controller Identifier	M	Paging Controller ID Acting as Anchor PC

2 ## 4.10.6 Idle Mode Operation and CSN Anchored Mobility Management

3 Support for Foreign Agent migration in Idle Mode is optional. Support for each of the distinct, different methods of
4 FA migration in Idle Mode is optional.

5 If FA migration in Idle Mode is supported, FA migration in Idle Mode SHALL only occur at an indeterminate,
6 implementation specific time after any successful Secure Location Update.

7 If FA migration in Idle Mode is supported, the network SHALL be aware of the MS mobility management client
8 type, either CMIP or PMIP, and the network topology, and employ the appropriate FA migration method.

9 ### 4.10.6.1 Anchor DPF and FA

10 Anchor DPF and FA are collocated in the event that FA is present (which will be in the case of CMIP4 and PMIP4).
11 In the event that there is no FA present in the network (which will be in the case of MIP6), the Anchor DPF is an
12 independent functional entity. In the case of IPv6 and MIP6, there will be an anchor DPF functional entity that is
13 instantiated at the AR when the IPv6 ISF is established.

14 ### 4.10.6.2 CMIP in Idle Mode

15 Migration of foreign agent while the MS is in idle mode (e.g., when idle mode MS moves or for other
16 implementation reasons) requires that MS exit idle mode and complete network reentry to complete MIP registration
17 procedures [15]. If the MS exits Idle mode to complete MIP registration for FA migration, the network reentry and
18 subsequent Idle mode entry procedures SHALL comply with relevant sections of this document. Figure 4-82 and
19 Figure 4-83 show a FA migration following a successful location update. The FA migration can be initiated by the
20 Anchor PC or the new (target) FA.

21 If FA migration does not occur in Idle mode, data path establishment MAY occur across multiple ASNs when the
22 idle mode MS exit idle mode after moving across ASNs. When the MS exits Idle mode due to incoming or outgoing
23 data to/from the MS, it SHALL perform MIP registration procedures for FA migration and data path optimization
24 across R3 to the HA. The timing for FA migration in this case is implementation and deployment dependent.

25 #### 4.10.6.2.1 FA Migration During Idle Mode: Anchor PC Initiated

26 This call flow shows a FA migration following a successful location update. The MS performs a mobility event (i.e.
27 inter-ASN idle mode handoff) such that it moves to a new serving BS/ASN and perfoms a location update. Upon
28 completion of the Location update procedure the Anchor PC determines that a FA migration is needed and will
29 proceed to initiate paging procedures to exit the MS out of idle mode. Additionally the Anchor PC will also send a
30 trigger to the new FA to initiate sending of the Foreign Agent Advertisement message.

1
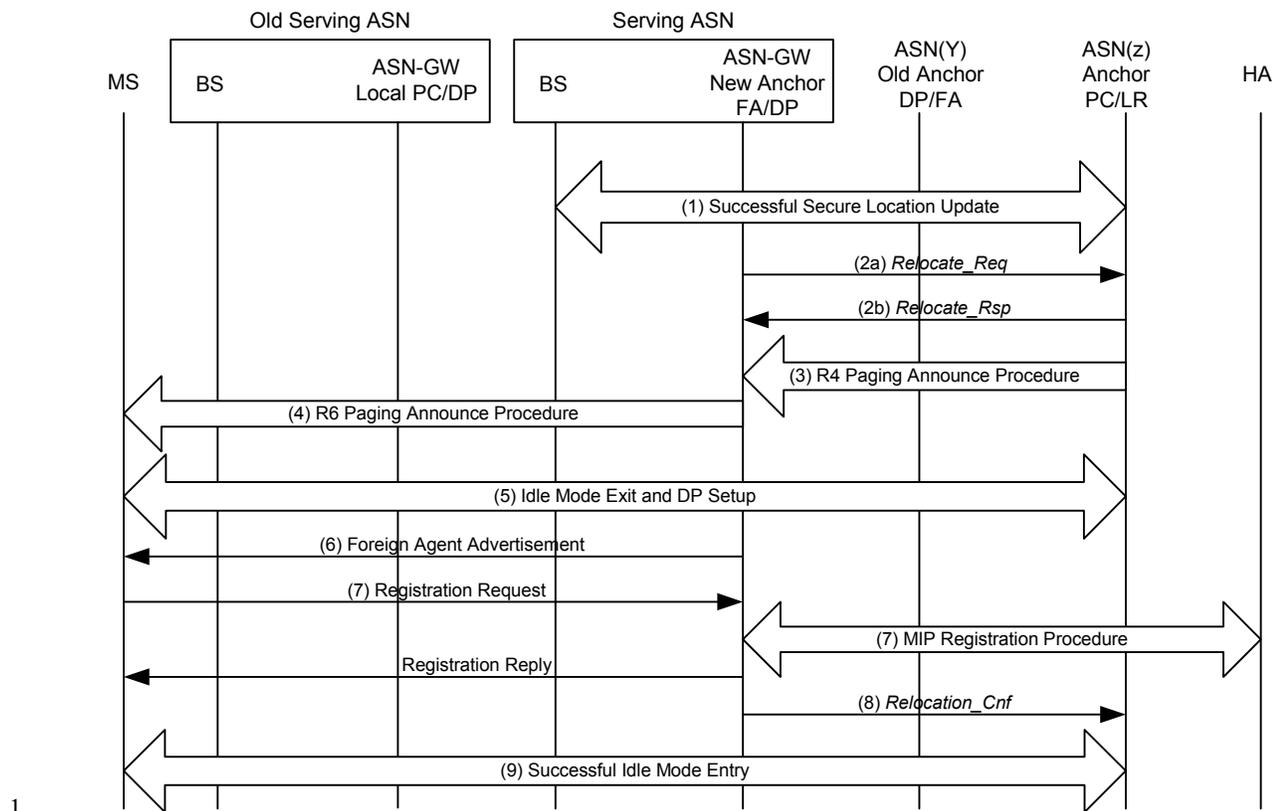
2 **Figure 4-82 – FA Migration During Idle Mode: Anchor PC Initiated**

3 **STEP 1**

4 The MS performs a secure location update with the Anchor PC (see section 4.10.2 for details on this procedure)

5 **STEP 2**

6 The Anchor-PC determines that a FA migration is needed. Details on determination of when a FA migration is
7 needed are outside the scope of this document. The Anchor PC/ASN send R3 *Relocation_Req* message to the new
8 selected FA. In this call scenario is assumed that the selected FA accepts the re-location request and responds with
9 R3 *Relocation_Rsp* message.

10 **STEP 3**

11 The Anchor-PC initiates R4 paging procedures and send R4 *Paging_Announce* message to the Local PC. The
12 Anchor PC includes the new FA ID in the *Paging_Announce* message.

13 **STEP 4**

14 The Local-PC initiates R6 paging procedures with the MS.

15 **STEP 5**

16 The MS performs idle mode exit procedures (as specified in section 4.10.4) and establishes a DP to with the new
17 anchor DPF.

18 **STEP 6**

19 Upon completion of the data path, the new FA sends a Foreign Agent Advertisment message to the MS.

1 **STEP 7**

2 The MS send a registration request message to the FA to perform MIP Rgistration procedures with the HA. The FA
3 sends a registration response message to the MS.

4 **STEP 8**

5 Upon successful registration of the MS with the HA, the FA sends a R3 *Relocation_Cnf* message to the Anchor PC

6 **STEP 9**

7 The Serving ASN initiates network initiated idle mode entry procedures (as specified in section 4.10.5.2) to
8 transition the MS to the idle mode.

9 **4.10.6.2.2 FA Migration during Idle Mode: New (target) FA Initiated**

10 This call flow shows a FA migration following a successful location update. The MS performs a mobility event (i.e.
11 inter-ASN idle mode handoff) such that it moves to a new serving BS/ASN and perfoms a location update. Upon
12 completeion of the Location update procedure the new (target) FA determines that a FA migration is needed and
13 will trigger the PC to proceed to initiate paging procedures to exit the MS out of idle mode. Upon successful exit
14 from idle mode, the new FA will send the Foreign Agent Advertisement message to the MS.
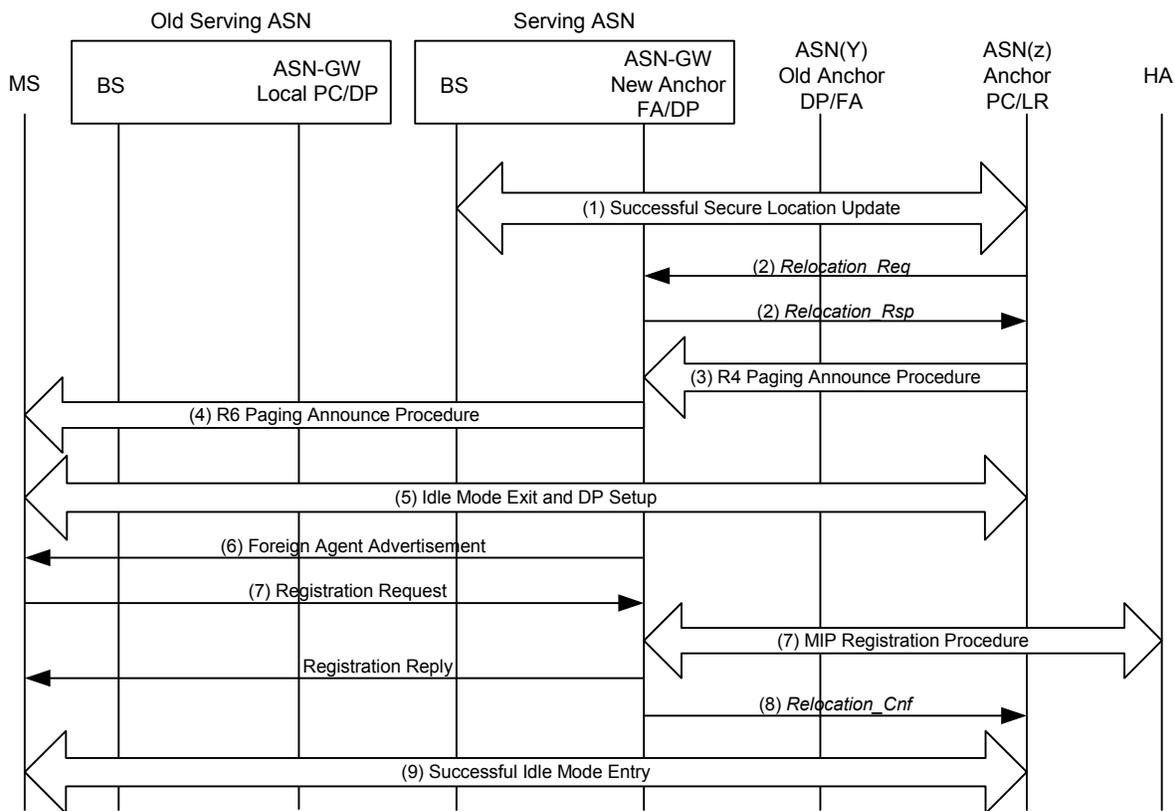
16 **Figure 4-83 – FA Migration During Idle Mode: New (target) FA Initiated**

17 **STEP 1**

18 The MS performs a secure location update with the Anchor PC (see section 4.10.2 for details on this procedure)

1 **STEP 2**

2 The New (Anchor) FA determines that a FA migration is needed. Details on determination of when a FA migration
3 is needed are outside the scope of this document. The New (Anchor) FA send R3 *Relocation_Req* message to the
4 Anchor PC/ASN to trigger paging procedures for the MS. The R3 *Relocation_Req* message contains the FA ID of
5 the New (Anchor) FA. In this call scenario is assumed that Anchor PC accepts the request to trigger Paging for the
6 MS and responds with R3 *Relocation_Rsp* message.

7 **STEP 3**

8 The Anchor-PC initiates R4 paging procedures and send R4 *Paging_Announce* message to the Local PC. The
9 Anchor PC includes the new FA ID in the *Paging_Announce* message.

10 **STEP 4**

11 The Local-PC initiates R6 paging procedures with the MS.

12 **STEP 5**

13 The MS performs idle mode exit procedures (as specified in section 4.10.4) and establishes a DP to with the new
14 anchor DPF.

15 **STEP 6**

16 Upon completion of the data path, the new FA sends a Foreign Agent Advertisment message to the MS.

17 **STEP 7**

18 The MS send a registration request message to the FA to perform MIP Rgistration procedures with the HA. The FA
19 sends a registration response message to the MS.

20 **STEP 8**

21 Upon successful registration of the MS with the HA, the FA sends a R3 *Relocation_Cnf* message to the Anchor PC

22 **STEP 9**

23 The Serving ASN initiates network initiated idle mode entry procedures (as specified in section 5.10.5.2) to
24 transition the MS to the idle mode.

25 **4.10.6.3 PMIP4 in Idle Mode**

26 Migration of FA for an Idle mode MS in a PMIP4 enabled ASN MAY be supported. The migration of the FA MAY
27 be triggered when the MS moves across ASNs.

28 After Secure Location update procedure is complete, either Anchor PC-ASN or Target ASN (New FA) MAY trigger
29 FA migration following the normal CSN MM HO procedure defined in section 4.8.2.3.7.1. The two methods are
30 identified to provide support for topologically aware, and topologically unaware network models, but are not limited
31 to such use.

32 Figure 4-84 illustrates the call flow for FA migration for an Idle Mode MS in a PMIP4 enabled ASN triggered by
33 the Anchor PC-ASN.

34 Figure 4-85 illustrates the call flow for FA migration triggered by Target ASN (New FA) for an Idle Mode MS in a
35 PMIP4 enabled ASN with Anchor MM context retrieving. The Target ASN (New FA) MAY obtain Anchor MM
36 context information through Context Request and Context Report procedures through Anchor PC-ASN without
37 involving the Secure Location Update procedure.

1   **4.10.6.3.1 PMIP4 in Idle Mode – FA Migration Triggered from the Anchor PC-ASN**
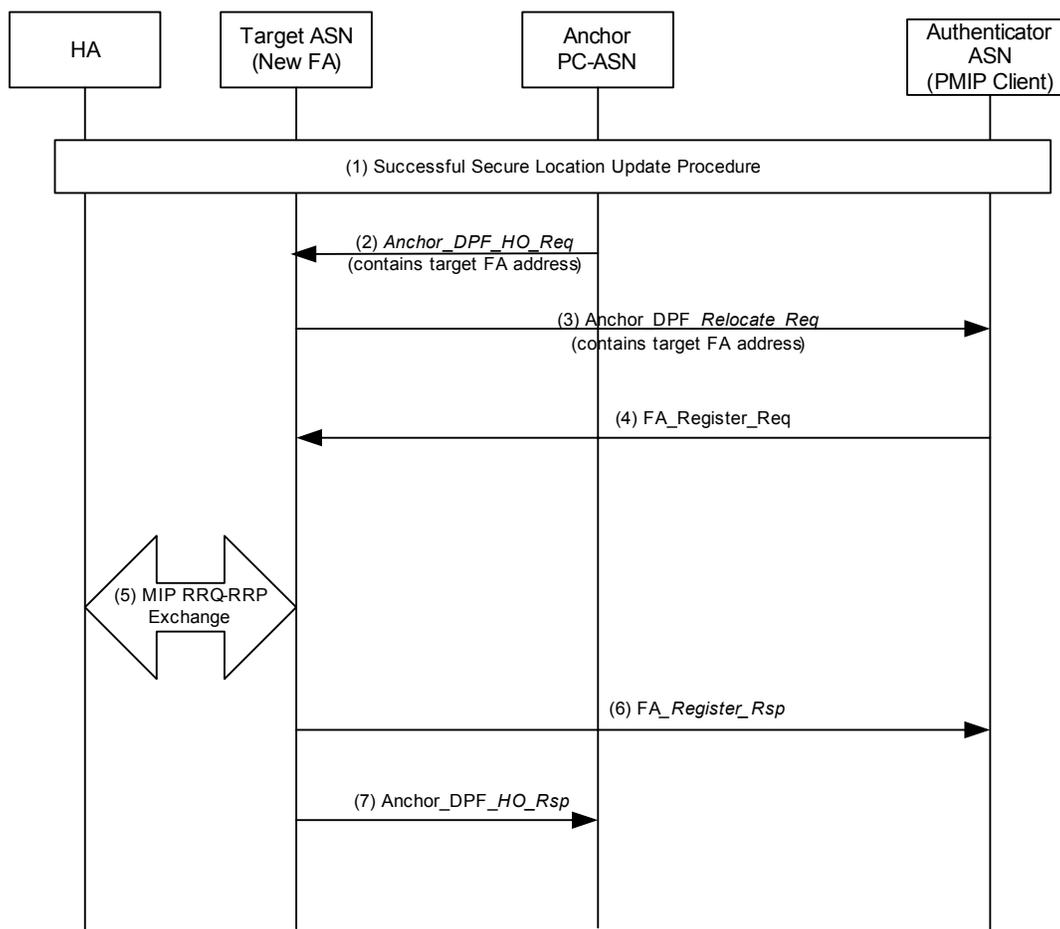
2

3   **Figure 4-84 – Anchor PC-ASN Triggered FA Migration for an Idle Mode MS in a PMIP-enabled ASN**

4   **STEP 1**

5   This depicts a successful Secure Location Update procedure as specified in 4.10.2. An indeterminate,
6   implementation specific time may elapse between Step 1 and Step 2.

7   **STEP 2**

8   The Anchor PC-ASN sends an *Anchor_DPF_HO_Request* to the Target ASN (New FA), to start the FA Migration.
9   This trigger message contains the CoA FA and, optionally, the Target FA that the MS has moved under. The Anchor
10   PC-ASN will obtain the address of the Authenticator ASN (PMIP4 client) as part of the entry idle mode procedure
11   when the MS went idle.

12   **STEP 3**

13   The Target ASN (New FA) sends the Anchor_DPF_Relocate_Req to the Authenticator ASN (PMIP4 client). The
14   message contains CoA for the target FA, and target FA address if it is different than the CoA. In addition to target
15   FA-CoA, current FA-CoA is included in the message.

16   **STEP 4**

17   The PMIP4 client verifies that the current FA-CoA indeed matches the FA on its record, and starts the MIP
18   registration with the target FA by sending FA_Register_Req message.

1 **STEP 5**

2 This depicts the standard MIP RRQ-RRP exchange as specified in the CSN-MM between the Target ASN (New FA)
3 and the HA.

4 **STEP 6**

5 The Target ASN (New FA) sends FA_Register_Rsp message to the PMIP4 client. The PMIP4 client updates the FA
6 in its record.

7 **STEP 7**

8 The Target ASN (New FA) sends Anchor_DPF_HO_Rsp to the Anchor PC-ASN indicating the successful FA
9 migration.

10 **4.10.6.3.2 PMIP4 in Idle Mode – FA Migration triggered from the Target ASN (New FA)**
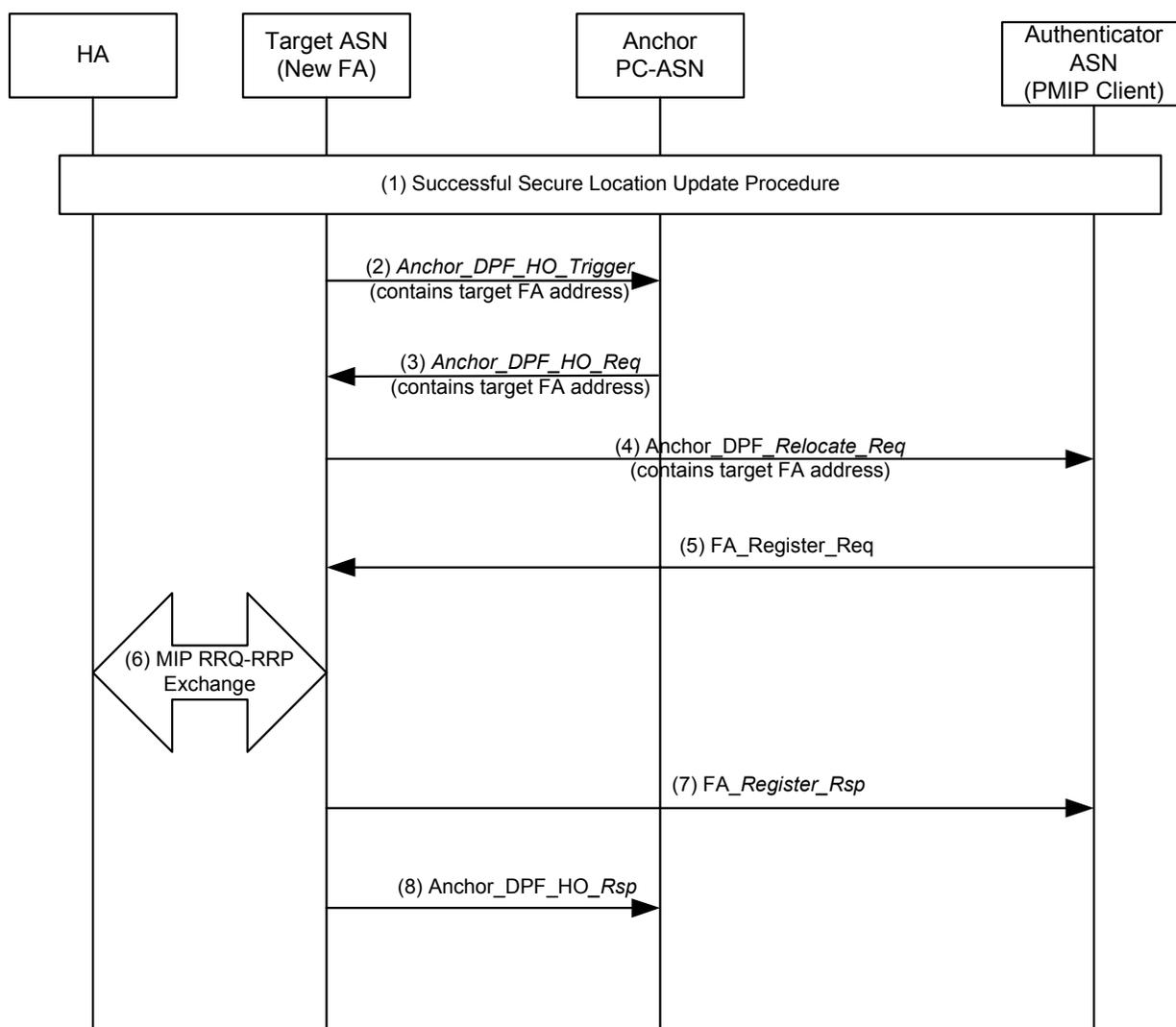
11

12 **Figure 4-85 – Target ASN (New FA) Triggered FA Migration for an Idle Mode MS in a PMIP-enabled**
13 **ASN**

1 **STEP 1**

2 This depicts a successful Secure Location Update procedure as specified in **4.10.2**. An indeterminate,
3 implementation specific time may elapse between Step 1 and Step 2

4 **STEP 2**

5 The Target ASN (New FA) sends *Anchor_DPF_ HO_Trigger* to Anchor PC-ASN to indicate to the Anchor PC for
6 the FA migration for the MS in Idle Mode

7 **STEP 3 to 8**

8 **Same as steps 2 to 7 in section 4.10.6.3.1**.

9 4.11 IPv6

10 IPv6 in WiMAX can be operated in multiple ways. The packet convergence sublayer (CS) specified in the IEEE
11 802.16d/e specification is used for transport of all packet based protocols such as Internet protocol, IEEE Std
12 802.3/Ethernet and, IEEE Std 802.1Q. IPv6 can be run over the IP specific part of the packet CS or alternatively
13 over the Ethernet (802.3/802.1Q) specific part of the packet CS.. The operation of IPv6 over the IP specific part of
14 the Packet CS is specified in [Reference to IETF I-D: draft-ietf-16ng-ipv6-over-ipv6cs-01] and should be referred to
15 for understanding the basic mechanism. This section provides additional information about IPv6 operation that is
16 WiMAX specific. IPv6 over 802.3 and 802.1Q specific parts of the packet CS are described in [REF draft-riegel-
17 16ng-ip-over-eth-over-80216-01.txt]. It should be noted that only the IP specific part of the packet CS is a
18 mandatory requirement and support for 802.3 and 802.1Q parts of the packet CS is optional.

19 4.11.1 Network Model

20 The default IPv6 router or 1st hop router from the MS perspective is the access router in the ASN. The AR is an
21 entity that resides in an ASN-GW in case of profiles A and C and is a functional entity within the ASN in the case of
22 Profile B. The MS autoconfigures an address based on the prefix advertised by the AR or is assigned an address via
23 DHCPv6. This address is a globally routable address. The routability of this address is via a CSN. Figure 4-86
24 shows the network model for IPv6.
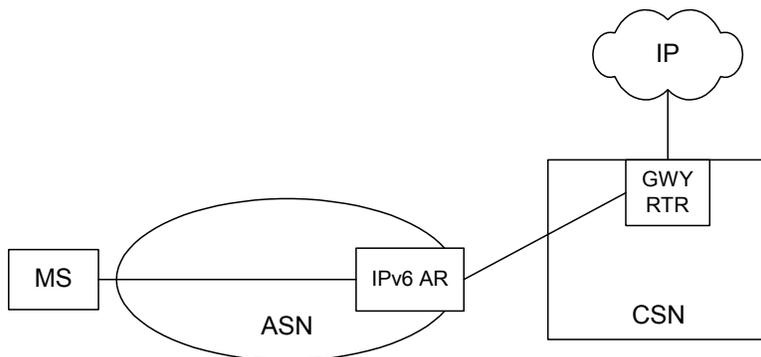
25

26 **Figure 4-86 – IPv6 Network Model**

27 4.11.2 Point to Point Link Between the MS and AR

28 The link between the MS and the AR in the ASN is considered as a point-to-point link for IPv6 over the IP specific
29 part of the packet CS. The combination of the transport connection over the air-interface (MS-BS, i.e. R1) and the
30 L2 tunnel (GRE) over the R6 interface, between the BS and AR, in the case of Profiles A and C forms the point-to-
31 point link. The BS-AR connection in the case of Profile B is unspecified. With the point-to-point type of link
32 underlying the IPv6 layer, each MS is assigned one or more unique IPv6 prefixes. The only entities on the link are
33 the MS and the AR. The granularity of the GRE tunnel between the BS and AR, in the case of profiles A and C,
34 SHALL be on a per MS or per SF basis.

1   The anchor data path function in the AR interfaces with the Anchor paging controller for paging an MS when
2   needed.

4.11.3 IPv6 Link Establishment

4   The mobile station performs initial network entry as described in [refer to network entry procedure in section 4.5].
5   The subscriber profile is downloaded to the ASN as part of the successful completion of the network entry
6   procedure.

7   On completion of the network entry procedure, the initial service flow (ISF) for IPv6 is established by the network.
8   In case of a dual-stack MS which has an IPv4 ISF, the IPv6 ISF is a separate or unique service flow which maps to a
9   unique transport connection identifier over the air interface. The ISF establishment procedure is described in [refere
10   to section TBD]. The trigger or decision to establish the IPv6 ISF is based on the subscriber's profile and indication
11   by the MS in the SBC-REQ message (capability exchange). It is controlled by the SFA in the ASN.

12   The establishment of the IPv6 ISF enables the sending and receiving of IPv6 packets between the MS and the access
13   router in the ASN. On completion of the establishment of the ISF, router advertisements and address assignment
14   procedures are initiated. The successful establishment of the IPv6 ISF can be viewed as the trigger for the AR to
15   send the router advertisement. The MS may also simultaneously send a router solicitation. The AR can be
16   configured to send zero or more router advertisements on establishment of the IPv6 ISF.

17   An MS receives an RA from the AR on completion of the establishment of the IPv6 ISF. An MS may also send
18   router solicitations on completion of the establishment of the ISF. If the MS does not receive an unsolicited RA from
19   the AR or in response to a router solicitation, the MS will initiate network exit and re-entry procedures.

20   An MS can have multiple IPv6 service flows with different QoS characteristics. However the IPv6 ISF can be
21   considered as the primary service flow. The concept of the ISF is described in [refer to section TBD]. The ASN
22   GW/AR treats each ISF, along with the other service flows to the same MS, as a unique link and manages it as a
23   separate (virtual) interface per link.

24   The IPv6 prefix assigned to an MS may be used as the classifier at the AR for the downlink associated with the MS.
25   Finer grain classifiers which may include the complete IPv6 address and/or port numbers can be established as well.

4.11.4 Address Configuration

27   The addressing scheme for IPv6 hosts in WiMAX follows the IETF recommendation for hosts specified in [49]. The
28   IPv6 node requirements RFC specifies a set of RFCs that are applicable for addressing. These include:

29   • IPv6 Addressing Architecture – [52] (Updated by [53])

30   • IPv6 stateless address autoconfiguration - [34]

31   • Privacy Extensions for Address Configuration in IPv6 - [54]

32   • Default Address Selection for IPv6 - RFC 3484

33   • Stateful Address Autoconfiguration - DHCPv6, [50]

34   The node requirements [49] specifies which of the above addressing related RFCs are mandatory to implement and
35   which are optional

4.11.4.1 Interface Identifier (IID)

37   The MS has a 48-bit MAC address as specified in [Ref1]. This MAC address is used to generate the 64 bit interface
38   identifier which is used by the MS for address autoconfiguration. The IID is generated by the MS as specified in
39   RFC2464.

40   IPv6 address is formed by adding an Interface Identifier (IID) to the prefix learnt from Router Advertisement. The
41   IID forms the least significant bits of the IPv6 address as shown below

42

IPv6 Prefix (64 bits)	Interface Identifier (64 bits)

43   **Figure 4-87 – IPv6 Address Format**

1   The length of the IID is fixed and SHALL be 64-bits for all nodes in the WIMAX Network.

2   The IID for 802.16 interfaces is based on the EUI-64 identifier derived from the interface's built-in 48-bit MAC
3   address. EUI-64 bit identifier is formed by inserting 0xFFFE in the MAC address between the company ID (first 24
4   bits) and the manufacturer selected extension ID (last 24 bits). The IID is then formed from the EUI-64 by inverting
5   the universal/local (u/l) bit. This is the 7th bit of the most significant octet. Inverting this bit will generally change a
6   0 value to a 1 meaning globally unique IPv6 IID.

7
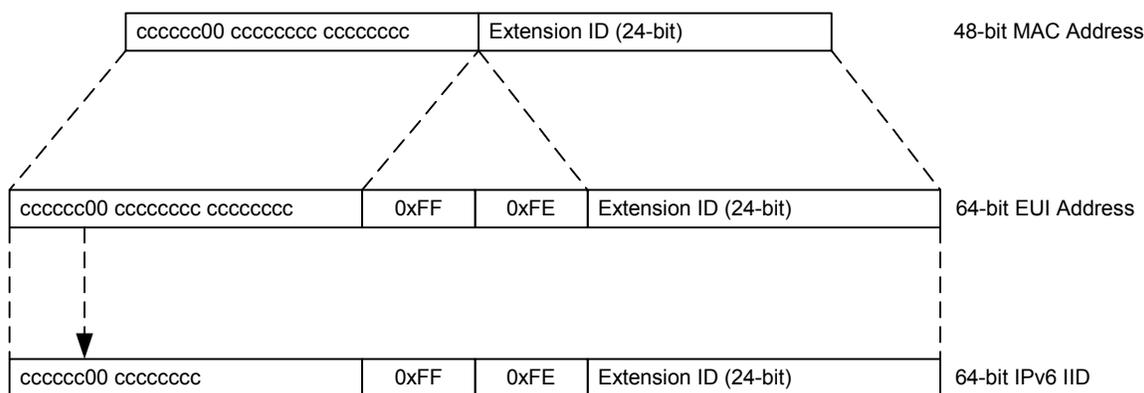
8   **Figure 4-88 – Illustration of Forming the IID**

9   For addresses that are based on privacy extensions, the MS may generate random IIDs as specified in RFC3041.

10   **4.11.4.2 Duplicate Address Detection (DAD)**

11   DAD is performed as per RFC 2461, [34].

12   **4.11.4.3 Stateless Address Auto-configuration**

13   Stateless address auto-configuration is performed as per RFC 2461, [34]. The access router in the ASN is the default
14   router that advertises a prefix that is used by the MS to configure an address

15   **4.11.4.4 Stateful Address Auto-configuration**

16   If the M-flag is set in the RA message from the access router to the MS, the MS MAY perform stateful address
17   autoconfiguration. For this purpose, the MS SHALL use DHCPv6 procedures as defined in [50]. The MS SHALL
18   send the DHCP request message to the all-nodes DHCP server or all-nodes DHCP relay addresses. The ASN-
19   GW/AR acts as the DHCP-server (proxy) or DHCP-relay to assist the MS to acquire an IPv6 address in a stateful
20   manner. If acting as a DHCP relay, the ASN-GW SHALL follow the relay procedures defined in [50].

21   **4.11.5 DNS Discovery**
22   In order to be able to use the Domain Name Service (DNS), the MS has to be configured with the IPv6 DNS server
23   addresses. The IPv6 specified standard mechanism for dynamically configuring the DNS server addresses is via
24   Dynamic Host Configuration Protocol (DHCP) for IPv6 using DNS Configuration options [Reference to RFC
25   3646].

26   Choosing the right DNS Server configuration method is dependent on the address allocation mechanisms. If stateful
27   address auto-configuration is used; then DHCPv6 DNS Configuration options SHALL be used. However, when
28   using stateless address auto-configuration, well-known addresses, or stateless DHCPv6 [RFC3736] SHALL be used.

29   **4.11.5.1 DHCPv6 DNS Configuration Options**

30   The DHCPv6 DNS configuration options are defined in [RFC3646]. The DNS recursive name server options
31   SHALL be populated by the network's name server addresses. In addition, the Domain search list option MAY be
32   present and populated with the network's search list.

1 The MS MAY use DHCPv6 DNS Configuration Options [RFC3646] – either with DHCPv6 [50] when stateful
2 address configuration is used, or Stateless DHCPv6[RFC3736] when stateless address auto-configuration is used.

3 The network SHALL support DHCPv6 [50] and DHCPv6 DNS Configuration Options [RFC3646] when stateful
4 address auto-configuration, is used. The network SHALL support stateless DHCPv6 [50] with the DNS
5 Configuration options [RFC3646] when stateless address auto-configuration is used

6 4.11.6 Uplink and Downlink Transmission of IPv6 Packets

7 4.11.6.1 Uplink

8 IPv6 packets can be sent by the MS over the IP specific part of the Packet CS with IPv6 classifiers, via a transport
9 connection that maps to either the IPv6 Initial service flow or to another IPv6 pre-provisioned service flow in the
10 ASN. The MS sends IPv6 packets that are carried over a transport connection identified by a connection Identifier
11 (CID). The IP specific part of the packet CS at the BS receives the IPv6 packet. Based on the CID that the packet
12 was received on, the BS has a mapping to a service flow which maps to a Data Path ID (GRE key). The BS uses the
13 Data path ID (GRE key) to send the packet to the Access router (AR) via the GRE tunnel (R6) when the BS and
14 Access router are separated (Profiles A and C). In the case of Profile B, the BS forwards the IPv6 packet to the AR.

15 4.11.6.2 Downlink

16 When a packet destined for an MS arrives at the AR, the AR looks at the IPv6 packet header and/or flow ID to
17 determine the service flow ID (SFID) that this packet needs to be mapped on to. The SFID maps to a data path ID.
18 The ASN GW uses the GRE key associated with the data path ID to forward the IPv6 packet via the GRE tunnel to
19 the BS in the case when the AR and the BS are separated by the R6 interface (Profiles A and C). In the case of
20 Profile B, the AR forwards the packet to the BS. When the BS receives the IPv6 packet the BS forwards the IPv6
21 packet on a transport connection identified by a CID to the appropriate MS using the mapping of the SFID to the
22 transport connection. The BS may also utilize the IPv6 classifiers to determine the transport connection to be used
23 for sending the packet.

24 4.11.7 IPv6 AR Relocation (R3 relocation)

25 Relocation of the IPv6 AR causes the MS to be assigned a new prefix and hence a new address. The decision to
26 relocate the AR for an MS is determined by a functional entity in the ASN. AR relocation also causes the MS to
27 update its binding with an HA in the case of Mobile IPv6. The decision to relocate the AR for an MS is always
28 controlled by the network. The types of triggers that can cause AR/R3 relocation are:

29   a.   MS mobility: The MS hands off to a new Base Station under a new Access Router.

30   b.   Wake-up from idle mode: The MS wakes up from the idle mode under a different Access Router than the
31   one under which it entered the idle mode.

32   c.   Resource optimization: The network decides for resource optimization purposes to transfer the R3 endpoint
33   for the MS from the serving Access Router to a new Access Router.

34 AR relocation for an MS requires the MS to perform network re-entry procedure in the scenario the MS wakes up
35 from Idle mode and receives an RA with a prefix that is different from the one it previously had received. In case of
36 R3 relocation as a result of MS mobility and/or resource optimization reasons, network re-entry is not required. The
37 classifier associated with the service flows will however have to be updated with the new prefix. AR relocation can
38 be triggered when the MS is in active mode or in Idle mode.

39 4.12 VoIP Services

40 Details are beyond the scope of Release 1.0.0.

41 4.13 Utility Call Flows

42 The following sections describe specify commonly used R4 call flows and referenced by other sections in this
43 specification.

4.13.1 Data Path Pre-Registration Procedure

The following call flow describes the R4 Data Path Pre-Registration procedure. Data Path Pre-Registration may be initiated by the Target ASN(s), or when the Anchor ASN is co-located with the Serving ASN, by the Serving/Anchor ASN.
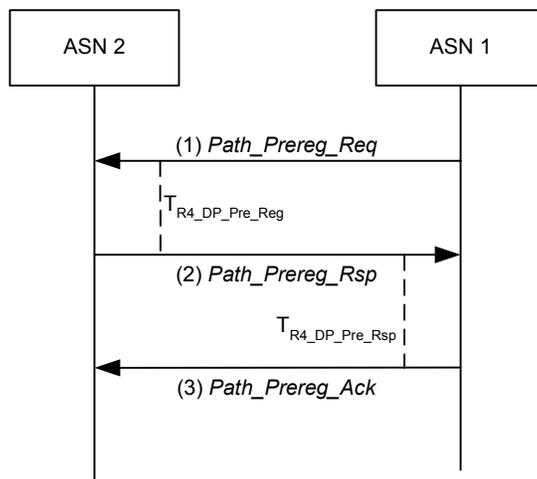
Figure 4-89 – R4 Data Path Pre-Registration Procedure

STEP 1

ASN 1 initiates pre-establishment of the data path for an MS by sending an R4 *Path_Prereg_Req* message to ASN 2 and starts timer $T_{R4\_DP\_Pre\_Reg}$.

STEP 2

ASN 2 sends an R4 *Path_Prereg_Rsp* message to ASN 1 and starts timer $T_{R4\_DP\_Resp.}$ Upon receipt of the R4 *Path_Prereg_Rsp* message, ASN 1 stops timer $T_{R4\_DP\_Pre\_Reg}$.

STEP 3

ASN 1 sends an R4 *Path_Prereg_Ack* message to ASN 2. Upon receipt of the R4 *Path_Prereg_Ack* message, ASN 2 stops timer $T_{R4\_DP\_Rsp.}$

A transaction responder may reject a transaction by sending negative response with Failure Indication TLV.

4.13.2 R4 Context Retrieval Procedure

The following call flow describes the Context Retrieval procedure. A Serving or Target ASN MAY initiate this procedure to request AK context information for a mobile from an Authenticator ASN. A Target ASN MAY also use this procedure to request the most recent MAC context from the Serving ASN.

1
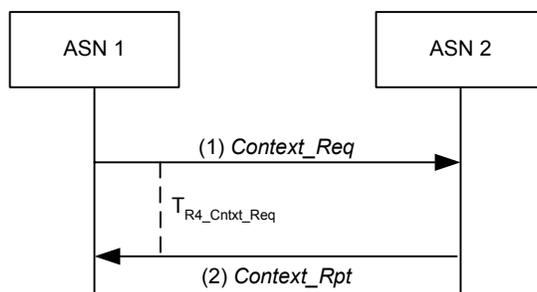
2 **Figure 4-90 – R4 Context Retrieval Procedure**

3 **STEP 1**

4 ASN1 sends an R4 *Context_Req* message to ASN2 to request the stored context associated with a specified MS.
5 ASN 1 starts timer $T_{R4\_Cntxt\_Req.}$

6 **STEP 2**

7 ASN 2 responds by sending the requested context information for the mobile in the R4 *Context_Rpt* message. Upon
8 receipt of the R4 *Context_Rpt* message, ASN1 stops timer $T_{R4\_Cntxt\_Req}$.

9 A transaction responder may reject a transaction by sending negative response with Failure Indication TLV.

10 **4.13.3 R4 Data Path Registration Procedure**

11 The following call flow describes the Data Path Registration procedure. The Data Path Registration procedure takes
12 occurs between a Target and Anchor ASN immediately after the MS has arrived at the Target ASN.

13
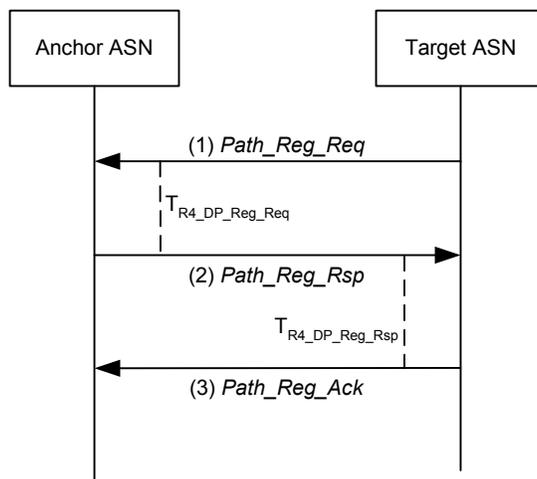
14 **Figure 4-91 – R4 Data Path Registration Procedure**

15 **STEP 1**

16 Target ASN initiates Data Path Registration procedure by sending an R4 *Path_Reg_Req* message to Anchor ASN
17 and starts timer $T_{R4\_DP\_Reg\_Req}$.

18 **STEP 2**

19 Anchor ASN sends an R4 *Path_Reg_Rsp* message to Target ASN. Anchor ASN starts timer $T_{R4\_DP\_Reg\_Rsp}$, if no Data
20 Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction. Upon receipt of
21 the R4 *Path_Reg_Rsp* message, Target ASN stops timer $T_{R4\_DP\_Reg\_Req}$.

1 **STEP 3**

2 If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then
3 Target ASN sends an R4 *Path_Reg_Ack* message to Anchor ASN. Upon receipt of the R4 *Path_Reg_Ack* message,
4 Anchor ASN stops timer $T_{R4\_DP\_Reg\_Rsp}$.

5 A transaction responder may reject a transaction by sending negative response with Failure Indication TLV.

6 ## 4.13.4 R4 Data Path De-Registration Procedure

7 The following call flow describes the Data Path De-Registration procedure.
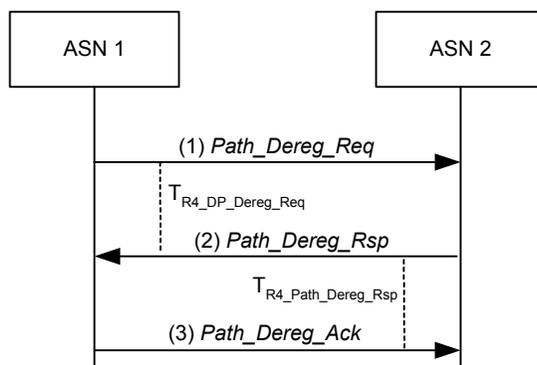
8

9 **Figure 4-92 – R4 Data Path De-Registration Procedure**

10 **STEP 1**

11 ASN 1 initiates Data Path De-Registration procedure by sending an R4 *Path_Dereg_Req* message to ASN 2 and
12 starts timer $T_{R4\_DP\_De-Reg\_Req}$.

13 **STEP 2**

14 ASN2 sends an R4 *Path_Dereg_Rsp* message to ASN1 and starts timer $T_{R4\_Path\_De-Reg\_Rsp}$. Upon receipt of the R4
15 *Path_Dereg_Rsp* message, ASN1 stops timer $T_{R4\_DP\_De-Reg\_Req}$.

16 **STEP 3**

17 ASN1 sends an R4 *Path_Dereg_Ack* message to ASN2. Upon receipt of the R4 *Path_Dereg_Ack* message, ASN2
18 stops timer $T_{R4\_Path\_De-Reg\_Rsp}$.

19 ## 4.13.5 R4 CMAC Key Count Update Procedure

20 The following call flow describes the R4 CMAC Key Count Update procedure.
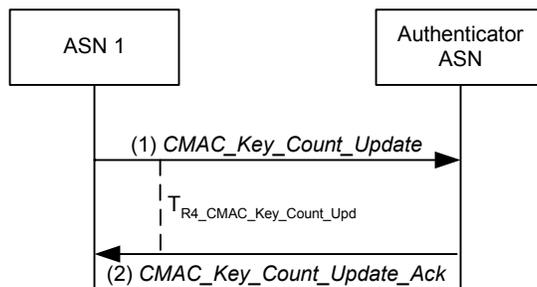
21

22 **Figure 4-93 – R4 CMAC Key Count Update Procedure**

1 **STEP 1**

2 ASN 1 initiates the R4 CMAC Count Update procedure by sending an R4 *CMAC_Key_Count_Update* message to
3 the Authenticator ASN and starts timer $T_{R4\_CMAC\_Key\_Count\_Upd}$.

4 **STEP 2**

5 The Authenticator ASN updates the key count for the MS, then sends an R4 *CMAC_Key_Count_Update_Ack*
6 message to ASN 1. Upon receipt of the R4 *CMAC_Key_Count_Update_Ack* message, ASN 1 stops timer
7 $T_{R4\_CMAC\_Key\_Count\_Upd}$.

8 Please note that when the Authenticator and Anchor ASN are co-located, the CMAC Count Update exchange can be
9 piggybacked to the R4 *Path_Reg_Req* and *Path_Reg_Rsp* exchange. Such Piggybacking can be accomplished only
10 after the mobile enters the network.

4.13.6 R6 CMAC Key Count Update Procedure

12 The following call flow describes the R6 CMAC Key Count Update procedure.
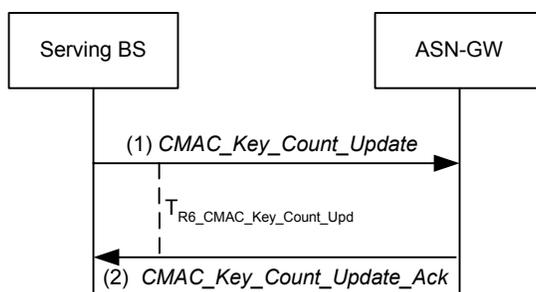
13

14 **Figure 4-94 – R6 CMAC Key Count Update Procedure**

15 **STEP 1**

16 A Serving BS initiates the R6 CMAC Key Count Update procedure by sending an R6 *CMAC_Key_Count_Update*
17 message to the ASN-GW and starts timer $T_{R6\_CMAC\_Key\_Count\_Upd}$.

18 **STEP 2**

19 Upon successfully updating the Authenticator ASN with the new key count, the ASN-GW sends an R6
20 *CMAC_Key_Count_Update_Ack* message to the Serving BS. Upon receipt of the R6
21 *CMAC_Key_Count_Update_Ack* message, the Serving BS stops timer $T_{R6\_CMAC\_Key\_Count\_Upd}$.

4.13.7 R4 CMAC Key Count Request Procedure

23 A Serving ASN MAY initiate this procedure to request the current CMAC Key count from the Authenticator ASN.
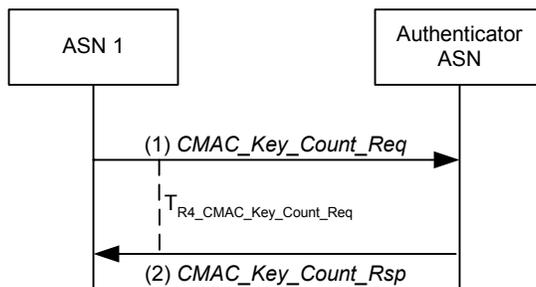
24

25 **Figure 4-95 – R4 CMAC Key Count Request Procedure**

1 **STEP 1**

2 ASN 1 initiates a CMAC Key Count Request procedure by sending an R4 *CMAC_Key_Count_Req* message to the
3 Authenticator ASN and starts timer $T_{R4\_CMAC\_Key\_Count\_Req}$.

4 **STEP 2**

5 The Authenticator responds by sending an R4 *CMAC_Key_Count_Rsp* message to ASN 1 and ASN 1 stops timer
6 $T_{R4\_CMAC\_Key\_Count\_Rsp}$.

1 5. Message and Parameter Definitions

2 5.1 Constants and Counters

3 5.1.1 CMAC_Key_Count Counter

4 5.1.2 CMAC Packet Number Counter

5 5.1.3 CMAC_PN_* Counter

6 5.1.4 Entry Counter

7 5.1.5 HO_Req Retransmission Limit

8 5.1.6 R6 HO_Req Retry Counter

9 5.2 Message Definitions

10   **Table 5-1 – Function and Message Types Index**

Function Type	Message Type	Message
1 (QoS)	1	*RR_Ack*
	2	*RR_Req*
	3	*RR_Rsp*
2 (HO Control	1	*HO_Ack*
	2	*HO_Complete*
	3	*HO_Cnf*
	4	*HO_Req*
	5	*HO_Rsp*
3 (Data Path Control)	1	*Path_Dereg_Ack*
	2	*Path_Dereg_Req*
	3	*Path_Dereg_Rsp*
	4	*Path_Modification_Ack*
	5	*Path_Modification_Req*
	6	*Path_Modification_Rsp*
	7	*Path_Prereg_Ack*
	8	*Path_Prereg_Req*
	9	*Path_Prereg_Rsp*
	10	*Path_Reg_Ack*

Function Type	Message Type	Message
	11	*Path_Reg_Req*
	12	*Path_Reg_Rsp*
	13	*MS_Attachment_Req*
	14	*MS_Attachment_Rsp*
	15	*MS_Attachment_Ack*
	16	*Key_Change_Directive*
4 (Context Transfer)	1	*Context_Rpt*
	2	*Context_Req*
	3	*Context_Ack*
	4	*CMAC_Key_Count_Update*
	5	*CMAC_Key_Count_Update_Ack*
5 (R3 Mobility)	1	*Anchor_DPF_HO_Req*
	2	*Anchor_DPF_HO_Trigger*
	3	*Anchor_DPF_HO_Rsp*
	4	*Anchor_DPF_Relocate_Req*
	5	*FA_Register_Req*
	6	*FA_Register_Rsp*
	7	*Anchor_DPF_Relocate_Rsp*
	8	*FA_Revoke_Req*
	9	*FA_Revoke_Rsp*
6 (Paging)	1	*Initiate_Paging_Req*
	2	*Initiate_Paging_Rsp*
	3	*LU_Cnf*
	4	*LU_Req*
	5	*LU_Rsp*
	6	*Paging_Announce*
	7	*CMAC_Key_Count_Req*
	8	*CMAC_Key_Count_Rsp*
7 (RRM)	1	R6 *PHY_Parameters_Req*
	2	R6 *PHY_Parameters_Rpt*
	3	R4/R6 *Spare_Capacity_Req*
	4	R4/R6 *Spare_Capacity_Rpt*
	5	R6 *Neighbor_BS_Resource_Status_Update*
	6	R4/R6 *Radio_Config_Update_Req*

Function Type	Message Type	Message
	7	R4/R6 *Radio_Config_Update_Rpt*
8 (Authentication Relay)	1	*AR_Authenticated_EAP_Start*
	2	*AR_Authenticated_EAP_Transfer*
	3	*AR_EAP_Start*
	4	*AR_EAP_Transfer*
	5	*AR_EAP_Complete*
9 (MS State)	1	*IM_Entry_State_Change_Req*
	2	*IM_Entry_State_Change_Rsp*
	3	*IM_Exit_State_Change_Req*
	4	*IM_Exit_State_Change_Rsp*
	5	*NW_ReEntry_State_Change_Directive*
	6	*MS_PreAttachment_Req*
	7	*MS_PreAttachment_Rsp*
	8	*MS_PreAttachment_Ack*
10 (Re-Authentication)		
	2	*Key_Change_Directive*
	3	*Key_Change_Cnf*
	4	*Relocation_Cnf*
	5	*Relocation_Confirm_Ack*
	6	*Relocation_Notify*
	7	*Relocation_Notify_Ack*
	8	*Relocation_Req*
	9	*Relocation_Rsp*

1 **5.2.1   Quality of Service**

2 **5.2.1.1   RR_Ack**

Function Type	Message Type	Top Level TLVs	
1	1	**TLV Name**	**M/O**
		MS Info	M
		BS Info	O

1 **5.2.1.2   RR_Req**

Function Type	Message Type	Top Level TLVs	
1	2	**TLV Name**	**M/O**
		MS Info	M
		BS Info	O

2 **5.2.1.3   RR_Rsp**

Function Type	Message Type	Top Level TLVs	
1	3	**TLV Name**	**M/O**
		MS Info	M
		BS Info	O

3 **5.2.2   HO Control**

4 **5.2.2.1   HO_Ack**

Function Type	Message Type	Top Level TLVs	
2	1	**TLV Name**	**M/O**
		BS Info (Target, one or more)	M
		MS Info	O

5 **5.2.2.2   HO_Complete**

Function Type	Message Type	Top Level TLVs	
2	2	**TLV Name**	**M/O**
		Result Code	M
		MS Info	M
		BS Info (for each Target BS)	M

6 **5.2.2.3   HO_Cnf**

Function Type	Message Type	Top Level TLVs	
2	3	**TLV Name**	**M/O**
		MS Info	M
		HO Type	M

Function Type	Message Type	Top Level TLVs	
		HO Confirm Type	M
		BS Info (for each Serving or Target BS)	M

1 **5.2.2.4 HO_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
2	4	HO Type	M
		MS Info	M
		BS Info (for Serving and each Target BS)	M

2 **5.2.2.5 HO_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
2	5	HO Type	M
		Result Code	M
		MS Info	M
		BS Info (for Serving or each Target BS)	M

3 **5.2.3 Data Path Control**

4 **5.2.3.1 Path_Dereg_Ack**

5

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	1	Registration Type	M
		MS Info	O[14]

1 **5.2.3.2   Path_Dereg_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	2	Registration Type	M
		MS Info	O[15]
		BS Info	O

2 **5.2.3.3   Path_Dereg_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	3	Registration Type	M
		MS Info	O[16]
		BS Info	O

3 **5.2.3.4   Path_Modification_Ack**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	4	MS Info	O[17]
		BS Info	O

---

[14] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[15] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[16] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[17] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

1   **5.2.3.5   Path_Modification_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	5	Registration Type	M
		MS Info	O[18]
		BS Info	O

2   **5.2.3.6   Path_Modification_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	6	Registration Type	M
		MS Info	O[19]
		BS Info	O

3   **5.2.3.7   Path_Prereg_Ack**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	7	Registration Type	M
		MS Info	O[20]

4   **5.2.3.8   Path_Prereg_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	8	Registration Type	M
		BS Info	M
		MS Info	M

---

[18] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[19] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[20] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

1 **5.2.3.9   Path_Prereg_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	9	Registration Type	M
		MS Info	O[21]
		BS Info	O

2 **5.2.3.10 Path_Reg_Ack**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	10	HO Type	M
		MS Info	O[22]

3 **5.2.3.11 Path_Reg_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	11	Registration Type	M
		BS Info (Target)	O[23]
		Paging Information	O
		MS Info	M

4 **5.2.3.12 Path_Reg_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	12	Registration Type	M
		BS Info	O[24]
		Paging Information	O
		MS Info	O[25]

---

[21] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[22] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[23] BS Info TLV is Mandatory when message is used in the context of Mobility. See section 4.7.

[24] BS Info TLV is Mandatory when message is used in the context of Mobility. See section 4.7.

1   **5.2.3.13 MS_Attachment_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	13	MS Info	M
		BS Info	O

2   **5.2.3.14 MS_Attachment_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	14	MS Info	O

3   **5.2.3.15 MS_Attachment_Ack**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
3	15		

4   **5.2.4   Context Transfer**

5   **5.2.4.1   Context_Rpt**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
4	1	MS Info	M
		Context Purpose Indicator	M
		MS Info->AK Context (this TLV is only present when message is used for BS require AK Context from Anchor Authenticator) Note: AK Context include the CMAC_KEY_COUNT information for UL and DL.	O
		BS Info (Serving)	O[26]
		BS Info (Target)	O[27]

---

[25] MS Info TLV is only present when message is used in the context of QoS-handling. See section 4.6.

[26] BS Info(Serving) TLV is Mandatory when message is used in the context transfer between Serving to Target ASN. See section 4.7.2

[27] BS Info(Target) TLV is Mandatory when message is used in the context transfer between Serving ASN to Target ASN or Authenticator ASN and Target ASN. See section 4.7.2

Function Type	Message Type	Top Level TLVs	
		Failure Indication	O

5.2.4.2 Context_Req

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
4	2	Context Purpose Indicator	M
		BS Info (Serving)	O[28]
		BS Info (Target)	O[29]
		Authenticator ID	O[30]
		Paging Information	O
		DHCP Relay Info	O

5.2.4.3 Context_Ack

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
4	3	Context Purpose Indicator	M

5.2.4.4 CMAC_Key_Count_Update

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
4	5	MS Info	M
		BS Info	M

---

[28] BS Info(Serving) TLV is Mandatory when message is used in the context of Mobility between Serving to Target ASN. See section 4.7.2

[29] BS Info(Target) TLV is Mandatory when message is used in the context transfer between Serving ASN to Target ASN or Authenticator ASN and Target ASN. See section 4.7.2.

[30] Authenticator ID is Mandatory when message is used between target ASN to Authenticator ASN. See section 4.7.2

1 *5.2.4.5 CMAC_Key_Count_Update_Ack*

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
4	5	MS Info	M
		BS Info	M

2 **5.2.5 R3 Mobility**

3 **5.2.5.1 Anchor_DPF_HO_Req**

IE	Reference	M/O	Notes
Anchor MM context	5.3.2.11	M	DHCP Proxy Info, DHCP Server Info, MIPv4 Info etc

4 **5.2.5.2 Anchor_DPF_HO_Trigger**

IE	Reference	M/O	Notes

5 **5.2.5.3 Anchor_DPF_HO_Rsp**

IE	Reference	M/O	Notes
R3 Operation Status	Section 5.3.2.167	M	Success or failure indication

6 **5.2.5.4 Anchor_DPF_Relocate_Req**

IE	Reference	M/O	Notes
Care-Of Address	Section 5.3.2.28	M	
Anchor MM Context	Section 5.3.2.11	M	

7 **5.2.5.5 FA_Register_Req**

IE	Reference	M/O	Notes
RRQ	Defined in MIP RFC.	M	
FA-HA Key	Section 5.3.2.66	O	FA-HA if used

8 **5.2.5.6 FA_Register_Rsp**

IE	Reference	M/O	Notes
RRP	Defined IN MIP RFC	M	

9 **5.2.5.7 Anchor_DPF_Relocate_Rsp**

IE	Reference	M/O	Notes
R3 Operation Status	Section 5.3.2.167	M	Success or Failure indication.

1 ### 5.2.5.8 FA_Revoke_Req

IE	Reference	M/O	Notes
FA Revoke Reason	To be defined in a future release.	M	DHCP release, expiry, FA initiated release, HA initiated release

2 ### 5.2.5.9 FA_Revoke_Rsp

IE	Reference	M/O	Notes

3 ## 5.2.6 Paging Control

4 ### 5.2.6.1 Initiate_Paging_Req

Function Type	Message Type	Top Level TLVs	
6	1	**TLV Name**	**M/O**

5 ### 5.2.6.2 Initiate_Paging_Rsp

Function Type	Message Type	Top Level TLVs	
6	2	**TLV Name**	**M/O**

6 ### 5.2.6.3 LU_Cnf

Function Type	Message Type	Top Level TLVs	
6	3	**TLV Name**	**M/O**
		BS Info	O

7 ### 5.2.6.4 LU_Req

Function Type	Message Type	Top Level TLVs	
6	4	**TLV Name**	**M/O**
		BS Info	O
		Paging Information	O

1   **5.2.6.5   LU_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
6	5	BS Info	O
		Paging Information	O

2   **5.2.6.6   Paging_Announce**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
6	6	Paging Information	O

3   **5.2.6.7   CMAC_Key_Count_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
6	7		

4   **5.2.6.8   CMAC_Key_Count_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
6	6		

5   **5.2.7   RRM**

6   **5.2.7.1   R6 PHY_Parameters_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	1	Note: This message has no procedure-specific TLVs	M

1   **5.2.7.2   R6 PHY_Parameters_Rpt**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	2	MSID (Note: Obsolete if included in message header.)	O
		RRM BS-MS PHY Quality Info	M
		BS Info (Target, one or more)	O

2   **5.2.7.3   R4/R6 Spare_Capacity_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	3	RRM Spare Capacity Report Type	M
		BS ID	M
		RRM Reporting Characteristics	O
		RRM Averaging Time T	O
		RRM Reporting Period P	O
		RRM Absolute Threshold Value J	O
		RRM Relative Threshold RT	O

3   **5.2.7.4   R4/R6 Spare_Capacity_Rpt**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	4	RRM Spare Capacity Report Type	M
		RRM Reporting Characteristics	O
		RRM BS Info	M
		Failure Indication	O

4   **5.2.7.5   R6 Neighbor_BS_Resource_Status_Update**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	5	RRM BS Info (one or more)	M

1 **5.2.7.6   R4/R6 Radio_Config_Update_Req**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	6	BS ID (one or more)	M
		RRM Reporting characteristics	O
		RRM Reporting Period P	O

2 **5.2.7.7   R4/R6 Radio_Config_Update_Rpt**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
7	7	RRM Reporting Characteristics	O
		RRM BS Info	M

3 **5.2.8   Authentication Relay**

4 **5.2.8.1   AR_Authenticated_EAP_Start**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
8	1	MS Info	M
		BS Info	O

5 **5.2.8.2   AR_Authenticated_EAP_Transfer**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
8	2	EAP Payload	M

6 **5.2.8.3   AR_EAP_Start**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
8	3	MS Info	O
		BS Info	O

1 **5.2.8.4 AR_EAP_Transfer**

Function Type	Message Type	Top Level TLVs	
8	4	**TLV Name**	**M/O**
		EAP Payload	M
		BS Info	O

2 **5.2.8.5 AR_EAP_Complete**

Function Type	Message Type	Top Level TLVs	
8	5	**TLV Name**	**M/O**
		EAP Payload	M

3 **5.2.9 MS State Change**

4 **5.2.9.1 IM_Entry_State_Change_Req**

Function Type	Message Type	Top Level TLVs	
9	1	**TLV Name**	**M/O**
		BS Info	O

5 **5.2.9.2 IM_Entry_State_Change_Rsp**

Function Type	Message Type	Top Level TLVs	
9	2	**TLV Name**	**M/O**
		BS Info	O

6 **5.2.9.3 IM_Exit_State_Change_Req**

Function Type	Message Type	Top Level TLVs	
9	3	**TLV Name**	**M/O**
		BS Info	O

1 **5.2.9.4   IM_Exit_State_Change_Rsp**

Function Type	Message Type	Top Level TLVs	
9	4	**TLV Name**	**M/O**
		BS Info	O

2 **5.2.9.5   NW_ReEntry_State_Change_Directive**

Function Type	Message Type	Top Level TLVs	
9	5	**TLV Name**	**M/O**

3 **5.2.9.6   MS_PreAttachment_Req**

Function Type	Message Type	Top Level TLVs	
9	6	**TLV Name**	**M/O**
		BS Info	O

4 **5.2.9.7   MS_PreAttachment_Rsp**

Function Type	Message Type	Top Level TLVs	
9	7	**TLV Name**	**M/O**
		BS Info	O

5 **5.2.9.8   MS_PreAttachment_Ack**

Function Type	Message Type	Top Level TLVs	
9	8	**TLV Name**	**M/O**
		BS Info	O

1 **5.2.10 Authenticator Relocation**

2 **5.2.10.1 Relocation_Cnf**

Function Type	Message Type	Top Level TLVs	
10	4	**TLV Name**	**M/O**
		MS Info	M

3 **5.2.10.2 Relocation_Cnf_Ack**

Function Type	Message Type	Top Level TLVs	
10	5	**TLV Name**	**M/O**
		MS Info	M

4 **5.2.10.3 Relocation_Notify**

Function Type	Message Type	Top Level TLVs	
10	6	**TLV Name**	**M/O**
		MS Info	M

5 **5.2.10.4 Relocation_Notify_Ack**

Function Type	Message Type	Top Level TLVs	
10	7	**TLV Name**	**M/O**
		MS Info	M
		Accept/Reject Indication	M

6 **5.2.10.5 Relocation_Req**

Function Type	Message Type	Top Level TLVs	
10	8	**TLV Name**	**M/O**
		MS Info	M

1 **5.2.10.6 Relocation_Rsp**

Function Type	Message Type	Top Level TLVs	
		TLV Name	**M/O**
10	9	MS Info	M
		Accept/Reject Indication	M

2 **5.2.11 Network Exit and Entry**

3 This section describes the R4 and R6 message definitions for network entry and exit.

4 **5.2.11.1 Delete_MS_Entry_Req**

IE	Reference	M/O	Notes
VOID			

5 **5.2.11.2 R6 Session_Release_Req**

IE	Reference	M/O	Notes
MSID	5.3.2.102	O	MS MAC address.
R3 Release Reason	5.3.2.168	O	Release reason.

6 **5.2.11.3 R6 Session_Release_Rsp**

IE	Reference	M/O	Notes
MSID	5.3.2.102	O	MS MAC address.
Release Status	5.x.x	O	Status

7 **5.3 TLV Definitions**

8 **5.3.1 TLV Format**

9 The format of TLV appears below:

0 0							0 7							1 5							2 3							3 1
Type																Length														
Value (actual number of octets in the Value Field is specified in the value of the Length Field)																														

10 The type field defines the type of data element. It is 2 bytes long. The Length field defines the length of the value
11 portion in octets (thus a TLV with no value portion would have a length of zero). The TLV is padded to four-octet
12 alignment. Padding is not included in the length field (so a three octet value would have a length of three, but the
13 total size of the TLV would be eight octets). The Type equal to 65535 is reserved for vendor-specific extensions.
14 All other undefined type codes are reserved for future assignment. The value field itself could contain other TLVs,
15 and such TLVs are termed nested TLVs.

16 **5.3.2 TLV Encoding**

17 All enumeration values start from 0 unless specified otherwise.

1 **5.3.2.1 Accept/Reject Indicator**

Type	1
Length in octets	1
Value	• 0x00 = accept • 0x01 = reject
Description	Indicates Accept/Reject of the corresponding request.
Parent TLV(s)	Top

2 **5.3.2.2 Accounting Extension**

Type	2
Length in octets	Variable
Value	String
Description	This parameter indicates information relevant for accounting. The operation and the application content provider determine the format and value of the Accounting Extension.
Parent TLV	SF Info

3 **5.3.2.3 Action Code**

Type	3
Length in octets	2
Value	Enumerator. The values are: • 0x0000 = Deregister MS. MS SHALL immediately terminate service with the BS and should attempt network entry at another BS; • 0x0001 = Suspend all MS traffic including control traffic. MS SHALL listen to the current BS but SHALL not transmit until an RES-CMD message or DREG-CMD with Action Code 02 or 03 is received; • 0x0002 = Suspend user traffic (transport connections). MS SHALL listen to the current BS but only transmit on the Basic and Primary Management Connections; • 0x0003 = Resume traffic. MS SHALL return to normal operation and may transmit on any of its active connections. • 0x0004 = MS SHALL terminate current Normal Operations with the BS; the BS SHALL transmit this action code only in response to any SS DREG-REQ message; • 0x0005 - FFFF = Reserved.
Description	Indicates the action code to be used by BS in the DREG-CMD. Action Code TLV is used only in the messages directed to a BS.
Message Primitives That Use This TLV	Path Control messages (*Path_Dereg_Req*), MS State Change messages.

4 **5.3.2.4 Action Time**

Type	4
Length in octets	4

Value	32-bit unsigned integer
Description	Absolute time reference in airframe durations (e.g. 5 ms).
Parent TLV(s)	BS Info

1 **5.3.2.5 AK**

Type	5
Length in octets	20
Value	160-bit AK Value
Description	AK is derived from the PMK at the NAS.
Parent TLV(s)	AK Context

2 **5.3.2.6 AK Context**

Type	6	
Length in octets	Variable but not less than 10	
Value	Compound	
Description	Contains AK Context from Authenticator	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	AK	M
	AK ID	M
	AK Lifetime	M
	AK SN	M
	CMAC_KEY_COUNT	M
	EIK	O (see notes)
Parent TLV(s)	MS Info	

3 **Notes:**

4 1) EIK SHALL be included in the AK Context if Double EAP is employed and SHALL be omitted otherwise.

5 2) CMAC_KEY_COUNT SHALL be included only in *NW_ReEntry_State_Change_Directive* in order to notify
6 the Authenticator about the successful completion of HO Network Re-Entry. In other cases it SHALL be
7 omitted

8 **5.3.2.7 AK ID**

Type	7
Length in octets	8
Value	64-bit AK ID Value
Description	Identifies the AK that used for protecting the message
Parent TLV(s)	AK Context

1   **5.3.2.8   AK Lifetime**

Type	8
Length in octets	2
Value	16-bit AK Lifetime Value
Description	The time period during which the AK will be valid.
Parent TLV(s)	AK Context

2   **5.3.2.9   AK SN**

Type	9
Length in octets	1
Value	0X0000	4-bit AK SN
Description	The Sequence number of root keys (PMK/PMK2) for the AK.
Parent TLV(s)	AK Context

3   **5.3.2.10   Anchor ASN GW ID / Anchor DPF Identifier**

Type	10
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique identifier for the Anchor GW / Anchor Data Path Function.
Parent TLV(s)	MS Info

4   **5.3.2.11   Anchor MM Context**

Type	11	
Length in octets	Variable	
Value	Compound	
Description	Information related with FA relocation, which means all context maintained by some entities binding with FA relocation	
Elements (Sub-TLVs)	TLV Name	M/O
	MS Mobility Mode	M
	MIP4 Info	O
	DHCP Server List	O
	DHCP Proxy Info	O
	Idle Mode Info	O
Message Primitives That Use This TLV	Anchor DPF HO Request, Anchor DPF Relocate Request, R4 HO Request	

1   **5.3.2.12 Anchor PCID - Anchor Paging Controller ID**

Type	12
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	Unique identifier for the Paging Controller network entity, which administers paging activity for the MS while in Idle Mode and retains MS service and operational information. The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	
Parent TLV(s)	Paging Information

2   **5.3.2.13 Anchor PC Relocation Destination**

3   Exists if relocation is requested.

Type	13
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	
Description	Network identifier for the Paging Controller network entity, which administers paging activity for the MS while in Idle Mode and retains MS service and operational information. The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Parent TLV(s)	Paging Information

4   **5.3.2.14 Anchor PC Relocation Request Response**

5   Exists if relocation is requested.

Type	14
Length in octets	1
Value	
Description	Boolean field. 0xFF for accept, 0x00 for refuse.
Parent TLV(s)	Paging Information

6   **5.3.2.15 Associated PHSI**

Type	15
Length in octets	1
Value	8-bit unsigned integer
Description	The Associated PHSI value. It SHALL be equal to the PHSI value of the corresponding PHS Rule.
Parent TLV	Packet Classification Rule

1 **5.3.2.16 FA Revoke Reason**

Type	16
Length in octets	1
Value	• 0= DHCP Release • 1 = DHCP expiry • 2 = FA initiated release • 3 = HA initiated release • 4 – 255 = Reserved
Description	Indicates the FA Revoke Reason.
Parent TLV(s)	FA Revoke Req

2 **5.3.2.17 Authentication Complete**

Type	17	
Length in octets		
Value		
Description		
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Authentication Result	M
	PKM2 Message Code	M
Parent TLV		

3 **5.3.2.18 Authentication Result**

Type	18
Length in octets	1
Value	The value of this parameter indicates to BS the results of EAP authentication process: • 0 = Success • 1 = Failure Other values are reserved.
Description	Indication of EAP success
Parent TLV(s)	Authentication Complete

4 **5.3.2.19 Authenticator ID**

Type	19
Length in octets	Variable (could be of three fixed sizes: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique identifier of MS's Anchor Authenticator.
Parent TLV(s)	MS Info

1   **5.3.2.20 RRQ**

Type	20
Length in octets	variable
Value	Same as defined in [15] including IP/UDP headers
Description	MIP Register Request message defined in [15]
Parent TLV(s)	FA_Register_Req

2   Note [a]: Used only during HO/ Idle Mode entry/exit operations.

3   **5.3.2.21 Authorization Policy**

Type	21
Length in octets	2
Value	8-bit bitmask representing HO Authorization Policy. • Bit #0 = RSA authorization • Bit #1 = EAP authorization • Bit #2 = Authenticated-EAP authorization • Bit #3 = HMAC supported • Bit #4 = CMAC supported • Bit #5 = 64-bit Short-HMAC • Bit #6 = 80-bit Short-HMAC • Bit #7 = 96-bit Short-HMAC • Bits #8-15 Reauthentication Policy (TBD)
Description	This parameter is used to indicate authentication mode (single EAP, double EAP or both). In MS Security History TLV, it indicates the capability negotiated between ASN and MS.
Parent TLV	MS Info

4   **5.3.2.22 Available Radio Resource DL**

Type	22
Length in octets	1
Value	• 8-bit unsigned integer: • 0x00 = 0% • 0x01 = 1%, • ..., • 0x64 = 100% • 0x65 – 0xfe = reserved
Description	Available Radio Resource indicator DL SHALL indicate the average percentage of available physical radio resources for DL where averaging SHALL take place over a time interval specified by Averaging Time TLV of RRM *Spare_Capacity_Req* if provided; if omitted, the BS SHALL apply a default value. Available physical radio resources SHALL be defined as the number of slots available for data transmission in DL subframe, which are not used by any non-best-effort service flow class.

Parent TLV(s)	RRM BS Info

1 ### 5.3.2.23 Available Radio Resource UL

Type	23
Length in octets	1
Value	8-bit unsigned integer: 0x00 = 0% 0x01 = 1%, ..., 0x64 = 100% 0x65 – 0xFE = reserved
Description	Available Radio Resource indicator UL SHALL indicate the average percentage of available physical radio resources for UL where averaging SHALL take place over a time interval specified by Averaging Time TLV of RRM *Spare_Capacity_Req* if provided; if omitted, the BS SHALL apply a default value. Available physical radio resources SHALL be defined as the number of slots available for data transmission in UL subframe, which are not used by any non-best-effort service flow class.
Parent TLV(s)	RRM BS Info

2 ### 5.3.2.24 BE Data Delivery Service

Type	24	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for BE Data Delivery Service. If included in QoS Info, it implies BE Scheduling Service for UL connections	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Maximum Sustained Traffic Rate	O
	Traffic Priority.	O (if omitted means Traffic Priority = 0)
	Request/transmission policy.	O [a]
Parent TLV	QoS Info	

3 Note: [a] – Used only during HO/ Idle Mode entry/ exit operations.

4 ### 5.3.2.25 BS ID

Type	25
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique BS Identifier, referring to a single sector with a single frequency assignment.
Parent TLV(s)	BS Info

1   **5.3.2.26 BS Info**

Type	26	
Length in octets	Variable	
Value		
Description	Description of BS	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BS ID	M
	Serving/Target Indicator	M
	Round Trip Delay	O
	Relative Delay	O
	DL PHY Quality Info	O
	UL PHY Quality Info	O
	Data Path Establishment Option	O
	HO ID (see note)	O
	HO Process Optimization	O
	HO Authorization Policy Support	O
	Spare Capacity Indicator	O
	Service Level Prediction	O
	Preamble Index / Sub-channel Index	O
	SF Info	O
	Action Time	O
	Data Path Encapsulation Type	
Message Primitives That Use This TLV	Every Message	

2   Note: HO ID is defined in the IEEE 802.16e spec.

3   **5.3.2.27 BS-originated EAP-Start Flag**

Type	27
Length in octets	0
Value	
Description	Flag indicating that *AR_EAP_Start* message is originated by a BS (without receiving PKMv2 EAP-Start from an MS). A BS may use *AR_EAP_Start* with this flag to instigate reauthentication process when MS security context in BS is going to expire.
Message Primitives That Use This TLV	MS Info, *AR_EAP_Start*

1   **5.3.2.28 Care-Of Address (CoA)**

Type	28
Length in octets	4 bytes
Value	Care-Of Address (HoA) of the MS
Description	
Parent TLV(s)	MIP4 Info

2   **5.3.2.29 CID**

Type	29
Length in octets	2
Value	16-bit unsigned integer.
Description	CID definition as per 802.16.
Parent TLV(s)	SF Info

3   **5.3.2.30 Classifier**

Type	30	
Length in octets	Variable	
Value	Compound	
Description	This TLV defines one Packet Classifier • Classifier Index identifies the classifier to be specified • Classifier Value shall follow the syntax of IEEE Std 802.16e-2005 section 11.13.19.3.4 Packet Classification rule.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Classifier Type (1-byte)	O
	Classifier Value	O
Parent TLV(s)	SF Info	

4   **5.3.2.31 Classifier Action**

Type	31
Length in octets	1
Value	Classifier Action Code • 0 = Add Classifier • 1 = Replace Classifier • 2 = Delete Classifier
Description	Add, replace or delete the classifier for the classification of a specific service flow
Parent TLV	SF Info

1   **5.3.2.32 Classifier Rule Priority**

Type	32
Length in octets	1
Value	8-bit unsigned integer.
Description	The value of the field specifies the priority for the Classifier, which is used for determining the order of the Classifier. A higher value indicates higher priority. Classifiers may have priorities in the range 0–255 with the default value being 0.
Parent TLV	Packet Classification Rule

2   **5.3.2.33 Classifier Type**

Type	33
Length in octets	1-byte
Value	• 1 = IP TOS/DSCP Range and Mask • 2 = Protocol • 3 = IP Source Address and Mask • 4 =IP Destination Address and Mask • 5 = Protocol Source Port Range • 6 = Protocol Destination Port Range • 7 = IEEE 802.3/Ethernet Destination MAC address • 8 =IEEE 802.3/Ethernet Source MAC address • 9 = Ethertype/IEEE 802.2 SAP • 10 = IEEE 802.1D User_Priority • 11 = IEEE 802.1Q VLAN_ID • 12-255 = TBD
Descriptions	This TLV defines the types for different Classifiers
Parent TLV	Classifier

3   **5.3.2.34 CMAC_KEY_COUNT**

Type	34
Length in octets	2 bytes
Value	Unsigned 16-bit integer
Description	Value of the Entry Counter that is used to guarantee freshness of computed CMAC_KEY_* with every entry and provide replay protection. Upon initial network entry, count is reset to 0 in the MS and Serving BS, and to 1 in the Authenticator.
Parent TLV(s)	AK Context

4   **5.3.2.35 Combined Resources Required**

Type	35
Length in octets	2

Value	• 0x0000 = Not combined; • 0x0001 =Combined; • Other = Reserved
Description	Specifies if the complete reservation request should be rejected if a corresponding flow reservation fails. The Flow Reservation Request should be completely rejected if a request of any service flow with this indicator set to 1 fails, otherwise requests for service flow with this indicator set to 0 only take effects on itself. The absence of this TLV should be interpreted in the same way as if it is present where the value is set to 0.
Parent TLV	SF Info

1 **5.3.2.36 Context Purpose Indicator**

Type	36
Length in octets	4
Value	32-bit Bitmask. • Bit #0 = MS AK Context. • Bit #1 = MS Network Context • Bit #2 = MS MAC Context • Bit #3 = Service Authorization Context • Bit #4 = FA Context • Bit #5 = Accounting context The other bits are reserved and should be reset.
Description	Indicates the type of context to be delivered: • Setting Bit #0 requests delivering AK Context associated with a particular MS. • Setting Bit #1 requests delivery Network Addressable IDs (i.e. BS ID, Anchor GW ID, Authenticator ID, PC ID) associated with a particular MS and known to the responder. • Setting Bit#2 requests delivery of MAC Context associated with a particular MS that is available in BS. • Setting Bit#3 requests delivery of service authorization and policy context (e.g. authorization code) associated with a particular MS. • Setting Bit#4 requests delivery of FA context associated with a particular MS. • Setting Bit#5 requests delivery of Accounting provisioning info
Message Primitives That Use This TLV	Context Delivery messages.

2 **5.3.2.37 Correlation ID**

Type	37
Length in octets	4
Value	32-bit unsigned integer
Description	Indicates correlation between Service Flows. Service Flows with the same Correlation ID are assumed to be related on higher layers and may be treated with common policy. Correlation ID may be associated with SDFID on R3, or allocated locally at the ASN.

Parent TLV(s)	SF Info

1 **5.3.2.38 Cryptographic Suite**

Type	38
Length in octets	4
Value	Cryptographic Suite allowed. • 0x00000 = No data encryption, no data authentication & 3-DES, 128 • 0x010001 = CBC-Mode 56-bit DES, no data authentication & 3-DES, 128 • 0x000002 = No data encryption, no data authentication & RSA, 1024 • 0x010002 = CBC-Mode 56-bit DES, no data authentication & RSA, 1024 • 0x020103 = CCM-Mode 128-bit AES, CCM-Mode, 128-bit, ECB mode AES with 128-bit key • 0x020104 = CCM-Mode 128bits AES, CCM-Mode, AES Key Wrap with 128-bit key • 0x030003 = CBC-Mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key • 0x800003 = MBS CTR Mode 128 bits AES, no data authentication, AES ECB mode with 128-bit key • 0x800004 = MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key All remaining values Reserved
Description	Indicates crytopgraphic suites allowed.
Parent TLV(s)	SA Descriptor

2 **5.3.2.39 CS Type**

Type	39
Length in octets	1
Value	• 1 = Packet, IPv4 • 2 = Packet, IPv6 • 3 = Packet, 802.3 • 4 = Packet, 802.1Q • 5 = Packet, IPv4over802.3 • 6 = Packet, IPv6over802.3
Description	Indicates type of convergence layer between MS and BS.
Parent TLV(s)	CS Negotiation Info, SF Info

3 **5.3.2.40 Data Integrity**

Type	40
Length in octets	1
Value	• 0x0 = No recommendation • 0x1 = Data integrity requested • 0x2 = Data delay jitter sensitive

Description	Specifies, if data integrity is recommended. The value "data integrity requested" advises the base station that mechanism like ARQ/HARQ are requested. The value "data delay jitter sensitive" advises the base station that ARQ/HARQ may have negative effects.
Parent TLV	QoS Info

5.3.2.41 Data Integrity Info

Type	41
Length in octets	
Value	
Description	
Parent TLV	

5.3.2.42 Data Path Encapsulation Type

Type	42
Length in octets	1
Value	• 1 = GRE • 2 = IP-in-IP • 3 = VLAN
Description	Data Path Type
Parent TLV	Data Path Info

5.3.2.43 Data Path Establishment Option

Type	43
Length in octets	1
Value	0 = Do not (Pre-) Establish DP 1 = (Pre-) Establish DP
Description	A flag indicating whether or not Data Path SHOULD be (pre-)established by the entity hosting the Target HO Function (e.g. Target BS, Target ASN)
Parent TLV	BS Info

5.3.2.44 Data Path ID

Type	44
Length in octets	4
Value	Data Path Identifier (e.g. GRE Key)
Description	Identifier for a data path.
Parent TLV	Data Path Info

5.3.2.45 Data Path Info

Type	45

Length in octets	Variable	
Value	Compound	
Description	Data Path Description	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Data Path ID	M
	Data Path Encapsulation Type	O
	Data Path Type	O
	Data Path Integrity Mechanism	O
Parent TLV	SF Info (for per SF Data Path)	

1 **5.3.2.46 Data Path Integrity Mechanism**

Type	46
Length in octets	1
Value	Note: Possible values are out of scope of Release 1.0.0 and will be defined in a future release.
Description	
Parent TLV	Data Path Info

2 **5.3.2.47 Data Path Type**

Type	47
Length in octets	1
Value	Enumerator: {Type1, Type2}
Description	Distinguishes between Type 1 and Type 2 datapaths.
Parent TLV	Data Path Info

3

4 **5.3.2.48 DCD/UCD Configuration Change Count**

Type	48
Length in octets	1
Value	8-bit integer: Bits #0…3 = The 4 LSBs of the BS's current DCD configuration change count; Bits #4…7 = The 4 LSBs of the BS's current UCD configuration change count.
Description	This includes the 4 LSBs of the BS's current DCD and UCD configuration change count figures
Parent TLV(s)	RRM BS Info

5 **5.3.2.49 DCD Setting**

Type	49
Length in octets	Variable

Value	Compound, as specified in [802.16e-2005], section 11.1.7
Description	This is an IEEE802.16e-2005 defined TLV. The DCD_settings is a TLV value that encapsulates a DCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. The DCD settings fields SHALL contain only neighbor's DCD TLV values that are different from the serving BS corresponding values. For values that are not included, the MS SHALL assume they are identical to the corresponding values of the serving BS. The duplicate TLV encoding parameters within a Neighbor BS SHALL not be included in DCD setting. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info
Message Primitives That Use This TLV	*Neighbor_BS_Resource_Status_Update*.

5.3.2.50 Device Authentication Indicator

Type	50
Length in octets	1
Value	Enumerator with the following values: • 0 = Reserved • 1 = Certificate-based device authentication has been successfully performed (MS MAC address is verified). • 2 = Device authentication has been successfully performed. • 14 – 255 = Reserved
Description	This parameter indicates that device authentication has been performed and informs whether it was certificate-based (MS MAC address is verified) or not. Absence of this parameter indicates that no device authentication has been performed.
Parent TLV(s)	MS Security History

5.3.2.51 DHCP Key

Type	51
Length in octets	20 bytes
Value	160-bit unsigned integer
Description	Key used to calculate and authenticate messages between the DHCP relay in the ASN and DHCP server in the CSN, as per [31]. This TLV SHALL be included in the Context-Response message (as part of DHCP Relay Info TLV) if Context Purpose TLV was set to DHCP-Relay-Info
Message Primitives That Use This TLV	DHCP Relay Info

5.3.2.52 DHCP Key ID

Type	52

Length in octets	4 bytes
Value	32-bit unsigned integer
Description	Key ID associated with the key used to compute authentication suboption as per [31]. This TLV SHALL be included in the Context-Response message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
Message Primitives That Use This TLV	DHCP Relay Info

1   **5.3.2.53 DHCP Key Lifetime**

Type	53
Length in octets	4 bytes
Value	32-bit unsigned integer
Description	The remaining lifetime in seconds of the DHCP key. This TLV SHALL be included in the Context-Response message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
Message Primitives That Use This TLV	DHCP Relay Info

2   **5.3.2.54 DHCP Proxy Info**

Type	54	
Length in octets	Variable	
Value	Compound	
Description	Information about the DHCP Proxy	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	IP Remained Time	O
Message Primitives That Use This TLV	Anchor MM Context	

3   **5.3.2.55 DHCP Relay Address**

Type	55
Length in octets	4 bytes
Value	IPv4 address
Description	DHCP relay's IPv4 address facing the DHCP server. This TLV SHALL be included in the *Context_Req* message (as part of DHCP Relay Info TLV) if Context Purpose TLV is set to DHCP-Relay-Info
Message Primitives That Use This TLV	DHCP Relay Info

1   **5.3.2.56 DHCP Relay Info**

Type	56	
Length in octets	Variable	
Value	Compound	
Description	Information about the DHCP Relay. This TLV SHALL be included in the *Context_Req* and *Context_Rpt* messages if Context Purpose TLV is set to DHCP-Relay-Info	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	DHCP Server Address	O
	DHCP Relay Address	O
	DHCP Key	O
	DHCP Key ID	O
	DHCP Key Lifetime	O
Message Primitives That Use This TLV	*Context_Req* and *Context-Rpt.*	

2   **5.3.2.57 DHCP Server Address**

Type	57
Length in octets	4 bytes
Value	IPv4 address
Description	IPv4 address of the DHCP server. This TLV SHALL be included in the Context-Response message (as part of DHCP Relay Info TLV) if Context Purpose TLV was set to DHCP-Relay-Info. This TLV may be included multiple times as part of the DHCP Server List TLV.
Message Primitives That Use This TLV	DHCP Relay Info and DHCP Server List

3   **5.3.2.58 DHCP Server List**

Type	58	
Length in octets	Variable	
Value	Compound	
Description	List of DHCP servers.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	DHCP Server Address	O
Message Primitives That Use This TLV	Anchor MM Context	

1   **5.3.2.59 Direction**

Type	59
Length in octets	2
Value	• 0x0000 = For Uplink • 0x0001 = For Downlink • Other = Reserved
Description	Describes the unidirectional Service Flow direction (i.e. UL or DL).
Parent TLV	SF Info

2   **5.3.2.60 DL PHY Quality Info**

Type	60
Length in octets	4
Value	32-bit integer encoding 8-bit DL RSSI Mean, 8-bit DL RSSI Std, 8-bit DL CINR Mean, 8-bit DL CINR Std.
Description	
Parent TLV	BS Info

3   **5.3.2.61 DL PHY Service Level**

Type	61
Length in octets	4
Value	32-bit integer representing DL PSL
Description	
Parent TLV	BS Info

4   **5.3.2.62 EAP Payload**

Type	62
Length in octets	Variable
Value	EAP Payload (for EAP over R6 Authentication Relay)
Description	EAP Messages
Message Primitives That Use This TLV	EAP Relay messages

5   **5.3.2.63 EIK**

Type	63
Length in octets	20
Value	160-bit EIK Value
Description	EIK key value

Parent TLV(s)	AK Context

1 **5.3.2.64 ERT-VR Data Delivery Service**

Type	64
Length in octets	Variable
Value	Compound
Description	This compound TLV contains the QoS parameters relevant for ERT-VR Data Delivery Service. If included in QoS Info, it implies ertPS Scheduling Service for UL connections

Elements (Sub-TLVs)	**TLV Name**	**M/O Flag**
	Minimum Reserved Traffic Rate	M
	Maximum Latency	M
	Tolerated Jitter	O (omission means jitter equal to maximum latency)
	Unsolicited Grant Interval	M
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
	Request / Transmission Policy	O (see Note [a])
	Maximum Traffic Burst	O
Parent TLV	QoS Info	

2 Note [a]: Used only during HO/ Idle Mode entry/exit operations.

3 **5.3.2.65 Exit IDLE Mode Operation Indication**

4 Proposed to be harmonized as described previously.

Type	65
Length in octets	1
Value	<u>Enumerator</u>: Idle Mode to Active Transition 0 = No 1 = Yes
Description	
Parent TLV(s)	Paging Information

5 **5.3.2.66 FA-HA Key**

Type	66
Length in octets	20 bytes
Value	160-bit unsigned integer

Description	Using FA-HA key to calculate and authenticate FA-HA-AE, integrity can be protected between HA and FA.
Message Primitives That Use This TLV	MIP4 Security Info

1 **5.3.2.67 FA-HA Key Lifetime**

Type	67
Length in octets	4 bytes
Value	32-bit unsigned integer
Description	Time of FA-HA key remaining valid.
Message Primitives That Use This TLV	MIP4 Security Info

2 **5.3.2.68 FA-HA Key SPI**

Type	68
Length in octets	4 bytes
Value	32-bit unsigned integer
Description	Key ID of FA-HA key. It should be equal to the SPI (Key ID) of HA-RK.
Message Primitives That Use This TLV	MIP4 Security Info

3 **5.3.2.69 Failure Indication**

Type	69
Length in octets	1 byte

Value	Most significant bit is reserved as an error extension flag
	• 0 = Unspecified Error
	Error Codes: 1-16 Message Header Failure Codes
	• 1 = Incompatible Version Number
	• 2 = Invalid Function Type
	• 3 = Invalid Message Type
	• 4 = Unknown MSID
	• 5 = Transaction Failure
	• 6 = Unknown Source Identifier
	• 7 = Unknown Destination Identifier
	• 8 = Invalid Message Header
	• 9-15 = Reserved for Future Use
	Error Codes: 16-31 General Message Body Failure Codes
	• 16 = Invalid message format
	• 17 = Mandatory TLV missing
	• 18 = TLV Value Invalid
	• 19 = Unsupported Options
	• 20-31 = Reserved for Future Use
	Error Codes: 32-47 Message Generic Failure Codes
	• 32 = Timer expired without response
	• 33-47 = Reserved for Future Use
	Error Codes: 48-127 Message Specific Failure Codes
	• 48 = Requested Context Unavailable
	• 49 = Authorization Failure
	• 50 = Registration Failure
	• 51 = No Resources
	• 52-127 = Reserved for Future Use
	(To be updated with sub section team specific error handling)
Description	Indicates the reason for failure of a previous request message
	Failure indication should be the First TLV in a response message when it is failure for the request message.
Parent TLV	None

5.3.2.70 FA IP Address

Type	70
Length in octets	4 bytes
Value	IP address of the entity which contain FA function
Description	
Parent TLV(s)	Anchor MM Context

1 **5.3.2.71 FA Relocation Indication**

Type	71
Length in octets	1
Value	• 0 = Success • 1 = Failure
Description	Indicates the FA relocation process. It shall be set to indicate "Success" if FA relocation has been Successfully completed with authenticator relocation. otherwise it should indicate "Failure"
Parent TLV(s)	MS Info

2 **5.3.2.72 Full DCD Setting**

Type	72
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7
Description	This is an IEEE802.16e-2005 defined TLV. The DCD_settings is a TLV value that encapsulates a DCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Radio_Config_Update_Rpt*.

3 **5.3.2.73 Full UCD Setting**

Type	73
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7
Description	This is an IEEE802.16e-2005 defined TLV. The UCD_settings is a TLV value that encapsulates a UCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Radio_Config_Update_Rpt*.

4 **5.3.2.74 Global Service Class Change**

Type	74
Length in octets	6

Value	Global Service Class Name as defined in IEEE802.16e.
Description	Provides an authorized QoS parameters set in a length optimized format.
Parent TLV(s)	SF Info
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Radio_Configuration_Update_Rpt*.

1 **5.3.2.75 HA IP Address**

Type	75
Length in octets	Variable (either 4 or 16)
Value	IP address of HA. The Identifier might be in format of either 4-octet IPv4 Address or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	
Parent TLV(s)	MIP4 Info

2 **5.3.2.76 HO Confirm Type**

Type	76
Length in octets	1
Value	Enumerator: {Confirm, Unconfirm, Cancel, Reject }
Description	Indicates whether one of the candidate BSs is selected as the HO target or not. Here, "Confirm " is for when the network receives an explicit indication of handover target BS from MS, "Unconfirm" for when the network fails to receive an indication from MS but network presumes possible target BSs, "Cancel" for when MS cancels the handover, and "Reject" for when MS rejects handover to one of the candidate BSs proposed by the network.
Parent TLV(s)	HO_Cnf

3 **5.3.2.77 Home Address (HoA)**

Type	77
Length in octets	4 bytes
Value	Home Address (HoA) of the MS
Description	
Parent TLV(s)	MIP4 Info

4 **5.3.2.78 HO Process Optimization**

Type	78
Length in octets	1
Value	8-bit integer representing HO Process Optimization code.
Description	

Parent TLV	BS Info

5.3.2.79 HO Type

Type	79
Length in octets	4
Value	Enumerator. The values are: • 0x00000000 = Hard Handoff (HHO) • 0x00000001 = Fast Base Station Switching (FBSS) • 0x00000002 = Macro Diversity Handoff (MDHO)
Description	Allows communication of various handover types.
Message Primitives That Use This TLV	HO Control messages

5.3.2.80 IDLE Mode Info

Type	80
Length in octets	Variable
Value	Compound
Description	Indicates if the MS is in Idle state

Elements (Sub-TLVs)	TLV Name	M/O
	Anchor PC ID	O

Message Primitives That Use This TLV	Anchor MM Context

5.3.2.81 IDLE Mode Retain Info

Type	81
Length in octets	1
Value	
Description	Indicates which re-entry management messages SHALL be retained and managed. Encoded as in 802.16e.
Parent TLV(s)	Paging Information

5.3.2.82 IP Destination Address and Mask

Type	82
Length in octets	Nx8 (IPv4) or Nx32 (IPv6)
Value	List of the IP Destination Address/Mask pairs: {(Dst1, Dmask1),..., (DstN, DmaskN) }.

Description	List of IP destination addresses and their corresponding address masks An IP packet with IP destination address "ip-dst" matches this parameter if DstX = (ip-dst AND DmaskX) for any X from 1 to N. If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.
Parent TLV	Packet Classification Rule

1 **5.3.2.83 IP Remained Time**

Type	83
Length in octets	4 bytes
Value	32-bit unsigned integer.
Description	Remaining lease time for the assigned IP address. It is represented in unit of second.
Message Primitives That Use This TLV	DHCP Proxy Info

2 **5.3.2.84 IP Source Address and Mask**

Type	84
Length in octets	Nx8 (IPv4) or Nx32 (IPv6)
Value	List of the IP Source Address/Mask pairs: { (Src1, Smask1),..., (SrcN, SmaskN) }.
Description	This parameter specifies a list of IP source addresses and their corresponding address masks An IP packet with IP source address "ip-src" matches this parameter if SrcX = (ip-src AND SmaskX) for any X from 1 to N. If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.
Parent TLV	Packet Classification Rule

3 **5.3.2.85 IP TOS/DSCP Range and Mask**

Type	85
Length in octets	3
Value	The value field is structured as follows: • Lower Limit – 1 byte • Higher Limit – 1 byte • Mask – 1 byte
Description	The values of the field specify the matching parameters for the IP type of service/DSCP [IETF RFC 2474] byte range and mask. An IP packet with IP type of service (ToS) byte value "ip-tos" matches this parameter if tos-low less than or equal (ip-tos AND tos-mask) less than or equal tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.
Parent TLV	Packet Classification Rule

4 **5.3.2.86 Key Change Indicator**

Type	86
Length in octets	1

Value	• 0 = Success
	• 1 = Failure
	Other values are reserved.
Description	The value of this parameter indicates to ASN GW/Authenticator the results of PKMv2 3-way handshake process. Note, that BS indicates "Success" results when it ensures that MS had received PKMv2 SA-TEK-Response message and successfully enforced the new PMK/ AK contexts.
Message Primitives That Use This TLV	*Key_Change_Cnf*, *MS_Attachment_Req*

1 **5.3.2.87 L-BSID**

Type	87
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique BS Identifier, referring to a single sector with a single frequency assignment.
Parent TLV	

2 **5.3.2.88 Location Update Status**

Type	88
Length in octets	1
Value	• 0 = Refuse
	• 1 = Accept
Description	
Parent TLV(s)	Paging Information

3 **5.3.2.89 Location Update Success/Failure Indication**

Type	89
Length in octets	1
Value	
Description	Enumerator:
	• Value of "0" = Success
	• Non "0" value = Failure with some cause (the non-zero value will correspond to failure cause. Currently open issue: list of failure causes.)
Parent TLV(s)	Paging Information

4 **5.3.2.90 LU Result Indicator**

Type	90
Length in octets	1

Value	• 0 = Success
	• 1 = Failure
Description	Boolean that indicates the result of the LU operation.
Parent TLV(s)	

1 5.3.2.91 Maximum Latency

Type	91
Length in octets	4
Value	32-bit integer specifies the maximum latency (in milliseconds)
Description	Time period between the reception of a packet by the BS or MS on its network interface and the delivering the packet to the RF Interface of the peer device. If defined, this parameter represents a service commitment (or admission criteria) at the BS or MS and SHALL be guaranteed by the BS or MS. A BS or MS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Parent TLV	• UGS Data Delivery Service
	• ERT-VR Data Delivery Service
	• RT-VR Data Delivery Service

2 5.3.2.92 Maximum Sustained Traffic Rate

Type	92
Length in octets	4
Value	32-bit integer representing rate (in bits per second).
Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Parent TLV	• ERT-VR Data Delivery Service
	• RT-VR Data Delivery Service
	• NRT-VR Data Delivery Service
	• BE Data Delivery Service

3 5.3.2.93 Maximum Traffic Burst

Type	93
Length in octets	4
Value	32-bit integer representing burst size (in bytes).

Description	This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Parent TLV	• ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service

1 **5.3.2.94 Media Flow Type**

Type	94
Length in octets	1 + Variable
Value	The 1st octet is enumerator with the following values: • 0 = Reserved • 1 = Voice over IP • 2 = Robust Browser • 3 = Secure Browser/ VPN • 4 = Streaming video on demand • 5 = Streaming live TV • 6 = Music and Photo Download • 7 = Multi-player gaming • 8 = Location-based services • 9 = Text and Audio Books with Graphics • 10 = Video Conversation • 11 = Message • 12 = Control • 13 = Data • 14 – 254 = Reserved • 255 = Media Description in SDP format is included The 1st octet is always present in this TLV as an enumerator. Other fields presence and format depends on the code value set in the enumerator: If the 1st octet enumerator is set to indicate "Media Description in SDP format" (value 255), then variable-length SDP string is added: <SDP string> encoded as specified in IETF RFC 2327. The rules for information to be included – FFS. The rules for information to be included – FFS.
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Parent TLV	QoS Info

2 **5.3.2.95 Minimum Reserved Traffic Rate**

Type	95
Length in octets	4

Value	32-bit unsigned integer representing rate (in bits per second).
Description	This parameter specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second and specifies the minimum amount of data to be transported on behalf of the service flow when averaged over time. The specified rate SHALL only be honored when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter SHALL be satisfied by assuring the available data is transmitted as soon as possible.
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service

1 **5.3.2.96 MIP4 Info**

Type	96	
Length in octets	Variable	
Value	Compound	
Description	MIP4 Information about the MS	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	HA IP Address	O
	Home Address (HoA)	O
	CoA Address	O
Message Primitives That Use This TLV	ANCHOR MM Context	

2 **5.3.2.97 RRP**

Type	97
Length in octets	variable
Value	Same as defined in [15] including IP/UDP headers
Description	MIP Register Response message defined in [15]
Parent TLV(s)	FA_Register_Rsp

3 **5.3.2.98 MN-FA Key**

Type	98
Length in octets	20 bytes
Value	160-bit unsigned integer
Description	Using MN-FA key to calculate and authenticate MN-FA-AE, integrity can be protected between MN and FA.
Message Primitives That Use This TLV	MIP4 Security Info

1   **5.3.2.99 MN-FA SPI**

Type	99
Length in octets	4 bytes
Value	32-bit unsigned integer
Description	Key ID of MN-FA key.
Message Primitives That Use This TLV	MIP4 Security Info

2   **5.3.2.100 MS Authorization Context**

Type	100	
Length in octets	Variable	
Value	Compound	
Description		
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	MS NAI	M
	WiMAX Capability	M
	CUI	O
	Class	O
	Framed IP Address	O
	Framed IPv6 Prefix	O
	AAA Session ID	M
	Packet Flow Descriptor	O
	QoS Descriptor	O
	Acct Interim Interval	O
Parent TLV	MS Info	

3   **5.3.2.101 MS FA Context**

Type	101
Length in octets	Variable
Value	
Description	Compound TLV including FA context parameters related to the specific MS, etc.
Parent TLV(s)	MS Info

4   **5.3.2.102 MSID**

Type	102

Length in octets	6
Value	48-bit MS MAC address
Description	Unique MS identifier (MS MAC address)
Parent TLV	MS Info

1   **5.3.2.103 MS Info[31]**

Type	103	
Length in octets	Variable but not less than 10	
Value	Compound	
Description	Information about the MS	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Failure Indication	O
	MSID	O
	SF Info	O[32] (Note 1)
	Data Path Info	O (Note 2)
	Anchor GW ID	O (Note 3)
	Authenticator ID	O (Note 4)
	AK Context	O (Note 5)
	SA Descriptor	O
	Service Authorization Code	O
	REG Context	O
	SBC Context	O
	PKM Context	O
	Anchor MM Context	O
	Tunnel Endpoint	O
	MS Security History	O[33]
	MS Authorization Context	O
	MS Networking Context	O
	FA Context	O
	Authentication Result	O[34]
	FA Relocation Indication	

---

[31] When MS Info is included in any other TLV, duplicated TLVs between the two may be avoided in the TLV where MS Info is included.

[32] SF Info TLV is Mandatory in HO_Req message in Mobility. See section 4.7.2.1.

[33] MS Security History is mandatory when MS Info is included in Relocation_Notify message

[34] Authentication Result is mandatory when MS Info is included in Relocation_Cnf message.

	BS-originated EAP Start Flag	O
Message Primitives That Use This TLV	Every Message	

1 **Notes**

2 1) One or more SF Info TLVs MAY be included in order to describe Service Flows in Data Path Control,
3 Reservation, and HO Control Messages. Data Path Control SF Info is included in the case of Per-SF data path
4 tunneling granularity.

5 2) DP Info shall be included as sub-TLV of MS Info in Data Path Control Messages in order to describe data path
6 with Per-MS tunneling granularity. In the case of Per-SF data path tunneling granularity, DP Info shall be
7 included as sub-TLV of SF Info.

8 3) Anchor GW ID points to the network entity that hosts Anchor DP Function.

9 It MAY be included as sub-TLV of MS Info in *HO_Req* message in order to inform the Target ASN (or Target
10 BS) about the location of the network entity that hosts Anchor DP Function.

11 Anchor GW ID MAY be included as sub-TLV of MS Info in Data Path Control messages in order to inform the
12 peer about the location of the network entity that hosts Anchor DP Function.

13 It MAY be included as sub-TLV of MS Info in Context Delivery messages.

14 4) Authenticator GW ID points to the network entity that hosts Authenticator Function.

15 It MAY be included as sub-TLV of MS Info in *HO_Req* message in order to inform the Target ASN (or Target
16 BS) about the location of the network entity that hosts Authenticator Function. It doesn't have to be included if
17 AK Context is included. If neither Authenticator GW ID nor AK Context is included means that the sender of
18 the *HO_Req* hosts the Authenticator Function for the MS.

19 Authenticator GW ID MAY be included as sub-TLV of MS Info in Data Path Control messages in order to
20 inform the peer about the location of the network entity that hosts Authenticator Function.

21 It MAY be included as sub-TLV of MS Info in Context Delivery messages.

22 5) AK Context shall be included as sub-TLV of MS Info in the following messages:

23   i. Key_Change_Directive Message in order to transfer the new security context (AK
24   Context) to BS and trigger the PKMv2 3-WHS process between the BS and the MS.

25   ii. Context_Rpt from authenticator ASN to Target ASN.

26   iii. May be included in HO-Req message.

27 **5.3.2.104 MS Mobility Mode**

Type	104
Length in octets	2 byte
Value	Indicates the R3 mobility the MS is using: • 00 = PMIP4 • 01 = CMIP4 • 10 = CMIP6 • 11 = Reserved
Description	
Parent TLV(s)	Anchor MM Context

1   **5.3.2.105 MS NAI**

Type	105
Length in octets	Variable up to 256 octets
Value	ASCII String
Description	MS Network Access Identifier character string
Parent TLV(s)	MS Security History

2   **5.3.2.106 MS Networking Context**

Type	106
Length in octets	Variable
Value	
Description	Compound TLV
Parent TLV(s)	MS Info

3   **5.3.2.107 MS Security Context**

Type	107	
Length in octets	Variable	
Value	Compound TLV	
Description	Groups MS security association descriptors.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	SA Descriptor	M [Note 1]
Parent TLVs	MS Info	

4   Note 1: Multiple SA Descriptor TLVs MAY be included.

5   **5.3.2.108 MS Security History**

Type	108	
Length in octets	Variable	
Value	Compound TLV	
Description	Security parameters presenting the history of MS authentication	
Elements (Bus-TLVs)	**TLV Name**	**M/O**
	PMK SN	M
	PMK2 SN	O
	MS NAI	M
	Authorization Policy	M [Note 1]
	Device Authentication Indicator	O
	VAAA Realm	O [Note 2]
	VAAA IP Address	O [Note 2]

Parent TLV(s)	MS Info

1 Note 1: Authorization Policy TLV in MS Security History indicates the authentication modes as previously
2 negotiated with MS (single EAP, double EAP, both).

3 Note 2: Either VAAA Realm or VAAA IP Address TLV should be present.

4 **5.3.2.109 Network Exit Indicator**

Type	109
Length in octets	1
Value	Enumerator. The values are: • 0x00 = MS Power Down indication (used if Network Exit Indicator is requested in RNG REQ), • 0x01 = Radio link with MS is lost, • 0x02 - 0xFF = Reserved
Description	Present in operations related to MS Network Exit and indicates MS Network Exit reason
Parent TLV(s)	Paging Information, Path Control messages (*Path_Dereg_Req*), MS State Change messages.

5 **5.3.2.110 Newer TEK Parameters**

Type	110	
Length in octets	Variable	
Value	Compund TLV	
Description	Set of the Newer TEK Parameters	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
Parent TLVs	SA Descriptor	

6 **5.3.2.111 NRT-VR Data Delivery Service**

Type	111	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for NRT-VR Data Delivery Service. If included in QoS Info, it implies nrtPS Scheduling Service for UL connections.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Minimum Reserved Traffic Rate	M

Traffic Priority	O (if omitted means Traffic Priority = 0)
Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
Request / Transmission Policy	O (see Note [a])
Maximum Traffic Burst	O
Parent TLV	QoS Info

1   Note [a]: Used only during HO/ Idle Mode entry/exit operations.

2   **5.3.2.112 Older TEK Parameters**

Type	112	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of the Older TEK Parameters	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
Parent TLVs	SA Descriptor	

3   **5.3.2.113 Old Anchor PCID**

Type	113
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	Unique identifier for the Old Anchor Paging Controller network entity, which administers paging activity for the MS while in Idle Mode and retains MS service and operational information. The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	
Parent TLV(s)	Paging Information

4   **5.3.2.114 Packet Classification Rule / Media Flow Description (one or more)**

Type	114
Length in octets	Variable
Value	Compound

Description	Contains sub-elements representing Classifier Rule Priority and Set of Classifiers functionally equivalent to those defined in 802.16. All parameters pertaining to a specific classification rule SHALL be included in the same Packet Classification Rule compound parameter. The TLV contains one packet classification rule.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Classifier	M
	Classification Rule Action Note: The Classifier Rule Action applies "only" to the service flow modification; and it does not apply to the service flow creation or deletion.	M
	Classifier Rule Priority	O
	IP TOS/DSCP Range and Mask	O
	Protocol	O
	IP Source Address and Mask	O
	IP Destination Address and Mask	O
	Protocol Source Port Range	O
	Protocol Destination Port Range	O
	Associated PHSI	O
	ROHC/ECRTP Context ID	O
Parent TLV	SF Info	

1 **5.3.2.115 Paging Announce Timer**

Type	115
Length in octets	2 octet
Value	
Description	PagingAnnounce timer = 0 stands for infinite tries. The PagingAgent will continue paging this MS until it receives a Paging::Stop message for this MS. PagingAnnounce Time > 0 implies that the Paging Agent will page the MS until this timer expires.
Parent TLV(s)	Paging Information

2 **5.3.2.116 Paging Cause**

Type	116
Length in octets	1
Value	• 01 = LCS • 02 = Incoming Data for Idle MS • 03 = Acknowledge Exiting Idle Mode. • 04 = Reserved
Description	
Parent TLV(s)	Paging Information

1   **5.3.2.117 Paging Controller Identifier**

Type	117
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	Unique identifier for the Paging Controller network entity network entity, which partakes in forwarding of Idle mode and Paging related network messages to the Paging region. The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Value	
Parent TLV(s)	Paging Information

2   **5.3.2.118 Paging Cycle**

Type	118
Length in octets	2
Value	
Description	Cycle in which the paging message is transmitted within the paging group (aligned with 802.16e)
Parent TLV(s)	Paging Information

3   **5.3.2.119 Paging Information**

Type	119	
Length in octets	Variable	
Value		
Description	Set of Paging related IEs.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Paging Cycle	O
	Paging Offset	O
	Relocation Response	O
	Relocation Success Indication	O
	Paging Group ID	O
	Paging Controller ID	O
	Anchor Paging Controller ID	O
	Location Update Success / Failure Indication	O
	Exit Idle Mode Operation Indication	O
	Idle Mode Retain Info	O
	Paging Start / Stop	O
	Anchor PC Relocation Destination	O
	Anchor PC Relocation Request Response	O

	Network Exit Indicator	O
	Location Update Status	O
	Paging Cause	O
Message Primitives That Use This TLV	Paging Function messages; Data Path Control messages; Context Delivery messages.	

1 **5.3.2.120 Paging Offset**

Type	120
Length in octets	2
Value	
Description	Determines the frame within the cycle in which the paging message is transmitted. SHALL be smaller then the PAGING CYCLE value.
Parent TLV(s)	Paging Information

2 **5.3.2.121 Paging Start/Stop**

Type	121
Length in octets	1
Value	
Description	Indicates to the BSs whether to start/stop paging on the airlink
Parent TLV(s)	Paging Information

3 **5.3.2.122 PC Relocation Indication**

Type	122
Length in octets	1
Value	
Description	Request from the Current Anchor PC to the New Anchor PC to perform PC relocation
Message Primitives That Use This TLV	R4 *LU_Rsp*

4 **5.3.2.123 PGID - Paging Group ID**

Type	123
Length in octets	
Value	
Description	16-bit ID representing Paging Group. Some places in 16e mention 8 bits
Parent TLV(s)	Paging Information

1 **5.3.2.124 PHSF**

Type	124
Length in octets	Variable
Value	Byte string
Description	String of bytes containing the header information to be suppressed
Parent TLV	PHS Rule

2 **5.3.2.125 PHSI**

Type	125
Length in octets	1
Value	8-bit unsigned integer
Description	PHSI has a value between 1 and 255, which uniquely references the suppressed byte string. The index is unique per service flow. The uplink and downlink PHSI values are independent of each other.
Parent TLV	PHS Rule

3 **5.3.2.126 PHSM**

Type	126
Length in octets	Variable
Value	Bit string
Description	The value of this field is used to interpret the values in the PHSF. It is used at both the sending and receiving entities. The PHSM allows fields, such as sequence numbers or checksums (which vary in value), to be excluded from suppression with the constant bytes around them suppressed: - Bit 0: 0 = Do not suppress first byte of the suppression field, 1 = Suppress first byte of the suppression field - Bit 1: 0 = Do not suppress second byte of the suppression field, 1 = Suppress second byte of the suppression field - Bit x: 0 = Do not suppress (x+1) byte of the suppression field, 1 = Suppress (x+1) byte of the suppression field.
Parent TLV	PHS Rule

4 **5.3.2.127 PHS Rule**

Type	127	
Length in octets	Variable	
Value	Compound	
Description	Parameters associated with a PHS Rule. Omission means PHS is disabled.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	PHSI	M
	PHSS	M

	PHSF	M
	PHSM	M
	PHSV	M
	Vendor-specific PHS Parameters	O
	PHS Rule Action	O
Parent TLV	SF Info	

1 **5.3.2.128 PHS Rule Action**

Type	128
Length in octets	1
Value	PHS Action Code • 0 = Add PHS Rule • 1 = Replace PHS Rule • 2 = Delete PHS Rule • 3 = Delete All PHS Rules
Description	
Parent TLV	SF Info

2 **5.3.2.129 PHSS**

Type	129
Length in octets	1
Value	8-bit unsigned integer
Description	The value of this field is the total number of bytes in the header to be suppressed and then restored in a service flow that uses PHS. This TLV is used when a service flow is being created. For all packets that get classified and assigned to a service flow with PHS enabled, suppression SHALL be performed over the specified number of bytes as indicated by the PHSS and according to the PHSM. If this TLV is not included in a service flow definition, or is included with a value of 0 bytes, then PHS is disabled. A nonzero value indicates PHS is enabled.
Parent TLV	PHS Rule

1   **5.3.2.130 PHSV**

Type	130
Length in octets	1
Value	• 0 = Verify • 1 = Don't verify
Description	The value of this field indicates to the sending entity whether or not the packet header contents are to be verified prior to performing suppression. If PHSV is enabled, the sender SHALL compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM.
Parent TLV	PHS Rule

2   **5.3.2.131 PKM Context**

Type	131
Length in octets	1
Value	8-bit unsigned integer
Description	Identifies the profile of the PKM related capabilities of the MS. • 0 = PKM Capabilities defined in the MTG Profile. Other values are not used.
Parent TLV	MS Info

3   **5.3.2.132 PMIP4 Client Location**

Type	132
Length in octets	4 bytes
Value	IP address of the entity which contain the MS corresponding PMIP4 client function
Description	
Parent TLV(s)	Anchor MM Context

4   **5.3.2.133 PMK SN**

Type	133
Length in octets	1
Value	0X0000	4-bit PMK SN
Description	PMK Sequence Number as specified by IEEE 802.16e.
Parent TLV(s)	MS Security History

5   **5.3.2.134 PKM2**

Type	134
Length in octets	1

Value	The value of this parameter indicates to BS the message code that SHOULD be used on PKMv2 and indirectly the state of authentication process:
	• 18 = EAP Transfer
	• 19 = Authenticated EAP Transfer
	• 29 = EAP Complete
	Other values are reserved
Description	
Parent TLV(s)	Authentication Complete

5.3.2.135 PMK2 SN

Type	135
Length in octets	1
Value	0X0000 | 4-bit PMK2 SN
Description	PMK2 Sequence Number as specified by IEEE 802.16e.
Parent TLV(s)	MS Security History

5.3.2.136 PN Counter

Type	136
Length in octets	4
Value	Unsigned 32-bit integer
Description	Last value of PN Counter used on DL (for AES CCM cipher suite)
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

5.3.2.137 Preamble Index/Sub-channel Index

Type	137
Length in octets	1
Value	8-bit integer representing Preamble Index/Sub-channel Index
Description	
Parent TLV	BS Info

5.3.2.138 Protocol

Type	138
Length in octets	Nx2
Value	16 bit integers, each representing IP Protocol: {prot1, prot2,...protN}.
Description	The value of the field specifies a list of matching values for the IP Protocol field. For IPv6 (IETF RFC 2460), this refers to next header entry in the last header of the IP header chain. The encoding of the value field is that defined by the IANA document "Protocol Numbers." If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

Parent TLV	Packet Classification Rule

1 **5.3.2.139 Protocol Destination Port Range**

Type	139
Length in octets	Variable
Value	Destination Protocol Port Ranges: { (DstPortLow1, DstPortHigh1),..., (DstPortLowN, DstPortHighN) }.
Description	The value of the field specifies a list of non-overlapping ranges of protocol destination port values. Classifier rules with port numbers are protocol specific; i.e., a rule on port numbers without a protocol specification SHALL not be defined. An IP packet with protocol port value "DstPort" matches this parameter if DstPort is greater than or equal to DstPortLow and DstPort is less than or equal to DstPortHigh. If this parameter is omitted, the protocol source port is irrelevant. This parameter is irrelevant for protocols without port numbers.
Parent TLV	Packet Classification Rule

2 **5.3.2.140 Protocol Source Port Range**

Type	140
Length in octets	Variable
Value	Source Protocol Port Ranges: { (SrcPortLow1, SrcPortHigh1),..., (SrcPortLowN, SrcPortHighN) }.
Description	The value of the field specifies a list of non-overlapping ranges of protocol source port values. Classifier rules with port numbers are protocol specific; i.e., a rule on port numbers without a protocol specification SHALL not be defined. An IP packet with protocol port value "SrcPort" matches this parameter if SrcPort is greater than or equal to SrcPortLow and SrcPort is less than or equal to SrcPortHigh. If this parameter is omitted, the protocol source port is irrelevant. This parameter is irrelevant for protocols without port numbers.
Parent TLV	Packet Classification Rule

3 **5.3.2.141 QoS Parameters**

Type	141	
Length in octets	Variable	
Value	Compound	
Description	This compound parameter contains the QoS parameters. All parameters pertaining to a specific QoS description SHALL be included in the same QoS Info compound parameter.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BE Data Delivery Service	O
	UGS Data Delivery Service	O
	NRT-VR Data Delivery Service	O
	RT-VR Data Delivery Service	O

	ERT-VR Data Delivery Service	O
	Global Service Class Name	O
	Service Class Name	O
	Media Flow Type	O
	Reduced Resources Code	O
	Date Integrity [Note: TBD}	O
Parent TLV	SF Info	

1 If no Data Delivery Service Sub-TLV is included then the Data Delivery Service defaults to BE Data Delivery
2 Service with Traffic Priority equal to zero and Request Transmit Policy equal to zero.

3 **5.3.2.142 Radio Resource Fluctuation**

Type	142
Length in octets	1
Value	8-bit unsigned integer.
Description	Radio Resource Fluctuation is used to indicate the degree of fluctuation in DL and UL channel data traffic throughputs. When Radio Resource Fluctuation is set to 0, it implies that the DL and UL data traffic is constant in data throughput. Hence, there is no fluctuation in Available Radio Resource. When Radio Resource Fluctuation is set to maximum value 255, the data traffic is very volatile in nature which makes the Available Radio Resource unpredictable. The Radio Resource Fluctuation for all traffic models should be in the range of 0 to 255."
Parent TLV(s)	RRM BS Info

4 **5.3.2.143 Reduced Resources Code**

Type	143
Length in octets	0
Value	Value = Null, see Description
Description	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available. (TBD: encoding)
Parent TLV	QoS Info

5 **5.3.2.144 REG Context**

Type	144
Length in octets	1
Value	8-bit unsigned integer
Description	Identifies the profile of the capabilities of the MS negotiated during REG handshake • 0 = REG handshake related capabilities defined in the MTG Profile. Other values are not used.
Parent TLV(s)	MS Info

1   **5.3.2.145 Registration Type**

Type	145
Length in octets	4
Value	Enumerator. The values are: {Initial Network Entry, HO, In-Service Data Path Establishment, MS Network Exit, Idle Mode Entry and Idle Mode Exit }.
Description	Indication of the process which includes data path (Pre-) Registration.
Message Primitives That Use This TLV	DP Control messages (Path (Pre-/De-) Registration/Modification Request/Response/Acknowledge)

2   **5.3.2.146 Relative Delay**

Type	146
Length in octets	1
Value	8-bit integer representing Target BS Relative Delay in msecs.
Description	
Parent TLV	BS Info

3   **5.3.2.147 Relocation Destination ID**

Type	147
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	
Description	Identifier of the PC function that we want to relocate the Anchor PC to. Presence of this TLV implicitly constitutes a request for relocation of Anchor PC The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Parent TLV(s)	Paging Information

4   **5.3.2.148 Relocation Response**

Type	148
Length in octets	1
Value	
Description	Boolean ("Refuse" (0) and Accept (1)) response to *Relocation_Req*.
Parent TLV(s)	Paging Information

5   **5.3.2.149 Relocation Success Indication**

Type	149
Length in octets	1
Value	

Description	(Boolean (Success (0) and Failure (1)) Indicates confirmation of whether the Relocation was accepted and completed by the Relocation Destination
Parent TLV(s)	Paging Information

5.3.2.150 Request/Transmission Policy

Type	150
Length in octets	4
Value	32-bit bitmask. • Bit #0 = Service flow SHALL not use broadcast bandwidth request opportunities. (Uplink only) • Bit #1 = Reserved. • Bit #2 = Service flow SHALL not piggyback requests with data. (Uplink only) • Bit #3 = Service flow SHALL not fragment data. • Bit #4 = Service flow SHALL not suppress payload headers (CS parameter) • Bit #5 = Service flow SHALL not pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 = Service flow SHALL not include CRC in the MAC PDU. All other bit positions are reserved.
Description	The value of this parameter provides the capability to specify certain attributes for the associated service flow. These attributes include options for PDU formation, and for uplink service flows, restrictions on the types of bandwidth request options that may be used. An attribute is enabled by setting the corresponding bit position to 1.
Parent TLV	QoS Info

5.3.2.151 Reservation Action

Type	151
Length in octets	2
Value	The Action field is a 16 bit vector with the following meaning for each bit being set to "1": • Bit 15 (0x0001) = Create service flow • Bit 14 (0x0002) = Admit service flow • Bit 13 (0x0004) = Activate service flow • Bit 12 (0x0008) = Modify service flow • Bit 11 (0x000A) = Delete service flow • Bits 0 – 10 = Undefined More than one of bits 13-15 MAY be set to 1 at the same time (for instance, create & admit, or create/admit/activate/ modify a service flow).
Description	Identifies the requested resource reservation action
Parent TLV	SF Info

5.3.2.152 Reservation Result

Type	152

Length in octets	2
Value	Result can be one of the following: • 0x0000 = Successfully Created • 0x0001 = Request Denied – No resources • 0x0002 = Request Denied due to Policy • 0x0003 = Request Denied due to Requests for Other Flows Failed. • 0x0004 = Request Failed (Unspecified reason) • 0x0005 = Request Denied due to MS reason • Other = Reserved
Description	Indicates the result of a Resource Reservation Request.
Parent TLV	SF Info

1   **5.3.2.153 Response Code**

Type	153
Length in octets	1
Value	Enumerator: The values are: • 0x00 = Not allowed - Paging Reference is zero • 0x01 = Not allowed - No such SF
Description	Indicates reason for not paging the MS
Message Primitives that Use This TLV	Initiated_Paging_Rsp

2   **5.3.2.154 Result Code**

Type	154
Length in octets	1
Value	Enumerator: The values are: • 0x00 = Success • 0x01 = Failure – No resources • 0x02 = Failure – Not supported
Description	Indicates if the requested action was successfully supported at the intended target.
Message Primitives that use this TLV	HO related messages, Path (pre-)registration related messages.

3   **5.3.2.155 ROHC/ECRTP Context ID**

Type	155
Length in octets	TBD
Value	TBD
Description	

Parent TLV	Packet Classification Rule

1   **5.3.2.156 Round Trip Delay**

Type	156
Length in octets	1
Value	8-bit integer representing Serving BS Round Trip Delay in seconds
Description	
Parent TLV	BS Info

2   **5.3.2.157 RRM Absolute Threshold Value J**

Type	157
Length in octets	1
Value	8-bit unsigned integer: • 0x00 = 0% • 0x01 = 1%, ..., • 0x64 = 100% • 0x65 – 0xFE = reserved
Description	The threshold value J is used by BS (RRA) as the absolute threshold for reporting.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

3   **5.3.2.158 RRM Averaging Time T**

Type	158
Length in octets	2
Value	16-bit unsigned integer, in units of 100 msec.
Description	Used by BS (RRA) as the measurement interval for producing the information requested by RRC.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

1   **5.3.2.159 RRM BS Info**

Type	159	
Length in octets	Variable	
Value	Compound	
Description	Contains a description of BS parameters which are not related to a specific MS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BS ID	M
	Available Radio Resource DL	O
	Total slots DL	O
	Available Radio Resource UL	O
	Total slots UL	O
	Radio Resource Fluctuation	O
	DCD/UCD Configuration Change Count	O
	Full DCD Setting	O
	Full UCD Setting	O
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Neighbor_BS_Resource_Status_Update*, RRM *Radio_Config_Update_Rpt*.	

1 **5.3.2.160 RRM BS-MS PHY Quality Info**

Type	160
Length in octets	Variable
Value	Compound
Description	This compound TLV contains the PHY quality indicators of the radio channel between a BS and a specific MS identified by MSID in the message header.

Elements (Sub-TLVs)	TLV Name	M/O
	BS ID	M
	Round Trip Delay (Serving Only)	O
	Relative Delay (Target Only)	O
	DL PHY Quality Info	O
	DL PHY Service Level	O
	UL PHY Quality Info	O
	UL PHY Service Level	O
	Temporary BS ID	O
	HO ID	O
	Service Level Prediction	O
	Preamble Index / Sub-channel Index	O
	SF Info (for Data Integrity)	O

Message Primitives That Use This TLV	RRM *PHY_Parameters_Rpt*

2 **5.3.2.161 RRM Relative Threshold RT**

Type	161
Length in octets	1
Value	8-bit unsigned integer: • 0x00 = 0% • 0x01 = 1%, • ..., • 0x64 = 100% • 0x65 – 0xFE = reserved
Description	The threshold value RT is used by BS (RRA) to keep track of the threshold from the last measurement period.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

1 **5.3.2.162 RRM Reporting Characteristics**

Type	162
Length in octets	4
Value	32-bit bitmask representing the characteristics of reporting. • Bit #0 = periodically as defined by reporting period P • Bit #1 = regularly whenever resources have changed as defined by RT since the last measurement period. • Bit #2 = regularly whenever resources cross predefined total threshold(s) defined by reporting absolute threshold values J • Bit #3 = DCD/UCD Configuration Change Count modification • Bit #4 – #31 = reserved
Description	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

2 **5.3.2.163 RRM Reporting Period P**

Type	163
Length in octets	2
Value	16-bit unsigned integer, in units of 100 msec.
Description	Used by BS (RRA) as the reporting period for producing the information requested by RRC. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

3 **5.3.2.164 RRM Spare Capacity Report Type**

Type	164
Length in octets	1
Value	Encoded as follows: • 0: "Type 1" which refers to reporting of the "Available radio resource indicator" • 1…255: reserved for future reporting types.
Description	The value of this parameter specifies the type of RRM *Spare_Capacity_Rpt* Forward compatibility: To allow for other types of spare capacity reports in future releases.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

1   **5.3.2.165 RT-VR Data Delivery Service**

Type	165	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for RT-VR Data Delivery Service. If included in QoS Info, it implies rtPS Scheduling Service for UL connections	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Minimum Reserved Traffic Rate	M
	Maximum Latency	M
	Unsolicited Polling Interval	M
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
	Request / Transmission Policy	O (see Note [a])
	Maximum Traffic Burst	O
Parent TLV	QoS Info	

2

3   **5.3.2.166 RxPN Counter**

Type	166
Length in octets	4
Value	Unsigned 32-bit integer
Description	Last value of PN Counter used on UL (for AES CCM cipher suite)
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

4

5   **5.3.2.167 R3 Operation Status**

Type	167
Length in octets	2 byte
Value	Indicates the operation result: • 00 = Success • 01 = Failure • 10 = Pending • 11 = Reserved
Description	
Parent TLV(s)	TBD

1   **5.3.2.168 R3 Release Reason**

Type	168
Length in octets	1 byte
Value	Indicates the R3 release reasons: • 00000000 = MS Initiated power down • 00000001 = Anchor Authenticator Initiated • 00000010 = Serving ASN Initiated • 00000011 = Anchor ASN Initiated • 00000100 - 11111111 = Reserved
Description	Release reasons included in R6 Session Release Request
Parent TLV(s)	None

2   **5.3.2.169 SAID**

Type	169
Length in octets	4
Value	SAID definition as per 802.16.
Description	The SAID is a 16-bit identifier for the SA
Parent TLV(s)	SF Info, SA Descriptor

3   **5.3.2.170 SA Descriptor**

Type	170	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of SA-related IEs	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	SA ID	M
	SA Type	M
	SA Service Type	O
	Cryptographic Suite	M
	Older TEK Parameters	O
	Newer TEK Parameters	O
	SA Index	
Parent TLVs	MS Info	

4   **5.3.2.171 SA Index**

Type	171
Length in octets	4

Value	Index which AAA Server assigns to an SA.
Description	
Parent TLV(s)	SA Descriptor

1 **5.3.2.172 SA Service Type**

Type	172
Length in octets	1
Value	• 0 = Unicast Service • 1 = Group Multicast Service • 2 = MBS Service • 3 – 255 = Reserved
Description	This attribute indicates service types of the corresponding SA type. This attribute SHALL be included only when the SA type is Static SA or Dynamic SA. The GTEK SHALL be used to encrypt connection for group multicast service. The MTK SHALL be used to encrypt connection for MBS service.
Parent TLV(s)	SA Descriptor

2 **5.3.2.173 SA Type**

Type	173
Length in octets	1
Value	Code identifying the value of SA-type as defined below. • 0 = Primary • 1 = Static • 2 = Dynamic • 3 – 127 = Reserved • 128 – 255 = Vendor Specific
Description	Type of SA.
Parent TLV(s)	SA Descriptor

3 **5.3.2.174 SBC Context**

Type	174
Length in octets	1
Value	8-bit bitmask

Description	Identifies the profile of the capabilities of the MS negotiated during SBC handshake
	• Bit#0 = Support OFDMA PHY parameter set A
	• Bit#1 = Support OFDMA PHY parameter set B
	• Bit#2-#4 = HARQ parameters set
	– 0b000 = HARQ set 1
	– 0b001 = HARQ set 2
	– 0b010 = HARQ set 3
	– 0b011 = HARQ set 4
	– 0b100 = HARQ set 5
	– 0b101-0b111 = Reserved
	• Bit# = Support OFDMA MAC parameters set A
	• Bit#6 = Support OFDMA MAC parameters set B
	• Bit#7 = Reserved
	Note: Bit#0 and #1 SHALL not be set to 1 together. Bit#5 and #6 SHALL not be set to 1 together.
Parent TLV(s)	

1   **5.3.2.175 SDU BSN Map**

Type	175
Length in octets	Variable
Value	Bitmap expressing which Blocks of the SDU have been transmitted and/or acknowledged.
Description	
Parent TLV	SDU Info

2   **5.3.2.176 SDU Info**

Type	176	
Length in octets	Variable	
Value		
Description	Information about an SDU involved in Data Path Integrity operations.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	SDU SN	M
	SDU BSN Map	O
Parent TLV	SF Info	

3   **5.3.2.177 SDU Size**

Type	177
Length in octets	1
Value	8-bit unsigned integer. Default = 49

Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	UGS Data Delivery Service

5.3.2.178 SDU SN

Type	178
Length in octets	4
Value	SDU Sequence Number (for Data Path Integrity operations)
Description	
Parent TLV	SDU Info

5.3.2.179 Service Class Name

Type	179
Length in octets	2 - 128
Value	Service Class Name as defined in IEEE802.16e
Description	ASCII string, which is known at the BS and which indirectly specifies a set of QoS Parameters.
Parent TLV	SF Info

5.3.2.180 Service Level Prediction

Type	180
Length in octets	1
Value	8-bit integer representing Service Level Prediction
Description	
Parent TLV	BS Info

5.3.2.181 Service Authorization Code

Type	181
Length in octets	
Value	
Description	
Parent TLV	

1 **5.3.2.182 Serving/Target Indicator**

Type	182
Length in octets	1
Value	Enumerator: The values are: • 0x00 = Serving • 0x01 = Target
Description	Indicates if the designated BS is the Serving BS or Target BS for the handover.
Message Primitives That Use This TLV	HO related messages.

2 **5.3.2.183 SF Classification**

Type	183
Length in octets	1
Value	• 0 = SF classification not supported • 1 = SF classification supported
Description	This parameter explains whether the service flow classification is supported or not.

3 (NOTE: The SF-classification parameter should be added to "Datapath Info" parent TLV as Mandatory.)

4 **5.3.2.184 SFID**

Type	184
Length in octets	4
Value	32-bit unsigned integer.
Description	SFID definition as per 802.16.
Parent TLV(s)	SF Info

5 **5.3.2.185 SF Info**

Type	185	
Length in octets	Variable	
Value		
Description	Service Flow Description	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	SFID	M
	Reservation Action	O
	Reservation Result	O
	Failure Indication	O
	Direction	M

	CID	O
	SAID	O
	Packet Classification Rule / Media Flow Description (one or more)	O
	QoS Parameters	O
	Reduced Resources	
	CS Type	O
	Data Path Info	O
	SDU Info	O
	PHS Rule Action	O
	Combined Resources Required	O
	Accounting Extension	O
	Data Integrity Info	O
	SA Descriptor	O
	Correlation ID	O
Parent TLV	MS Info	

1   **5.3.2.186 Spare Capacity Indicator**

Type	186
Length in octets	2
Value	16-bit signed integer
Description	The value defines how many MSs with certain Quality Of Service Parameters and certain PHY Quality Info may be accommodated. Negative value indicates that even the existing MSs suffer from degradation of service.
Parent TLV	BS Info

2   **5.3.2.187 TEK**

Type	187
Length in octets	Two fixed sizes, either 8 or 16
Value	64-bit or 128-bit string
Description	Traffic Encryption Key.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

3   **5.3.2.188 TEK Lifetime**

Type	188
Length in octets	4
Value	32-bit unsigned integer

Description	The remaining TEK Lifetime in seconds. Zero means that the corresponding TEK is not valid.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

1 **5.3.2.189 TEK SN**

Type	189
Length in octets	1
Value	8-bit unsigned integer with valid values from 0 to 3.
Description	2-bit TEK Sequence Number.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

2 **5.3.2.190 Tolerated Jitter**

Type	190
Length in octets	4
Value	32-bit unsigned integer (in milliseconds).
Description	This parameter represents the maximum delay variation (jitter) (in milliseconds).
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service

3 **5.3.2.191 Total Slots DL**

Type	191
Length in octets	2
Value	16-bit unsigned integer:
Description	Total number of slots in the DL frame. This is the total (max) number of slots possible in DL. This would depend on the RF channelization and the subchannelization schemes employed.
Parent TLV(s)	RRM BS Info

4 **5.3.2.192 Total Slots UL**

Type	192
Length in octets	2
Value	16-bit unsigned integer:
Description	Total number of slots in the UL frame. This is the total (max) number of slots possible in UL. This would depend on the RF channelization and the subchannelization schemes employed.
Parent TLV(s)	RRM BS Info

5 **5.3.2.193 Traffic Priority/QoS Priority**

Type	193

Length in octets	1
Value	0 to 7 = Higher numbers indicate higher priority. Default 0.
Description	The value of this parameter specifies the priority assigned to a service flow as it is defined for the Traffic Priority in IEEE802.16e [2]. Given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.
Parent TLV	- BE Data Delivery Service - UGS Data Delivery Service - NRT-VR Data Delivery Service - RT-VR Data Delivery Service - ERT-VR Data Delivery Service

5.3.2.194 Tunnel Endpoint

Type	194
Length in octets	4 or 16
Value	Either IPv4 or IPv6 Address
Description	Specifies the IP Address of the GRE tunnel associated with the Data Path. If omitted than the IP Address is defaulted to the Source Address of the sender of Path (Pre-) Registration Request
Parent TLV(s)	Data Path Info

5.3.2.195 UCD Setting

Type	195
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7
Description	This is an IEEE802.16e-2005 defined TLV. The UCD_settings is a TLV value that encapsulates a UCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. The UCD settings fields SHALL contain only neighbor's UCD TLV values that are different from the serving BS corresponding values. For values that are not included, the MS SHALL assume they are identical to the corresponding values of the serving BS. The duplicate TLV encoding parameters within a Neighbor BS SHALL not be included in UCD setting. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info
Message Primitives That Use This TLV	*Neighbor_BS_Resource_Status_Update*.

1 **5.3.2.196 UGS Data Delivery Service**

Type	196
Length in octets	Variable
Value	Compound
Description	This compound TLV contains the QoS parameters relevant for UGS Data Delivery Service. If included in QoS Info, it implies UGS Scheduling Service for UL connections
Elements (Sub-TLVs)	**TLV Name**
	Minimum Reserved Traffic Rate
	Maximum Latency
	Tolerated Jitter
	SDU Size
	Unsolicited Grant Interval
	Traffic Priority
	Request/Transmission Policy
Parent TLV	QoS Info

	TLV Name	M/O Flag
	Minimum Reserved Traffic Rate	M
	Maximum Latency	M
	Tolerated Jitter	O (omission means jitter equal to maximum latency)
	SDU Size	O (omission means variable size SDU)
	Unsolicited Grant Interval	M
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Request/Transmission Policy	O (see Note [a])

2 Note [a]: Used only during HO/ Idle Mode entry/exit operations.

3 **5.3.2.197 UL PHY Quality Info**

Type	197
Length in octets	4
Value	32-bit integer encoding 8-bit UL RSSI Mean, 8-bit UL RSSI Std, 8-bit UL CINR Mean, 8-bit UL CINR Std.
Description	
Parent TLV	BS Info

4 **5.3.2.198 UL PHY Service Level**

Type	198
Length in octets	4
Value	32-bit integer representing UL PSL
Description	
Parent TLV	BS Info

5 **5.3.2.199 Unsolicited Grant Interval**

Type	199
Length in octets	2
Value	16-bit unsigned integer representing the grant interval (in milliseconds).

Description	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for a UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	• ERT-VR Data Delivery Service • UGS Data Delivery Service

1 **5.3.2.200 Unsolicited Polling Interval**

Type	200
Length in octets	2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Parent TLV	RT-VR Data Delivery Service

2 **5.3.2.201 VAAA IP Address**

Type	201
Length in octets	4 or 16
Value	The length defines the format of this value – IPv4 or IPv6. The value with length of 4 octets provides IPv4 address. The value with 16 octets provides IPv6 address.
Description	VAAA IPv4 or IPv6 address.
Parent TLV(s)	MS Security History

3 **5.3.2.202 VAAA Realm**

Type	202
Length in octets	Variable up to 256 octets
Value	ASCII String
Description	VAAA realm character string
Parent TLV(s)	MS Security History

4 **5.3.2.203 BS HO RSP Code**

Type	203
Length in octets	1Byte
Value	0: success 1: Target BS doesn't support this HO Type; 2: Target BS's air link resource is not enough; 3: Target BS's CPU overload; 4: Target BS rejects for other reasons. 5-255: Reserved
Description	This TLV is used to carry HO failure reason for target BS.

Parent TLV(s)	BS Info

1 5.3.2.204 Accounting Context

Type	204
Length in octets	Variable
Value	Compound
Description	Accounting Context

Elements (Sub-TLVs)	TLV Name	M/O
	Accounting Mode Provisioning	M

Message Primitives That Use This TLV	RR_Req (Create) / HO_Req/Context_Rpt / IM_Exit_State_Change_Req

2 5.3.2.205 HO ID

Type	205
Length in octets	Shall follow 802,16e
Description	This IE is defined in the IEEE 802.16e spec

3 5.3.2.206 Place holder left intentionally empty

4 5.3.2.207 R3 Wimax Capability

Type	207
Length	Variable.
Value	Compound
Description	

Elements	TLV Name	M/O
	Accounting Capabilities	M
	Idle Mode Notification Capabilities	O
Parent TLV	Ms Authorization Context	

5 5.3.2.208 R3 Accounting Capabilities

Type	208
Length	1
Value	• 0x00 = No accounting. Only valid at the HA. • 0x01 = IP-Session-based accounting. Default value for the ASN. • 0x02 = Flow-based accounting
Description	Accounting Capabilities
Parent TLV	Wimax Capability

1 **5.3.2.209 R3 Idle Notification Capabilities**

Type	209
Length	1
Value	• 0x00 = Idle Mode notification is not supported or is not required. • 0x01 = Idle Mode notification is supported or is required.
Description	Idle notification Capabilities
Parent TLV	Wimax Capability

2 **5.3.2.210 R3 CUI**

Type	210
Length	Variable.
Value	String
Description	CUI
Parent TLV	Ms Authorization Context

3 **5.3.2.211 R3 Class**

Type	211
Length	Variable.
Value	String
Description	Class
Parent TLV	Ms Authorization Context

4 **5.3.2.212 R3 Framed IP Address**

Type	212
Length	4
Value	32bits unsigned integer
Description	Framed-IP-Address
Parent TLV	Ms Authorization Context

5 **5.3.2.213 R3 Framed IPv6 Prefix**

Type	213
Length	Variable
Value	0-16 bytes
Description	Framed-IPv6-Prefix
Parent TLV	Ms Authorization Context

6 **5.3.2.214 R3 AAA Session ID**

Type	214

Length	Variable.
Value	String
Description	AAA Session ID
Parent TLV	Ms Authorization Context

1   **5.3.2.215 R3 Packet Flow Descriptor**

Type	215	
Length	Variable.	
Value	Compound	
Description		
Elements	**TLV Name**	**M/O**
	Packet Data Flow ID	M
	Service Data Flow ID	O
	Service Profile ID	O
	Direction	O
	Activation Trigger	O
	Transport Type	O
	Uplink Qos ID	O
	Downlink Qos ID	O
	Uplink Classifier	O
	Downlink Classifier	O
Parent TLV	Ms Authorization Context	

2   **5.3.2.216 R3 Packet Data Flow ID**

Type	216
Length	2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid,
Description	Packet data flow ID
Parent TLV	Packet-Flow Descriptor

3   **5.3.2.217 R3 Service Data Flow ID**

Type	217
Length	2
Value	Unsigned Short representing the Service flow identifier (most significant bit first). This value is assigned by the home network and is unique per mobile session for the life of the session. A value of zero(0) is invalid.
Description	Service data flow ID

Parent TLV	Packet-Flow Descriptor

1 **5.3.2.218 R3 Service Profile ID**

Type	218
Length	4
Value	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.
Description	Service Profile ID
Parent TLV	Packet-Flow Descriptor

2 **5.3.2.219 R3 Direction**

Type	219
Length	1
Value	0 = Reserved 1 = Uplink 2 = Downlink 3 = Bi-directional 4 – FF = Reserved
Description	Direction
Parent TLV	Packet-Flow Descriptor

3

4 **5.3.2.220 R3 Activation Trigger**

Type	220
Length	1
Value	0x00 = Reserved 0x01 = Provisioned (SHALL be set in case of ISF) 0x02 = Admit (SHALL be set in case of ISF) 0x04 = Activate (SHALL be set in case of ISF) 0x08 = Dynamically Changeable (not valid for ISF) 0x1z to 0x8z = Reserved
Description	Activation Trigger
Parent TLV	Packet-Flow Descriptor

5 **5.3.2.221 R3 Transport Type**

Type	221
Length	1
Value	0 = Reserved 1 = IPv4-CS 2 = IPv6-CS 3 = Ethernet

	4 – 255 = Reserved
Description	Transport Type
Parent TLV	Packet-Flow Descriptor

1 **5.3.2.222 R3 Uplink QoS ID**

Type	222
Length	1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
Description	Uplink Qos ID
Parent TLV	Packet-Flow Descriptor

2 **5.3.2.223 R3 Downlink QoS ID**

Type	223
Length	1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
Description	Downlink Qos ID
Parent TLV	Packet-Flow Descriptor

3 **5.3.2.224 R3 Uplink Classifier**

Type	224
Length	Variable
Value	String containing an IP-Filter Rule as pre RFC3588. Action is set to "permit".
Description	Uplink Classifier
Parent TLV	Packet-Flow Descriptor

4 **5.3.2.225 R3 Downlink Classifier**

Type	225
Length	Variable
Value	String containing an IP-Filter Rule as pre RFC3588. Action is set to "permit".
Description	Downlink Classifier
Parent TLV	Packet-Flow Descriptor

5 **5.3.2.226 R3 QoS Descriptor**

Type	226	
Length	Variable.	
Value	Compound	
Description		
Elements	**TLV Name**	**M/O**

	R3 QoS ID	M
	Global Service Class Name	O
	Service Class Name	O
	R3 Schedule Type	M
	Traffic Priority/QoS Priority	O
	Maximum Sustained Traffic Rate	O
	Minimum Sustained Traffic Rate	O
	Maximum Traffic Burst	O
	Tolerated Jitter	O
	Maximum Latency	O
	Reduced Resource Code	O
	Media Flow Type	O
	Unsolicited Granted Interval	O
	SDU Size	O
	Unsolicited Polling Interval	O
Parent TLV	Ms Authorization Context	

1 **5.3.2.227 R3 QoS ID**

Type	227
Length	1
Value	Unsigned Octet representing an ID
Description	Qos ID
Parent TLV	Qos Descriptor

2 **5.3.2.228 Global Service Class Name**

Type	228
Length in octets	6
Value	Global Service Class Name as defined in IEEE802.16e.
Description	Provides an authorized QoS parameters set in a length optimized format.
Parent TLV(s)	▪ SF Info ▪ R3 QoS Descriptor
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Radio_Configuration_Update_Rpt*.

3 **5.3.2.229 Service Class Name**

Type	229
Length in octets	2 - 128

Value	Service Class Name as defined in IEEE802.16e
Description	ASCII string, which is known at the BS and which indirectly specifies a set of QoS Parameters.
Parent TLV	▪ SF Info ▪ R3 QoS Descriptor

1 **5.3.2.230 R3 Schedule Type**

Type	230
Length	1
Value	0 = Reserved 1 = Reserved 2 = Best Effort 3 = nrtPS 4 = rtPS 5 = Extended rtPS 6 = UGS 7 – 255 = Reserved
Description	Schedule Type
Parent TLV	Qos Descriptor

2 **5.3.2.231 Traffic Priority/QoS Priority**

Type	231
Length in octets	1
Value	0 to 7 = Higher numbers indicate higher priority. Default 0.
Description	The value of this parameter specifies the priority assigned to a service flow as it is defined for the Traffic Priority in IEEE802.16e [2]. Given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.
Parent TLV	• BE Data Delivery Service • UGS Data Delivery Service • NRT-VR Data Delivery Service • RT-VR Data Delivery Service • ERT-VR Data Delivery Service • R3 QoS Descriptor

3 **5.3.2.232 Maximum Sustained Traffic Rate**

Type	232
Length in octets	4
Value	32-bit integer representing rate (in bits per second).

Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Parent TLV	• ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • BE Data Delivery Service • R3 QoS Descriptor

1   **5.3.2.233 Minimum Reserved Traffic Rate**

Type	233
Length in octets	4
Value	32-bit unsigned integer representing rate (in bits per second).
Description	This parameter specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second and specifies the minimum amount of data to be transported on behalf of the service flow when averaged over time. The specified rate SHALL only be honored when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter SHALL be satisfied by assuring the available data is transmitted as soon as possible.
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • R3 QoS Descriptor

2   **5.3.2.234 Maximum Traffic Burst**

Type	234
Length in octets	4
Value	32-bit integer representing burst size (in bytes).
Description	This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Parent TLV	• ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • R3 QoS Descriptor

1 **5.3.2.235 Tolerated Jitter**

Type	235
Length in octets	4
Value	32-bit unsigned integer (in milliseconds).
Description	This parameter represents the maximum delay variation (jitter) (in milliseconds).
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • R3 QoS Descriptor

2 **5.3.2.236 R3 Maximum Latency**

Type	236
Length in octets	4
Value	32-bit integer specifies the maximum latency (in milliseconds)
Description	Time period between the reception of a packet by the BS or MS on its network interface and the delivering the packet to the RF Interface of the peer device. If defined, this parameter represents a service commitment (or admission criteria) at the BS or MS and SHALL be guaranteed by the BS or MS. A BS or MS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • RT-VR Data Delivery Service • R3 QoS Descriptor

3 **5.3.2.237 Reduced Resources Code**

Type	237
Length in octets	0
Value	Value = Null, see Description
Description	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available. (TBD: encoding)
Parent TLV	• QoS Info • R3 QoS Descriptor

4 **5.3.2.238 R3 Media Flow Type**

Type	238
Length in octets	1 + Variable

Value	The 1st octet is enumerator with the following values:
	• 0 = Reserved
	• 1 = Voice over IP
	• 2 = Robust Browser
	• 3 = Secure Browser/ VPN
	• 4 = Streaming video on demand
	• 5 = Streaming live TV
	• 6 = Music and Photo Download
	• 7 = Multi-player gaming
	• 8 = Location-based services
	• 9 = Text and Audio Books with Graphics
	• 10 = Video Conversation
	• 11 = Message
	• 12 = Control
	• 13 = Data
	• 14 – 254 = Reserved
	• 255 = Media Description in SDP format is included
	The 1st octet is always present in this TLV as an enumerator. Other fields presence and format depends on the code value set in the enumerator:
	If the 1st octet enumerator is set to indicate "Media Description in SDP format" (value 255), then variable-length SDP string is added:
	<SDP string> encoded as specified in IETF RFC 2327. The rules for information to be included – FFS. The rules for information to be included – FFS.
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Parent TLV	▪ QoS Info
	▪ R3 QoS Descriptor

5.3.2.239 Unsolicited Grant Interval

Type	239
Length in octets	2
Value	16-bit unsigned integer representing the grant interval (in milliseconds).
Description	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for a UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	• ERT-VR Data Delivery Service
	• UGS Data Delivery Service
	• R3 QoS Descriptor

5.3.2.240 R3 SDU Size

Type	240
Length in octets	1

Value	8-bit unsigned integer. Default = 49
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	• UGS Data Delivery Service • R3 QoS Descriptor

1 **5.3.2.241 R3 Unsolicited Polling Interval**

Type	241
Length in octets	2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Parent TLV	• RT-VR Data Delivery Service • R3 QoS Descriptor

2 **5.3.2.242 R3 Acct Interim Interval**

Type	242
Length	4
Value	32bits unsigned integer
Description	Acct-Interim-Interval
Parent TLV	Ms Authorization Context

3

4 **5.3.2.243 Accounting Mode Provisioning**

5 In order to support the "optional" accounting agent at the BS to communicate with the Accounting Client, there
6 needs to be messaging over the R6 interface. The following accounting session provisioning TLV is included in
7 existing messages to indicate the different accounting options as described in the Stage 2 specifications.

Type	243 (Accounting Mode Provisioning TLV)		
Length in octets	TBD		
Description	Optional accounting extensions that is designed to enable the Accounting Agent, if present, to communicate with the accounting client. The optional accounting mode provisioning TLV is included in existing messages to indicate the different accounting options as described in the stage-2 specifications.		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	Accounting Type	The Accounting Type is datafilled in the AAA server and sent to the accounting client in the Access_Accept message. This information is used to instruct the accounting agent at the Accounting Agent to track volume counts, if requested, and to what granularity to track them, e.g. IP session vs. service flow level.	M

	Interim Update Interval	The Interim Update Interval is datafilled in the AAA server and sent to the Accounting Client in the Access_Accept message. This TLV is only used for volume-based accounting.	O
	Accounting Number of ToDs	The number of Time of Day Tariff Switch TLVs.	O
	Time of Day Tariff Switch	The Time of Day Tariff Switch TLV is datafilled in the AAA server and sent to the ASN-GW in the Access_Accept message. There can be more than one of these sent.	O

1   **5.3.2.244 Accounting Session/Flow Volume Counts**

Type	244 (Accounting Session/Flow Volume Counts TLV)		
Length in octets	16		
Description	The counts represent session or flow depending on the Accounting Type that has been specified for the MS. The counts are sent by the Accounting Agent to the Accounting Client during Service Flow Deletion/Modification, HO, entering Idle Mode, de-registering from the network, and reporting bulk interim accounting. The counts are cumulative meaning that the counts are not reset on the Accounting Agent each time the TLV is sent. Also the counts are simply the counts collected at the Accounting Agent. The overflow of any of these counters is handled by the Accounting Client.		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	Cumulative Uplink Octets	Shall include this TLV if the value is > 0	M
	Cumulative Downlink Octets	Shall include this TLV if the value is > 0	M
	Uplink Octets at Tariff Switch		O
	Downlink Octets at Tariff Switch		O
	Cumulative Uplink Packets	Shall include this TLV if the value is > 0	M
	Cumulative Downlink Packets	Shall include this TLV if the value is > 0	M
	Uplink Packets at Tariff Switch		O
	Downlink Packets at Tariff Switch		O

2   **5.3.2.245 Accounting Number of Bulk Sessions/Flows**

Type	245
Length in octets	1
Value	The number of Accounting Bulk Session/Flow TLVs

3   **5.3.2.246 Accounting Bulk Session/Flow**

Type	246 (Accounting Bulk Session/Flow TLV)
Length in octets	TBD
Description	The IP session or service flow based volume count information is carried in this TLV .

Elements (Sub-TLVs)	TLV Name	Description	M/O
	MSID		O
	IP Address		M
	SFID		O
	Accounting Session/Flow Volume Counts		M

1 **5.3.2.247 Account Type**

Type	247
Length in octets	1
Value	1st nibble: • 0x0 = No Accounting • 0x1 = Volume-Based Accounting at the Service Flow level • 0x2 = Volume-Based Accounting at the IP session level • 0x3 = Duration-Based Accounting at the Service Flow level • 0x4 = Duration-Based Accounting at the IP session level • 0x5 = Volume-Based and Duration-Based Accounting at the Service Flow level • 0x6 = Volume-Based and Duration-Based Accounting at the 2nd nibble: IP session level • 0x0 = Postpaid Accounting • 0x1 = Prepaid Accounting and Postpaid Accounting

2 **5.3.2.248 Interim Update Interval**

Type	248
Length in octets	2
Value	Interval in seconds

3 **5.3.2.249 Cumulative Uplink Octets**

Type	249
Length in octets	4
Value	Cumulative uplink volume count in octets

4 **5.3.2.250 Cumulative Downlink Octets**

Type	250
Length in octets	4
Value	Cumulative downlink volume count in octets

5 **5.3.2.251 Cumulative Uplink Packets**

Type	251
Length in octets	4
Value	Cumulative uplink volume count in packets

1   **5.3.2.252 Cumulative Downlink Packets**

Type	252
Length in octets	4
Value	Cumulative downlink volume count in packets

2

3   **5.3.2.253 Time of Day Tariff Switch**

Type	253	
Length in octets		
Elements (Sub-TLVs)	**TLV Name**	**M/O Flag**
	1. Time of Day Tariff Switch Time	M
	2. Time of Day Tariff Switch Offset	M

4   **5.3.2.254 Time of Day Tariff Switch Time**

Type	254
Length in octets	2
Value	The time of day time in hours and minutes Octet 1: Hour (0-23) Octet 2: Minute (0-59)

5   **5.3.2.255 Time of Day Tariff Switch Offset**

Type	255
Length in octets	4
Value	The time of day timezone offset Octet 1-4: Offset (+/- seconds from UTC)

6   **5.3.2.256 Accounting Number of ToDs**

Type	256
Length in octets	1
Value	UINT8 (0 .. 255)

7   **5.3.2.257 Uplink Octets at Tariff Switch**

Type	257
Length in octets	4
Value	UINT32 (0 .. 4294967295)

8

9   **5.3.2.258 Downlink Octets at Tariff Switch**

Type	258
Length in octets	4
Value	UINT32 (0 .. 4294967295)

1

5.3.2.259 Uplink Packets at Tariff Switch

Type	259
Length in octets	4
Value	UINT32 (0 .. 4294967295)

3

5.3.2.260 Downlink Packets at Tariff Switch

Type	260
Length in octets	4
Value	UINT32 (0 .. 4294967295)

5

5.3.2.261 Vendor Specific TLV

Vendor Specific TLV is an optional TLV. When TLV type indicates Vendor Specific TLV, but the Vendor ID is not recognized, then processing SHALL silently discard the TLV and continue processing the rest of the message.

The value field of the TLV contains the Vendor Identification (Vendor ID) specified by the 24-bit vendor-specific Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider.

Vendor Specific TLV Encoding Description

Table 5-2 – Vendor Specific TLV Information Element

IE	Type	Descriptions	M/O	Notes
Vendor Specific TLV	261	Vendor defined TLV	O	Support for R8, R4 and R6 Reference points

The content and format of the TLV is as follows:

Type	0xFFFF (65535)
Length in Octets	Variable
Value	Vendor Specific I information Field (VSIF)
Message Primitives That Use This TLV	Every message

The format of the Vendor Specific Information Field (VSIF) is as follows:

- First 24 bits – Vendor ID (mandatory)

- Rest of info in TLV (optional) – vendor-specific, out of scope for standard definition

The Vendor ID field SHALL be the first field of VSIF.

Vendor Specific TLV MAY be nested inside another TLV.

Multiple Vendor Specific TLVs can be inserted into one message across R6 or R4.

1 **Notes**

2 Note 1: One or more SF Info TLVs MAY be included in order to describe Service Flows in Data Path Control,
3 Reservation, and HO Control Messages. In Data Path Control SF Info is included in the case of Per-SF data
4 path tunneling granularity.

5 Note 2: In the case of Per-SF data path tunneling granularity, DP Info SHALL be included as sub-TLV of SF Info

6 Note 3: Anchor GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content is IP
7 address (v4 or v6).

8 It does not have to be included if AK Context is included. If neither Authenticator ID nor AK Context is
9 included means that the sender of the *HO_Req* hosts the Authenticator Function for the MS.

10 Anchor GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content is IP
11 address (v4 or v6).

12 ## 5.4   RADIUS Messages and Attributes

13 The section lists the standard attributes that are used across RADIUS-based WiMAX reference points, and all VSAs
14 (vendor-specific attributes) that are defined for WiMAX network operation as describe by this specification.

15

16 ### 5.4.1   RADIUS Messages

17 #### 5.4.1.1   Network Access Authentication between NAS and HAAA

18 The RADIUS attributes defined in the following tables, comprise:

19 • attributes used for EAP-based network access that are exchanged between the ASN and the HAAA in the
20 CSN.

21 • additional attributes for bootstrapping mobility service that are exchanged between ASN and the CSN
22 HAAA

23 • RADIUS attributes between ASN and HAAA for DHCP relay

24 **RADIUS Attribute Tables**

25 **Table 5-3 – RADIUS Messages between NAS and HAAA**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
User-Name	1	NAI obtained from the EAP-Response Identity (Outer-NAI)	1	0	0-1	0
Service-Type	6	Set to "Framed" for initial authentication and set to "Authenticate-Only" indicating Re-authentication. It MAY also be set to "Authorize-Only" when using to obtain prepaid quotas mid-session.	1	0	0-1	0
Framed-MTU	12	As used by WiMAX, as per [8] in an Access-	0-1[m]	0	0-1[m]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		Request during EAP authentication, this attribute provides the appropriate MTU size to avoid exceeding maximum payload size for PKMv2 (2008 bytes) during EAP exchange (the appropriate fragmentation is assumed in Authentication Server on the EAP application layer). The value of this attribute should be set between 1020 and 2000 bytes (the recommended value is 1400 bytes)." In an Access-Accept the use is as per [27].				
EAP-Message	79	The EAP exchanged transported over RADIUS.	1-n	1-n	1-n	1-n
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [8]	1	1	1	1
WiMAX-Capability	26/1	Identifies the WiMAX Capabilities supported by the NAS. Indicates capabilities selected by the RADIUS server.	1	0	0-1[k]	0
NAS-Identifier	32	This attribute contains a string identifying the NAS or HA origination the Access-Request. The format SHALL be the fully qualified domain name of the NAS.	1[b]	0	0	0
NAS-Port-Type	61	Identifies the type of port the request is associated with. Set to 27 for "Wireless – IEEE 802.16" when coming from a WiMAX ASN.	1	0	0	0
Calling-Station-Id	31	Set to the MAC address in binary format of the Device	1	0	0	0
Device-	26/2	Indicates whether the	0-1[i]	0	0	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Authentication-Indicator		Device authentication was performed and the result.				
CUI	89	Indication for support and desire to have the HAAA provide Chargeable User Identity. The NAS commits to include the CUI in all RADIUS Accounting packets.	0-1	0	0-1[a][k]	0
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS.	1	0	0	0
NAS-IP-Address	4	NAS IP Address.	0-1[b]	0	0	0
NAS-IPv6-Address	95	NAS-IPv6 address.	0-1[b]	0	0	0
Error-Cause	101	Error Codes generated during access authentication [28]	0	0-1	0	0-1
Class	25	Opaque value set by the Server used to bind authentication to accounting.	0	0	0-1[h][k]	0
Framed-IP-Address	8	The CMIP4 Home Address to be assigned to the MN.	0	0	0-1[c][k]	0
Session-Timeout	27	The maximum number of seconds of service to be provided to the user before termination of the session. Associated with the lifetime of the keys derived from the EAP authentication (ie MSK, EMSK and keys derived from EMSK) Session-Timeout in an Access-Challenge packet is used set the EAP-retransmission timer as per [8].	0	0-1	0-1[d][k]	0
Termination-Action	29	Indicates what action the NAS should take when service is completed.	0	0	0-1[d][k]	0
AAA-Session-ID	26/4	A unique identifier in the home realm for this	0-1[e]	0-1	1	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		Session as set by the HAAA.				
MSK	26/5	The Master Session Key derived as the result of successful EAP Authentication.	0	0	0-1[f]	0
Packet-Flow-Descriptor	26/28	The pre-provisioned Service Flows	0	0	0-n[k]	0
QoS-Descriptor	26/29	The QoS descriptor for the pre-provisioned flows	0	0	0-n[j][k]	0
BS-ID	26/46	Indicates the NAP-ID and BS-ID at the time the message was delivered	0-1[n]	0	0	0
NAP-ID	26/45	Indicated the operator id of the NAP at the time the message was delivered	0-1[n]	0	0	0
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1[k]	0
NSP-ID	26/57	The Operator ID of the NSP	0-1[p]	0	0	0

1 **Notes:**

[a] CUI SHALL appear if it was present in the Access-Request packet.

[b] NAS-ID SHALL appear in the Access-Request. One of NAS-IP-Address or NAS-IPv6 address MAY also appear.

[c] If this attribute is present then the Home Address assigned to the mobile SHALL be as specified by this attributes. If this attribute is absent then the Home Address is derived from MIP procedures or other means (E.g. DHCP).

[d] Except during the NAP authentication (first EAP authentication of Double EAP), both Session-Timeout and Termination-Action SHALL be present. Termination-Action SHALL be set to "RADIUS-Request"(1). This causes the NAS to re-authenticate when the Session-Timeout expires.

[e] SHALL not be included in the initial Access-Request message. SHALL be included in all subsequent Access-Requests message for this session if known by the NAS – for example during online accounting procedures

[f] The attribute SHALL be encrypted using the procedures in section 3.5 of [35]. MSK may be transmitted using MS_MPPE_Send_Key and MS_MPPE_Recv_Key as per [47] in which case MSK SHALL NOT appear in the Access-Accept packet.

[g] Intentionally not used.

[h] If more then one Class attribute is found in an Access-Accept message, the NAS SHALL only store the first one and discard the rest.

[i] SHALL appear in the Access-Request associated with the User Authentication phase of the Double EAP Device/User authentication procedure. Otherwise, the attribute SHALL not be present in the Access-Request message.

[j] Conditional mandatory: see requirements for Packet Flow Descriptor.

[k] Attributes SHALL NOT appear in the Access Accept sent associated with the Device Authentication phase of Double EAP.

[m] If the Framed MTU appears in an Access-Request during Access-Authentication then it indicates the MTU on the link between the NAS and the MS. As per [8] the RADIUS SHALL NOT send any subsequent packet in this EAP conversation containing EAP-Message attributes whose values, when concatenated, exceed the length specified by the Framed-MTU value.

[n] Either the BS-ID or NAP-ID SHALL be provided. If both are provided the receiver SHALL ignore the NAP-ID attribute.

[p] SHALL be present when the Access-Request packet arrives at the HAAA. Either the NAS (if it knows it) or the VCSN SHALL insert this attribute in the Access-Request packet.

1 Table 5-4 and Table 5-5 are the Mobility attributes exchanged between the ASN and the HAAA during the Network
2 Access Authentication.

3 **Table 5-4 – RADIUS Messages between ASN and HAAA for Bootstrapping Mobility Service**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
HA-IP-MIP4	26/6	IPv4 address of the HA. To be used by the PMIP4 client	0-1[a1]	0	1[a3]	0
HA-IP-MIP6	26/7	IPv6 of the HA to be used for CMIP6	0-1[a1]	0	1[a3]	0
MN-HA-MIP4-KEY	26/10	The MN-HA key used for Proxy MIP4 procedures.	0	0	1 [a3]	0
MN-HA-MIP6-KEY	26/12	Reserved for future release. The MN-HA key used for Proxy MIP6.	0	0	0-1 [a3][a4]	0
MN-HA-MIP4-SPI	26/11	The SPI associated with the MN-HA-MIP4-KEY.	0	0	1 [a3][a5]	0
MN-HA-MIP6-SPI	26/13	Reserved for future release. The SPI associated with the MN-HA-MIP6-KEY.	0	0	0-1 [a3][a4] [a5]	0
FA-RK-KEY	26/14	The FA-RK used to derive MN-FA for MIP4 operations.	0	0	1[a3]	0
FA-RK-SPI	26/?	The SPI associated with the FA-RK	0	0	1[a3]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
HA-RK-KEY	26/15	HA-RK key used to generate FA-HA keys for CMIP4 operations.	0	0	0-1 [a2][a3]	0
HA-RK-SPI	26/16	The SPI associated with the HA-RK.	0	0	0-1 [a2][a3][a6]	0
HA-RK-Lifetime	26/17	HA-RK key used to generate FA-HA keys for CMIP4 operations.	0	0	0-1[a2][a3][a6]	0

1 **Notes:**

[a1] The VCSN MAY include the HA-IP to indicate that it is capable of assigning an HA for the session and the IP address of the proposed HA

[a2] If the Home AAA does not include these attributes, then the proxy AAA responsible for the HA SHALL provide these attributes..

[a3] In case of Double EAP, these attributes SHALL NOT appear in the Access-Accept associated with the Device Authentication phase of Double EAP.

[a4] Reserved for future release. These attributes SHOULD only appear if the MS is allowed to perform PMIP6.

[a5] MN-HA-MIP4-SPI SHALL be present if MN-HA-MIP4-KEY is present. MN-HA-MIP6-SPI SHALL be present if MN-HA-MIP6-KEY is present.

[a6] The HA-RK-SPI and HA-RK-Lifetime SHALL be present when the HA-RK is present. If they are not present the receiver SHALL ignore the HA-RK attribute.

2 **Table 5-5 – RADIUS Attributes between ASN and HAAA for DHCP Relay**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
DHCPv4-Server	26/8	The IPv4address of the DHCP server to be used for Proxy Mobile IPv4.	0-1 [a1]	0	0-1 [a2][a3]	0
DHCPv6-Server	26/9	The IPv4/IPv6 address of the DHCP-Server to be used for Proxy Mobile IPv6.	0-1[a1]	0	0-1[a3]	0
DHCP-RK	26/40	DHCP-RK key used to derive keys to protect DHCP signaling between the DHCP proxy and the DHCP server.	0	0	0-1 [a2][a3]	0
DHCP-RK-Key-ID	26/41	Key identifier associated with the DHCP-RK, as per [31]	0	0	0-1 [a3][a4]	0
DHCP-RK-Lifetime	26/42	Lifetime of the DHCP-RK	0	0	0-1 [a3][a4]	0

DNS	26/52	The IPv4/IPv6 address of the DHCP server to be used by the DHCP relay.	0	0	0-n[a5]	0

1 **Notes:**

[a1]   The VCSN MAY include the DHCP-Server-IPv4 to indicate that it is capable of assigning an DHCP server for the session. If the VCSN includes DHCP-Server-IPv4 then it SHALL also include the HA-IP-MIP4 attribute.

[a2]   If the Home AAA does not include these attributes, then the proxy AAA responsible for the HA assignment MAY provide this attributes.

[a3]   In case of Double EAP, these attributes SHALL NOT appear in the Access-Accept associated with the Device Authentication phase of Double EAP.

[a4]   The DHCP-RK-Key-ID and DHCP-RK-Lifetime SHALL be present when the DHCP-RK attribute is present. These attributes are provided by the same AAA server that provided the DHCP-RK attribute. If they are not present the receiver SHALL ignore the DHCP-RK attribute.

[a5]   If more then one DNS server IP address are given, then the first one is the primary and the others are secondary servers.

2   **5.4.1.2   RADIUS Messages for MIP between HA and HAAA**

3   The RADIUS attributes exchanged between the HA and HAAA. The HA always sends RADIUS messages to a
4   AAA server that is located in the same CSN as the HA itself, in order to communicate with the HAAA server.

5   **Table 5-6 – RADIUS Messages between HA and HAAA**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
User-Name	1	NAI extension received in the MIP Registration Request or BU.	1	0	0	0
NAS-IP-Address	4	The IP Address of the HA's interface to the AAA server.	0-1[b]	0	0	0
NAS-IPv6-Address	95	The IPv6 Address of the HA's interface to the AAA server.	0-1[b]	0	0	0
NAS-Identifier	32	The FQDN of the HA's interface as seen by the AAA server.	1[b]	0	0	0
NAS-Port-Type	61	The absence of the NAS-Port-Type and presence of the MIP attributes indicates that the message is coming from an HA.	0	0	0	0
Message-Authenticator	80	Message Authenticator to integrity protect the AAA message	1	0	1	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Class	25	Opaque value set by the Server used to bind authentication to accounting.	0-1	0	0	0
WiMAX Capability	26/1	Identifies the WiMAX Capabilities supported by the HA. Indicates capabilities selected by the RADIUS server.	1	0	0-1	0
CUI	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1[c]	0	0-1[c]	0
AAA-Session-ID	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	0-1[d]	0	1[d]	0
HA-IP-MIP4	26/6	The IP address of the HA making this request	0-1[f]	0	0	0
HA-IP-MIP6	26/7	The IP address of the HA making this request	0-1[f]	0	0	0
RRQ-HA-IP	26/18	The HA-IP address contained in the Registration Request or Binding Update.	0-1[a]	0	0	0
MN-HA-MIP4-KEY	26/10	The MN-HA key used for MIP4 procedures.	0	0	1[g]	0
MN-HA-MIP6-KEY	26/12	The MN-HA key used for MIP6 procedures.	0	0	0-1 g]	0
MN-HA-MIP4-SPI	26/11	The SPI associated with the MN-HA-MIP4-KEY.	1	0	1	0
MN-HA-MIP6-SPI	26/13	The SPI associated with the MN-HA-MIP6-KEY.	0	0	0-1	0
RRQ-MN-HA-KEY	26/19	The MN-HA-KEY that is bound to the HA-IP address as reported by RRQ-HA-IP attribute.	0	0	0-1[a]	
HA-RK-KEY	26/15	HA-RK key used to generate FA-HA keys.	0	0	0-1[h]	0
HA-RK-SPI	26/16	The SPI associated with the HA-RK.	0-1	0	0-1[h]	0
HA-RK-	26/17	HA-RK key used to generate FA-HA keys for	0	0	0-1[h]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Lifetime		MIP4 operations.				
Framed-IP-Address	8	The Home Address extracted from the MIP messages or sent to the HA from the HAAA.	0-1	0	0-1	0
Framed-IPv6-Prefix	97	The HOA extracted from the BU MIP message or sent to the HA from the HAAA.	0-1[i]	0	0-1	0
BU-CoA-Ipv6	26/51	The IPv6 address extracted from the Care-of Address field in the BU.	0-1[i]	0	0	0
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1	0
HA-RK-Key-Requested	26/58	A flag indicating (value=1) that the HA needs the HA-RK key.	0-1[k]	0	0	0

1 **Notes:**

[a] SHALL be included if the HA-IP address in the MIP RRQ is different then the IP address of the HA. The RRQ-MN-HA SHALL be present in the Access-Accept packet if the RRQ-HA-IP address is present in the Access-Request packet.

[b] NAS-Identifier is required. Either NAS-IP or NAS-IPv6 MAY also be provided.

[c] CUI may be present in the Access-Request. CUI may be present in the Access-Accept. CUI SHALL be present in the Access-Accept if it was present in the Access-Request.

[d] AAA session ID SHALL NOT appear in the initial Access-Request for this mobile. It SHALL appear in all subsequent Access-Request if the HA knows the AAA-Session-ID

[e] In Access-Accept the MN-HA-SPI SHALL be present if it is different then the MN-HA-SPI received in the Access-Request

[f] Either HA-IP-MIP4 or HA-IP-MIP6 SHALL be present in an Access-Request.

[g] Either MN-HA-MIP4-KEY or MN-HA-MIP6-KEY SHALL be present in an Access-Accept

[h] MAY be present in an Access-Accept message. However, when present, all of the attributes SHALL be present otherwise the receiver SHALL silently discard the Access-Accept.

[i] SHALL be present if this is associated with MIP6 procedures.

[j] SHALL be present and should be set to 1 if the HA need HA-RK-Key.

2 **5.4.1.3   RADIUS Messages between DHCP and HAAA**

3 Table 5-7 defines the RADIUS messages that are exchanged between a DHCP server and the HAAA..

1   **Table 5-7 – RADIUS Messages between DHCP server and HAAA**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Message-Authenticator	80	Message Authenticator to integrity protect the AAA message	1	0	1	0
NAS Identifier	32	The FQDN of the DHCP server originating the request.	1	0	0	0
NAS-IP-Address	4	The IP address of the DHCP server making this request	0-1[b]	0	0	0
NAS-IPv6-Address	95	The IPv6 address of the DHCP server making this request.	0-1[b]	0	0	0
NAS-Port-Type	61	The absence of the NAS-Port-Type and the DHCP attributes indicate that this message comes from a DHCP Server	0	0	0	0
DHCPMSG-Server – IPv4	26/43	The DHCP server address contained in the DHCPDISCOVER message	0-1[a]	0	0	0
DHCP-RK-Key-ID	26/41	The key ID as received in the DHCPDISCOVER message	1	0	1	0
DHCP-RK	26/40	DHCP-RK key used to derive keys to protect DHCP signaling	0	0	1	0
DHCP-RK-Lifetime	26/42	Lifetime of the DHCP-RK	0	0	1	0

2   **Notes:**

[a]   This attribute is set to the IPv4 address to which the DHCPDISCOVER message was sent. It SHALL be included if the DHCP server address in the DHCPDISCOVER message is different then the address contained in the DHCP-Server-IPv4 attribute.

[b]   Either NAS-IP-Address or NAS-IPv6-Address MAY also be provided.

1 ## 5.4.1.4   RADIUS Message for Hotlining

2 Table 5-8 describes the RADIUS attributes sent from the HAAA to the Hotline Device (NAS or the HA).

3 **Table 5-8 – RADIUS Access-Accept (from HAAA to HLD)**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Hotline-Profile-ID	26/53	ID to uniquely identify the user's hotline profile	0	0	0-1[a][c]	0
HTTP-Redirection-Rule	26/54	Instructs the Hot-Lining Device where to redirect HTTP flows	0	0	0-n[a][c]	0
IP-Redirection-Rule	26/55	Used to specify which packet flow to redirect and where to redirect it	0	0	0-n[a][c]	0
NAS-Filter-Rule	TBD	As defined by RFC TBD	0	0	0-n[a][c]	0
Hotline-Session-Timer	26/56	Specifies the length of time in seconds that the user would be allowed to remain in the hotline session.	0	0	0-1	0
Hotline-Indication	26/24	Indicates that the flow is hotlined	0	0	0-1[b]	0

4 **Notes:**

[a]   If Hotline-Profile-ID is included HTTP-Redirection-Rule and IP-Redirection-Rule and Filter-Rule SHALL not be included. In the case where these are present, the receiver SHALL silently discard the attributes.

[b]   If the session is to be hotlined then this attribute SHALL be specified and the NAS SHALL include this attribute in the accounting messages.

[c]   When these attributes are specified Filter-ID(11) as defined by [27] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded

5 Table 5-9 lists the RADIUS attributes that appear in a COA message used to hotline the MS mid-session. The
6 procedures for sending COA messages as described in [28] are supported with the additional information as
7 specified by this table.

8 **Table 5-9 – RADIUS COA (from HAAA to HLD)**

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
User-Name	1	The NAI of the MS as received during Access-Authentication.	1	0	0
Calling-Station-Id	31	The MAC address in binary format of the MS.	1	0	0

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
AAA-Session-ID	26/4	The NAI contained in the User-Name and the AAA-Session-ID forms a unique identifier of the session at the NAS.	1	0	0
Hotline-Profile-ID	26/53	ID to uniquely identify the user's profile	0-1[a][c]	0	0
HTTP-Redirection-Rule	26/54	Instructs the Hot-Lining Device where to redirect HTTP flows	0-n[a][c]	0	0
IP-Redirection-Rule	26/55	Used to specify which packet flow to redirect and where to redirect it	0-n[a][c]	0	0
NAS-Filter-Rule	26/TBD		0-n[a][c]	0	0
Hotline Session Timer	26/56	Contains the length of time in seconds that the user would be allowed to remain in the hotline session.	0-1	0	0
Hotline-Indication	26/24	Indicates that the flow is hotlined.	0-1[b]	0	0

1 **Notes:**

[a]   If Hotline-Profile-ID is included HTTP-Redirection-Rule and IP-Redirection-Rule and Filter-Rule SHALL not be included. In the case where these are present, the receiver SHALL silently discard the attributes.

[b]   The IP address of the MS if known by the HAAA SHOULD be included.

[c]   When these attributes are specified Filter-ID(11) as defined by [27] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded.

1 **5.4.1.5   Messages for Online-Accounting**

2 Online-Accounting message happen during Network Access Authentication and mid-session to update quotas. The
3 following table lists the additional attributes used when online-accounting is used with the NAS and the HA.

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
PPAC	26/35	Prepaid Accounting Capability attribute. Used by the NAS to indicate support for prepaid features.	0-1[a]	0	0	0
Session Termination Capabilities	26/36	Indicates support by the NAS for termination.	0-1[b]	0	0	0
PPAQ	26/37	Prepaid Quota attribute.	0-n[c][e]	0	0-n[d][e]	0
Prepaid Tariff Switching	26/38	Prepaid Tariff Switching attribute.	0-n[e]	0	0-n[e]	0
Event-Timestamp	55	Indicates the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC	0-1[f]	0	0	0

4 **Notes:**

[a]   SHALL be included in an Access-Request if the NAS (ASN or HA) has support for prepaid capabilities. If
     included the NAS SHALL support the prepaid operations it has advertised in this attribute.

[b]   SHALL be included in an Access-Request if the NAS (ASN or HA) has support for session termination
     capabilities. If included the NAS SHALL support the session termination capabilities it has advertised in this
     attribute.

[c]   Available to be used in Access Request and Authorize-Only Access-Request (Service-Type =
     "AUTHORIZE-ONLY").

[d]   Available to be used in Access-Accept. If the NAS advertises support for prepaid the NAS SHALL process
     this attribute. If the NAS cannot process this attribute it SHALL treat the Access-Accept as an Access-Reject
     packet.

[e]   If a RADIUS message contains a Prepaid Tariff Switching attribute it SHALL also contain at least one PPAQ
     attribute.

[f]   If a RADIUS Access-Request message contains a PTS attribute or the PPAC "Tariff Switching supported"
     flag is set, it SHALL also contain an Event-Timestamp RADIUS attribute (see [9]).

5 **5.4.1.6   Offline Accounting**

6 **5.4.1.6.1   Status and Type**

Name	Type	Description	Start	Int	Stop
Acct-Status-Type	40	Indicates the record type: Start, Stop, Interim	1	1	1
Acct-Terminate-Cause	49	Indicates why the session stopped.	0	0	0-1[1]

Name	Type	Description	Start	Int	Stop
Session-Continue	26/21	True indicates that the stop is immediately followed by a start. If the attribute is missing or FALSE it means that this is the final stop.	0	0	0-1[5]
Beginning of Session	26/22	True: a new flow is starting. False or missing, this is a continuation of a previous flow.	0-1[5]	0	0
IP technology	26/23	Proxy CMIP4, CMIP4	0-1[5]	0-1[5]	0-1[5]
Hotline-Indicator	26/24	Indicates that the flow is hotlined	0-1[4]	0-1[4]	0-1[4]
Prepaid-Indicator	26/25	Indicates that the flow is being prepaid	0-1	0-1	0-1
Class	25	SHALL be inserted by the accounting client if received in Access-Accept.	0-1[2]	0-1[2]	0-1[2]
Idle-Mode-Transition	26/44	Indicates idle mode entry (1) or exit (0)	0	0-1[3,5]	0
Count-Type	26/58	Used to indicate if the record represents compressed counts over-the-air. • 0x00 = Uncompressed counts • 0x01 = Compressed counts	0	1	1

Notes:

[1]   Only included in Stop record when the session has terminated.

[2]   Class SHALL be included if received in RADIUS Access-Accept.

[3]   Only included when supported by the NAS and Idle Mode Notification has been requested by the HAAA. Never appears in messages from the HA.

[4]   If the session is hotlined, and the NAS received this in an Access-Accept or a COA message, then the NAS SHALL include this attribute as received in the Accounting messages.

[5]   SHALL NOT be included if accounting is from an HA.

5.4.1.6.2 Record Correlators

Name	Type	Description	Start	Int	Stop
Acct-Session-Id	44	Used to match Starts, Stop, and Interim. It is generated by the accounting client and is unique per start/stop pair.	1	1	1
Acct-Multi-Session-Id	50	This identifier is set to the value of AAA-Session-Id which is generated by AAA after successful authentication and delivered to the NAS in an Access-Accept message. It is unique per CSN and is used to match all accounting records within a session.	1	1	1
PDFID	26/26	This value matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios.	0-1 [1,4]	0-1 [1,4]	0-1 [1,4]
SDFID	26/27	This value matches all packet data flows from the	0-1	0-1	0-1

Name	Type	Description	Start	Int	Stop
		same service data flow.	[2,4]	[2,4]	[2,4]
Framed-IP-Address	8	The IPv4 address assigned to the MS. This identifies the IP-Session	0-1[3]	0-1[3]	0-1[3]
Framed-IPv6-Prefix	97	The IPv6 prefix assigned to the MS. This identifies the IP Session.	0-1[3]	0-1[3]	0-1[3]

Notes:

[1] SHALL be included when flow based accounting is being performed. SHALL not be included when Session-based accounting.

[2] SHALL not be included when session based accounting. Included if available when flow-based accounting is used.

[3] Either Framed-IP or Framed-IPv6 SHALL be present in Accounting messages. If both are present then the HAAA SHALL discard the Accounting message.

[4] SHALL NOT be included with messages coming from an HA.

5.4.1.6.3 User Identification

Name	Type	Description	Start	Int	Stop
User-Name	1	The identity and realm of the user used in the outer NAI during network access authentication and authorization	1	1	1
CUI	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1[1]	0-1[1]	0-1[1]
Calling-Station-Id	31	The MAC address in binary format of the MS	0-1[2]	0-1[2]	0-1[2]

Notes:

[1] SHALL be included if received in an RADIUS Access-Accept packet.

[2] SHALL be included from messages coming from a NAS. SHALL NOT be included from messaged coming from an HA

5.4.1.6.4 Infrastructure Identifiers

Name	Type	Description	Start	Int	Stop
NAS-ID	32	The identifiers of the NAS generating this record.	0-1[1]	0-1[1]	0-1[1]
HA-IP-MIP4	26/6	The IP address of the home agent.	1	1	1
HA-IP-MIP6	26/7	The IP address of the home agent.	1	1	1
NAS-IP-Address	4	The IPv4 address of the serving NAS.	0-1[1]	0-1[1]	0-1[1]
NAS-IPv6-Address	95	The IPv6 address of the serving NAS	0-1[1]	0-1[1]	0-1[1]
NAP-ID	26/45	An octet string that uniquely identifies the operator that generated this UDR. This value is configured at the Accounting Client and can be used for charging settlement between NSP and NAP.	0-1[2]	0-1[2]	0-1[2]

Name	Type	Description	Start	Int	Stop
BS-ID	26/46	An octet string that uniquely identifies the NAP-ID Base Station that is serving the MS at the time the UDR is generated.	0-1[2]	0-1[2]	0-1[2]
Location	TBD	TBD (Geopriv has an attribute for this)	0-1	0-1	0-1
NSP-ID	26/57	The operator ID idneitfying the NSP operator.	0-1[3]	0-1[3]	0-1[3]

1 **Notes:**

[1] At least NAS-ID or one of NAS-IP-Address or NAS-IPv6-Address SHALL appear in the Accounting packet.

[2] At least NAP-ID or BS-ID SHALL appear in the Accounting packet. If both appear then the receiver SHALL ignore the NAP-ID attribute. These attribute SHALL not be inserted by an HA generating accounting messages.

[3] This attribute SHALL be in the accounting packets (start,interim,stop) when they reach the HAAA. Either the NAS, or the VCSN, SHALL insert this attribute into the accounting stream. If the HA is located in the VCSN and the HA is generating accounting messages, then the HA SHALL insert this attribute into the accounting stream. Otherwise, the HA SHALL NOT insert this attribute into the accounting stream.

2 **5.4.1.6.5 Time**

Name	Type	Description	Start	Int	Stop
Acct-Session-Time	46	The number of seconds the flow or session was active.	0	0-1	0-1
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS or HA.	0-1	0-1	0-1
Event-Timestamp	55	The time the event occurred.	1	1	1
Active-Time	26/39	The time in which the MS is active as opposed to idle mode.	0	0-1[1]	0-1[1]

3 **Notes:**

[1] SHALL NOT be reported by a HA.

4 **5.4.1.6.6 L3 Counters**

Name	Type	Description	Start	Int	Stop
Acct-Input-Octets	42	The total number of octets in IP packets sent to the user, as received at the accounting agent from the IP network (i.e. prior to any compression and/or fragmentation).	0	0-1	0-1
Acct-Output-Octets	43	The total number of octets in IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1	0-1
Acct-Input-Packets	47	The total number of IP packets sent to the user, as received at the accounting agent from the IP network (i.e. prior to any compression and/or fragmentation).	0	0-1	0-1

Name	Type	Description	Start	Int	Stop
Acct-Output-Packets	48	The total number of IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1	0-1
Acct-Input-Gigawords	52	Incremented when attribute 42 overflows	0	0-1	0-1
Acct-Output-Gigawords	53	Incremented when attribute 43 overflows	0	0-1	0-1
Control-Packets-In	26/31	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.	0	0-1	0-1
Acct-Input-Packets-Gigaword	26/48	Incremented when attribute 47 overflows	0	0-1	0-1
Acct-Output-Packets-Gigaword	26/49	Incremented when attribute 48 overflows	0	0-1	0-1
Control Octets In	26/32	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Control Packets Out	26/33	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Control Octets Out	26/34	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]

Notes:

[1]   SHALL NOT be reported by a HA.

5.4.1.6.7 Flow Specification

Name	Type	Description	Start	Int	Stop
Flow-Description	26/50	IPFilter Rule that describes a PD flow with the header fields.	0	0-1[1]	0-1[1]

Notes:

[1]   Attribute SHALL not appear when Session-based accounting is performed.

The MS's IP address (HoA) SHALL be included as either in the source address or destination address depending on the PD flow direction.

The IP address of the correspondent node may be included.

The port number for each end may be included. The protocol field may be included.

If a specific field in the IPFilterRule is wild-carded, that field is not used while matching a PD flow against the IPFilterRule.

SHALL NOT be reported by a HA.

5.4.1.6.8 Granted-QoS

Name	Type	Description	Start	Int	Stop
Granted-QoS	26/30	Not handled in Release 1.0.0.	0	0-1[1]	0-1[1]

1   **Notes:**

[1]   Attribute SHALL NOT appear when Session-based accounting is performed or from an HA.

2   **5.4.1.7   RADIUS Disconnect Request Message**

3   Disconnect Request message should be defined as per [28] with the following:

Attribute	TYPE	Description	DR	DR-ACK	DR-NAK
User-Name	1	The NAI of the MS as received during Access-Authentication.	1	0	0
Calling-Station-Id	31	The MAC address in binary format of the MS	1	0	0
AAA-Session-ID	26/4	The NAI contained in the User-Name and the AAA-Session-ID forms a unique identifier of the session at the NAS	1	0	0

4   RADIUS Disconnect-ACK message is sent without any additional parameters

5   **5.4.1.7.1 RADIUS Disconnect NACK Message**

6   **Table 5-10 – RADIUS Disconnect NACK Message**

Attribute	ID	AR	Description	Source
Error-Cause	101	1		

7

8   **5.4.2   WIMAX RADIUS VSAs Definitions**

9   WiMAX RADIUS VSAs are transported in a RADIUS Vendor Specific Attribute.

10   The following describes the general format of WiMAX VSAs.

```
11     0                   1                   2                   3
12     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
13    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
14    | RADIUS TYPE 26| Length        |            Vendor-Id
15    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16    |     Vendor-Id (cont)          |            String
17    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
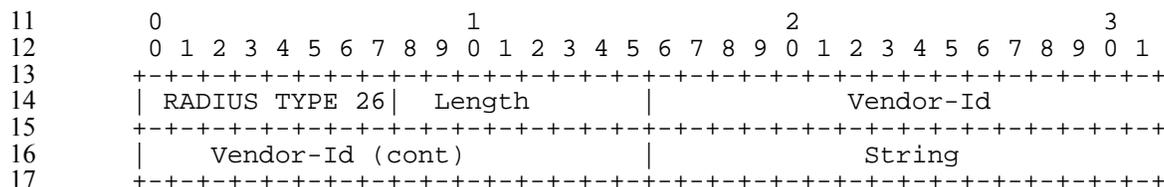
Type	26 for Vendor-Specific.
Length	Length of the entire structure which is given by: The length of the Header (=6) plus the length of the WiMAX Vendor Attribute.
Vendor-Id	The SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the "Assigned Numbers" [6]. The Vendor-Id for WiMAX is 24757
String	Contains one WiMAX Vendor attribute which is formatted as specified below.

```
1      0                   1                   2                   3
2      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
3     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
4     |   WiMAX Type  |   Length      |  Continuation |    Value
5     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WiMAX Type	0 is reserved.
	1-254 WiMAX Types as defined below.
	255 is reserved.
Length	>= 3. Length of the WiMAX attribute including the WiMAX Type, length, Continuation and Value field.
Continuation	The Continuation Field is defined as follows:
	``` 0 0 1 2 3 4 5 6 7 +-+-+-+-+-+-+-+-+ |C|r|r|r|r|r|r|r| +-+-+-+-+-+-+-+-+ ```
	The C-bit of the continuation field indicates if a WiMAX attribute is being fragmented.
	When the C-bit is set to one '1' this indicates that the attribute is being fragmented that is the next WiMAX VSA of the same WiMAX type is to be appended to this attribute.
	When the C-bit is set to zero '0' this indicates that the next attribute is not a fragment of this attribute.
	A WiMAX attribute that is not being fragmented w ill have the C-bit set to '0'. A WiMAX attribute that is being fragmented will have its C-bit set to '1' for all fragments until the last fragment which will have its C-bit set to '0' indicating it's the last fragment of the attribute.
	The r-bits are reserved for future use. They SHALL be set to zero by the sender and SHALL be ignored by the receiver.
Value	Value of the attribute which is one of the attribute formats given below or one or more sub-TLVs.

6   A sub-TLV has the following format:

```
7      0                   1                   2                   3
8      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
9     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
10    | SUB-TYPE      |   Length      |   Value
11    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
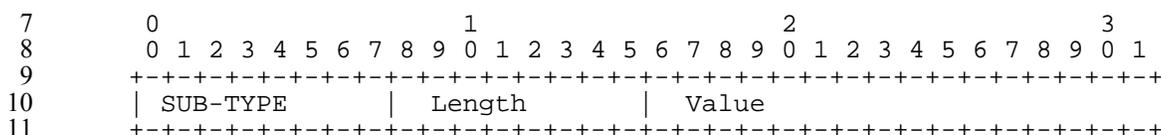
WType-ID	0 is reserved
	1-254 WiMAX Sub-Types
	255 is reserved
Length:	>= 3. Length of the WiMAX Sub-attribute including the Sub-type (1 octet), and Length Field (1 octet) and the length of the Value field (1 octet).
Value	Value of the attribute which is of one of the attribute formats defined below.

12   For each WiMAX VSA that consists of sub-TLVs a table summarizing the size and the presence of the TLVS in
13   each RADIUS message is given. The table indicates whether the sub-TLV is required or not in each message and
14   how many occurrences of the sub-TLV may appear in the message as follows:

0	The sub-TLV SHALL NOT appear.

1	The sub-TLV SHALL appear.
0-1	The sub-TLV MAY appear only once.
0-n	The sub-TLV MAY appear more than once.
1-n	The sub-TLV SHALL appear at least once.

1   The abbreviations used for the column headings for these tables are:

AR	Access-Request or if the attribute also appears in accounting then Accounting Request.
AA	Access-Accept.
AC	Access-Challenge
R	Access-Reject

2   The following table lists the attribute formats used in describing the WiMAX VSAs.

Attribute Format	Length	Description
Unsigned-Byte	1 octets	0 to 2^8-1. Most significant bit first
Unsigned-Short	2 octets	0 to 2^{16}-1. Most significant bit first
Unsigned Integer	4 octets	0 to 2^{32}-1. Most significant bit first
Text	> 1 octet	Contains UTF-8 encoded 10646 [7] characters. Text of length zero (0) SHALL NOT be sent; omit the entire attribute instead.
Octet-String	> 1 octet	Contains binary data (values 0 through 255 decimal, inclusive). Strings of length zero (0) SHALL NOT be sent; omit the entire attribute instead.

1   **5.4.2.1   WiMAX Capability**

```
2      0                   1                   2                   3
3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5     |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
6     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7     |     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
8     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9     |  Continuation |         TLVs
10    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
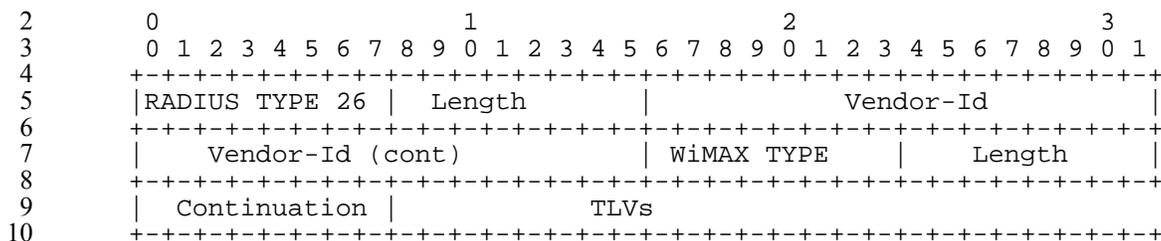
WType-ID	1 for WiMAX Capability Attribute
Description	In an Access-Request the attribute identifies the WiMAX Capabilities supported by the ASN or the HA. In an Access-Accept, identifies the options selected by the RADIUS server.
Length	6 + 3 + TLVs
Continuation	C-bit = 0
Value	One or more of the following sub-TLVs

11

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	WiMAX Release	6	1	0	0	0
2	Accounting Capabilities	3	1	1	0	0
3	Hotlining Capabilities	3	0-1[a]	0	0	0
4	Idle Mode Notification Capabilities	3	0-1[b]	0-1[c]	0	0

12   **Notes:**

[a]   The absence of this sub-TLV in an Access-Request (AR) means that the NAS or HA does not support hotlining.

[b]   The absence of this sub-TLV in an Access-Request (AR) means that the NAS does not support Idle Mode Notification. This sub-TLV SHALL NOT appear in Access-Request originating from an HA. The HAAA SHALL silently ignore this sub-TLV in messages originating from an HA.

[c]   The absence of this sub-TLV in an Access-Accept (AA) message means that the HAAA does not require Idle Mode Notification. The HAAA SHALL NOT send this sub-TLV to a HA. An HA SHALL silently ignore this sub-TLV.

13

TLV ID	1 for WiMAX Release
Description	In an Access-Request specifies the WiMAX release of the sender.
Length	2+Length of string
Value	A string indicating a WiMAX release formatted as: major + "." + minor. For example, the first release of WiMAX is indicated as "1.0"

14

TLV ID	2 for Accounting Capabilities
Description	In an Access-Request describes the accounting capabilities that are supported by the sender (ASN or HA). In an Access Accept, describes the accounting capabilities that the server selected for the session.
Length	2+1 octet
Value	In an Access-Request the NAS (ASN, HA) specifies the accounting capabilities that it supports as a bit-map. In an Access-Accept the server specifies one and only one of these options. 0 means that accounting is not required and is only valid when sending an Access-Accept to the HA. If the server selected more than one value or if the server selects a value not supported by the NAS, then the NAS SHALL treat the Access-Accept as an Access-Reject and it SHALL not provide any service to the MS. • 0x00 = No accounting. Only valid at the HA. • 0x01 = IP-Session-based accounting. Default value for the ASN. • 0x02 = Flow-based accounting

1

TLV ID	3 for Hotlining Capabilities
Description	In an Access-Request describes the hotline capacities supported by the ASN or the HA.
Length	2+1 octet
Value	In an Access-Request the NAS or HA specifies the hotlining capabilities that it supports as a bit-map. A value of zero or the omission of this subTLV means that hotlining is not supported. • 0x00 = Hotling is not Supported • 0x01 = Profile-based Hotlining is supported (using the Hotline-Profile-ID VSA) • 0x02 = Rule-based Hotlining is supported using NAS-Filter-Rule • 0x04 = Hotlining HTTP Redirection is supported. • 0x08 = Rule-based Hotlining is supported using IP-Redirection rule.

2

TLV ID	4 for Idle Mode Notification Capabilities
Description	In an Access-Request or Accept-Accept describes the idle mode notification capabilities supported by the ASN or required by the CSN. Omission of this sub TLV means that Idle Mode Notification is not supported or required.
Length	2+1 octet
Value	In an Access-Request the NAS (ASN) specifies if idle mode notification is supported at the ASN. In Access-Accept the HAAA specifies if idle mode notification is required at the HAAA. • 0x00 = Idle Mode notification is not supported or is not required. • 0x01 = Idle Mode notification is supported or is required.

3

1 ### 5.4.2.2 Device-Authentication-Indicator

```
2        0                   1                   2                   3
3        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5        |RADIUS TYPE 26 |    Length      |            Vendor-Id         |
6        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7        |     Vendor-Id (cont)           |   WiMAX TYPE   |    Length    |
8        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9        | Continuation  |    Value       |
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
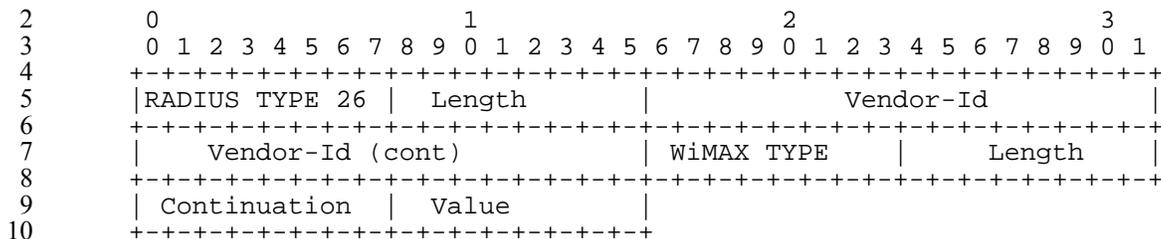
WType-ID	2 for Device-Authentication-Indicator
Description	The presence of the attribute in an Access-Request indicates that Device-Authentication was performed by the NAS. The value of the attributes indicates whether the authentication was successful or not.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned byte when set to 1 indicates that device authentication was successful. When set to 2 indicates that device authentication was unsuccessful.

11 ### 5.4.2.3 GMT-Time-Zone-Offset

```
12       0                   1                   2                   3
13       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       |RADIUS TYPE 26 |    Length      |            Vendor-Id         |
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17       |     Vendor-Id (cont)           |   WiMAX TYPE   |    Length    |
18       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19       | Continuation  |    Time-Zone-offset
20       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21                       |
22       +-+-+-+-+-+-+-+-+
```
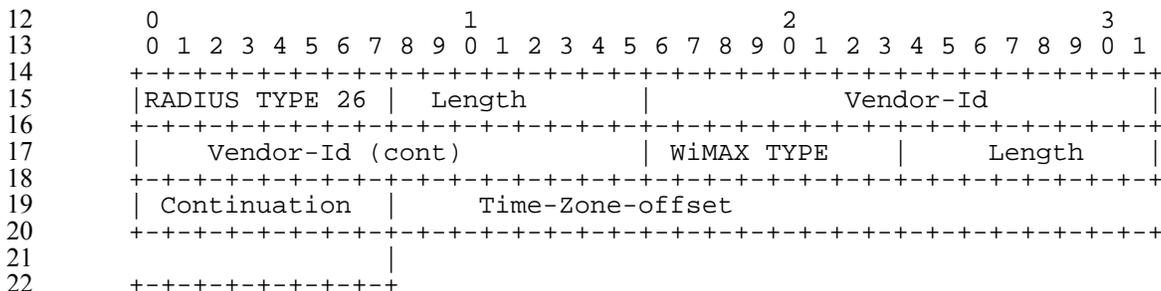
WType-ID	3 for GMT-Timezone-offset
Description	The current offset in seconds of the local time at the NAS with respect to GMT time.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	4 Octet-String interpreted as a Signed Integer (Most significant bit first) indicating a timeoffset in seconds.

23 ### 5.4.2.4 AAA-Session-ID

```
24       0                   1                   2                   3
25       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
26       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
27       |RADIUS TYPE 26 |    Length      |            Vendor-Id         |
28       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
29       |     Vendor-Id (cont)           |   WiMAX TYPE   |    Length    |
30       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
31       |  Continuation  |   AAA-Session-ID
32       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
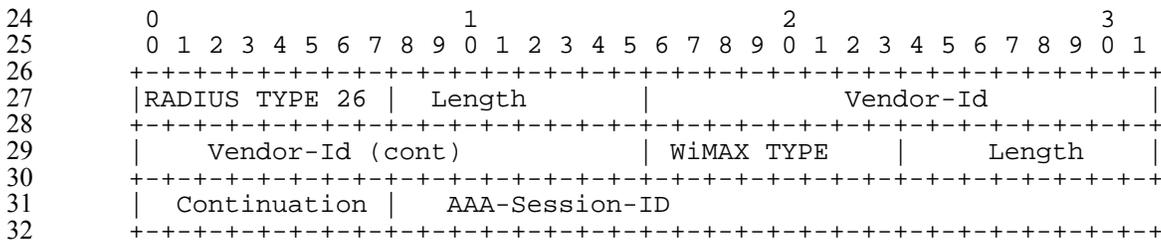
WType-ID	4 for AAA-Session-ID

Description	A unique per realm identifier assigned to the WiMAX session by the Home network during network entry.
	The value is included in all subsequent AAA packets for that session.
Length	6 + 3 + Length of ID
Continuation	C-bit = 0
Value	Octet String. The value of the AAA-Session-ID

5.4.2.5   MSK

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |  SALT                         |    String
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	5 for MSK
Description	The Master Session Key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted MSK.
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2 octet SALT (see [35]) and String containing the encrypted MSK formulated as per [35].

5.4.2.6   HA-IP-MIP4

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |   HA-IP
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
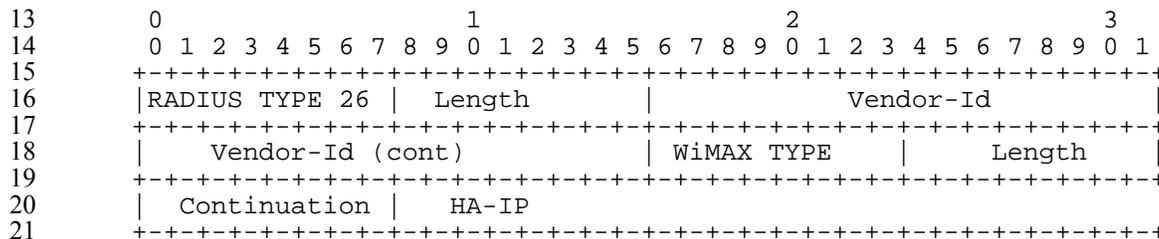
WType-ID	6 for HA-IP-MIP4
Description	The IPv4 address of the HA for CMIP4..
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first)

1 ### 5.4.2.7 HA-IP-MIP6

```
 2      0                   1                   2                   3
 3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 4      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 5      |RADIUS TYPE 26 |    Length     |              Vendor-Id        |
 6      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 7      |    Vendor-Id (cont)           |   WiMAX TYPE  |     Length    |
 8      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 9      |  Continuation |    HA-IP
10      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
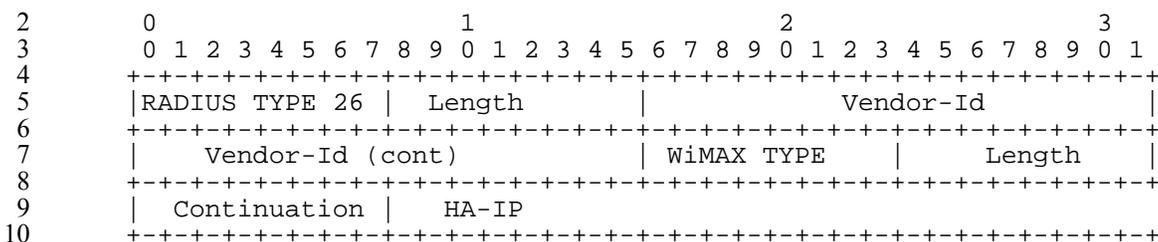
WType-ID	7 for HA-IP-MIP6
Description	The IPv4 or IPv6 address of the HA used for MIP6.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first)

11 ### 5.4.2.8 DHCPv4-Server

```
12      0                   1                   2                   3
13      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15      |RADIUS TYPE 26 |    Length     |              Vendor-Id        |
16      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17      |    Vendor-Id (cont)           |   WiMAX TYPE  |     Length    |
18      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19      |  Continuation |    DHCP-Server IPv4
20      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
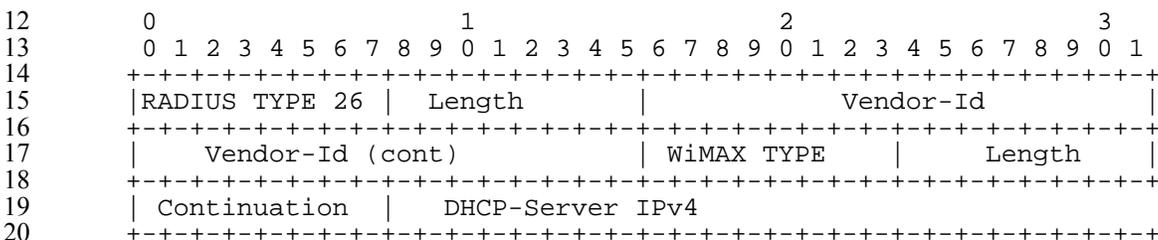
WType-ID	8 for DHCPv4-Server
Description	The IPv4 or IPv6 address of the DHCP-Server to use for IPv4 address allocation by the ASN.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first).

21 ### 5.4.2.9 DHCPv6-Server

```
22      0                   1                   2                   3
23      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
24      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
25      |RADIUS TYPE 26 |    Length     |              Vendor-Id        |
26      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
27      |    Vendor-Id (cont)           |   WiMAX TYPE  |     Length    |
28      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
29      |  Continuation |    DHCP-Server  IPv6
30      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
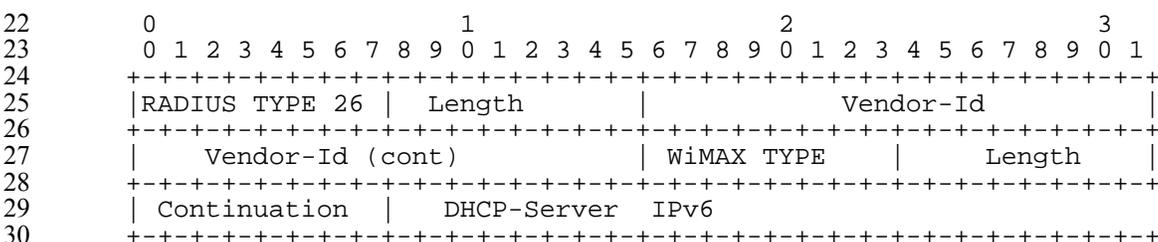
WType-ID	9 for DHCPv6-Server
Description	The IPv4 or IPv6 address of the DHCP-Server to use for IPv6 allocation by the ASN.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0

Value	Octet string containing an IPv4 or IPv6 address (most significant bit first).

1 **5.4.2.10 MN-HA-MIP4-KEY**

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |RADIUS TYPE 26 |    Length     |            Vendor-Id          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | Continuation  |            SALT               |    String
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	10 for MN-HA-MIP4-KEY
Description	The MN-HA-KEY sent by the RADIUS Server to the ASN (for PMIP) or HA use for CMIP4 (CMIP or PMIP). It is used by the ASN during PMIP4 to calculate the MN-HA-AE. It is sent to the HA to validate the MN-HA-AE (CMIP4) and to compute the MN-HA-AE for of the CMIP4 Registration Response or the AUTH for MIP6 Binding Answer based on the MIP version(MIP4 or CMIP6) and the SPI.
Length	6 + 3 +2(SALT)+ Length of the encrypted MN-HA-MIP4-KEY
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2 octet SALT (see [35]) and String containing the encrypted MN-HA-MIP4-KEY formulated as per [35].

12 **5.4.2.11 MN-HA-MIP4-SPI**

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |RADIUS TYPE 26 |    Length     |            Vendor-Id          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | Continuation  |               SPI                             |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |               |
     +-+-+-+-+-+-+-+-+-+
```
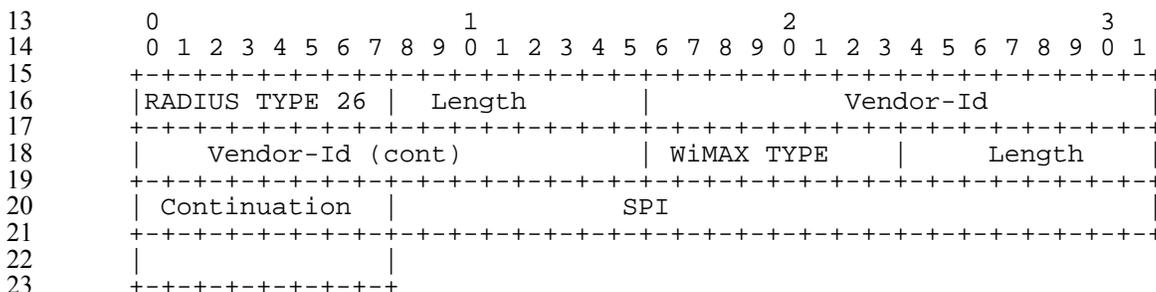
WType-ID	11 MN-HA-MIP4-SPI
Description	The SPI associated with the MN-HA-MIP4-KEY
Length	6+3+4
Continuation	C-bit = 0
Value	Unsigned 32-bit Integer.

1 ### 5.4.2.12 MN-HA-MIP6-KEY

```
2      0                   1                   2                   3
3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5     |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
6     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7     |     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
8     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9     | Continuation  |           SALT              |     String
10    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11
```

WType-ID	12 for MN-HA-MIP6-KEY
Description	The MN-HA-MIP6-KEY sent by the RADIUS Server to the ASN or HA used for CMIP6. It is used by the ASN during PMIP6 to calculate the AUTH for MIP6 BU. It is sent to the HA to validate AUTH and to compute the AUTH for MIP6 Binding Answer.
Length	6 + 3 + 2(SALT)+ Length of the encrypted MN-HA-MIP6-KEY
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2 octet SALT (see [35]) and String containing the encrypted MN-HA-MIP6-KEY formulated as per [35].

12 ### 5.4.2.13 MN-HA-MIP6-SPI

```
13     0                   1                   2                   3
14     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
15    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16    |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
17    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
18    |     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
19    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20    | Continuation  |            SPI                                |
21    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
22                    |
23    +-+-+-+-+-+-+-+-+
```
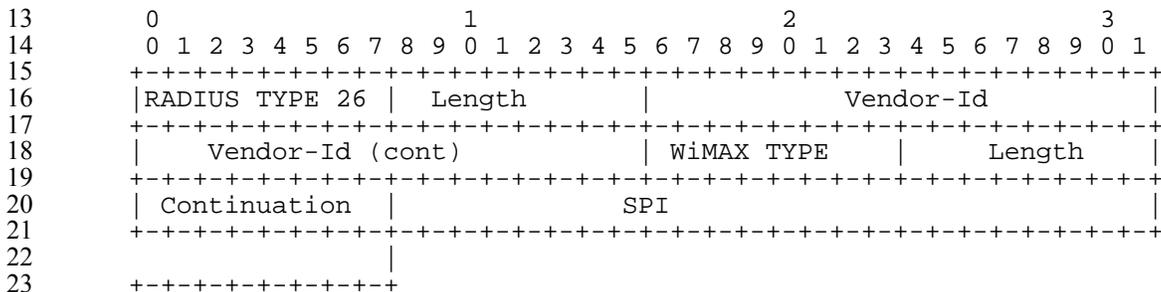
WType-ID	13 MN-HA-MIP6-SPI
Description	The SPI associated with the MN-HA-MIP6-KEY/
Length	6 +3+4
Continuation	C-bit = 0
Value	Unsigned 32-bit Integer.

1   **5.4.2.14 FA-RK-KEY**

```
2        0                   1                   2                   3
3        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5        |RADIUS TYPE 26 |    Length     |              Vendor-Id        |
6        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7        |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
8        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9        | Continuation  |     SALT                      |     String
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	14 for FA-RK-KEY
Description	The FA-RK determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate MN-FA keys.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted FA-RK-KEY.
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2-octet SALT (see [35]) and String containing the encrypted FA-RK formulated as per [35].

11   **5.4.2.15 HA-RK-KEY**

```
12       0                   1                   2                   3
13       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       |RADIUS TYPE 26 |    Length     |              Vendor-Id        |
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17       |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
18       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19       | Continuation  |     SALT                      |     String
20       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	15 for HA-RK-KEY
Description	The HA-RK-KEY determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate FA-HA keys.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted HA-RK-KEY.
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2-octet SALT (see [35]) and String containing the encrypted HA-RK formulated as per [35].

21   **5.4.2.16 HA-RK-SPI**

```
22       0                   1                   2                   3
23       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
24       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
1    |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
2    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
3    |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
4    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5    | Continuation  |    TLV
6    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
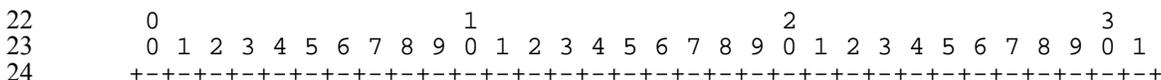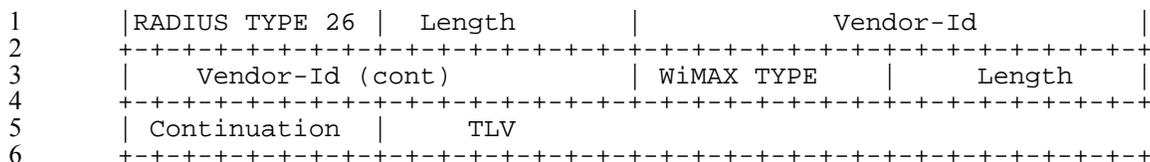
WType-ID	16 for HA-RK-SPI
Description	The SPI used for the HA-RK.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

7 **5.4.2.17 HA-RK-Lifetime**

```
8        0                   1                   2                   3
9        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11       |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
12       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
13       |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       | Continuation  |    TLV
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
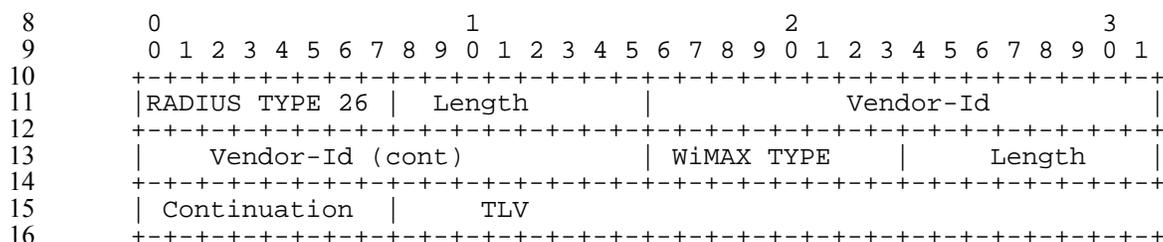
WType-ID	17 for HA-RK-Lifetime
Description	The Lifetime of the HA-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the time before the key expires in seconds.

17 **5.4.2.18 RRQ-HA-IP**

```
18       0                   1                   2                   3
19       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
20       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21       |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
22       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
23       |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
24       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
25       | Continuation  |    RRQ HA-IP
26       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
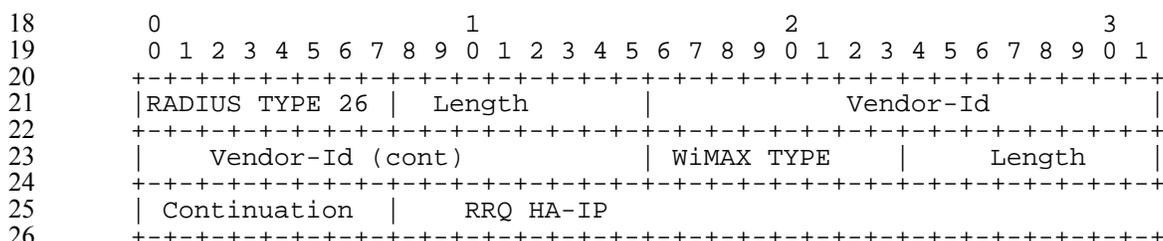
WType-ID	18 for RRQ-HA-IP
Description	The IPv4 or IPv6 address of the HA as contained in the MIP Registration Request or the BU.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first)

5.4.2.19 RRQ-MN-HA-KEY

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |    Length         |           Vendor-Id         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      Vendor-Id (cont)            |   WiMAX TYPE   |    Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation  |    SALT                         |    String
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	19 for RRQ-MN-HA-KEY
Description	The MN_HA key sent by the HAAA to the HA to be used to validate the MN-HA-AE of the Mobile IP Registration Request.
Length	6 + 3 +2(SALT)+ Length of the encrypted RRQ-MN-HA-KEY
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2-octet SALT (see [35]) and String containing the encrypted RRQ-MN-HA-KEY formulated as per [35].

5.4.2.20 Session-Continue

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |    Length         |           Vendor-Id         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      Vendor-Id (cont)            |   WiMAX TYPE   |    Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation  | Session-Continue Flag
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                |
   +-+-+-+-+-+-+-+-+
```
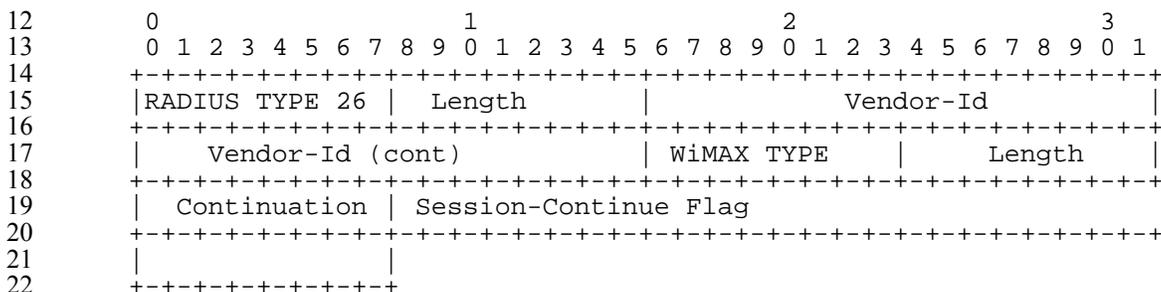
WType-ID	21 for Session-Continue
Description	This attribute when set to 'true' means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. 'False' means end of a session.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	If the value is set to 1 session continue is true. If the value is set to 0 session continue is false.

1 **5.4.2.21 Beginning of Session**

```
2        0                   1                   2                   3
3        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5        |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
6        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7        |     Vendor-Id (cont)          |   WiMAX TYPE  |     Length    |
8        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9        | Continuation  | Beginning of Session Flag
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
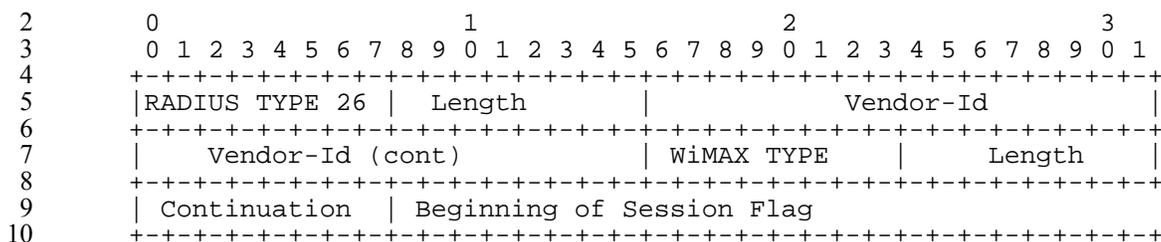
WType-ID	22 for Beginning of Session
Description	This attribute when set to 'true' means that this Accounting Start packet marks the start of a new flow. If set to 'False', this Accounting Start message is a continuation of a previous flow.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	If the value is set to 1 Beginning of Session is true. If the value is set to 0 Beginning of Session is false.

11 **5.4.2.22 IP Technology**

```
12       0                   1                   2                   3
13       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17       |     Vendor-Id (cont)          |   WiMAX TYPE  |     Length    |
18       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19       | Continuation  |         IP-Technology Enumeration
20       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21       |               |
22       +-+-+-+-+-+-+-+-+-+
```
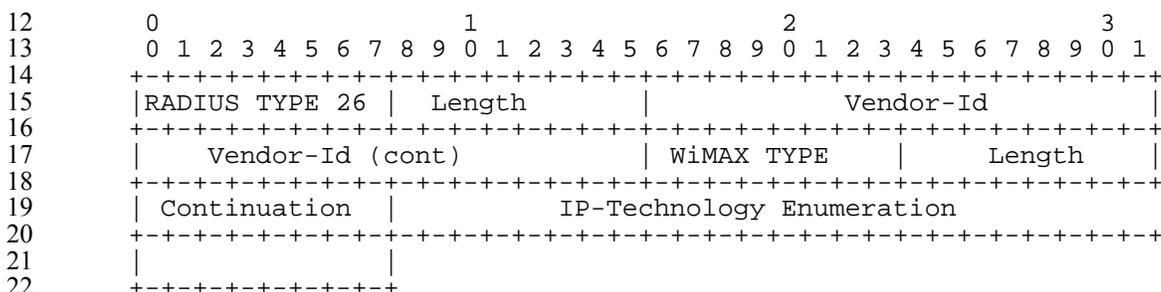
WType-ID	23 for IP-Technology
Description	This attribute indicates which type of WiMAX session is being used.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer. The enumeration is defined as follows: • 0 = Reserved • 1 = Reserved • 2 = PMIP4 • 3 = CMIP4 • 4 = CMIP6 • 5 = Ethernet-CS • 6 - 2^{32}-1 = Reserved

1 **5.4.2.23 Hotline-Indicator**

```
2        0                   1                   2                   3
3        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5        |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
6        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7        |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
8        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9        | Continuation  |       Hotline Indicator String
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	24 for Hotline Indicator
Description	This attribute in a RADIUS Accounting-Request message indicates to back-office systems (billing audit systems) that the session has been Hot-Lined. Exactly one Hot-Line Accounting Indication VSA may appear in a RADIUS Access-Accept message or RADIUS COA message. If the Hot-lining Device (PDSN, HA) received this attribute in a RADIUS Access-Accept or COA message, then it SHALL include the attribute in any subsequent RADIUS Accounting messages for that session.
Length	6 + 3 + Length of String (>0).
Continuation	C-bit = 0
Value	A string value which is to be opaque.

11 **5.4.2.24 Prepaid Indicator**

```
12       0                   1                   2                   3
13       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17       |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
18       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19       | Continuation  | Flag          |
20       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21
```
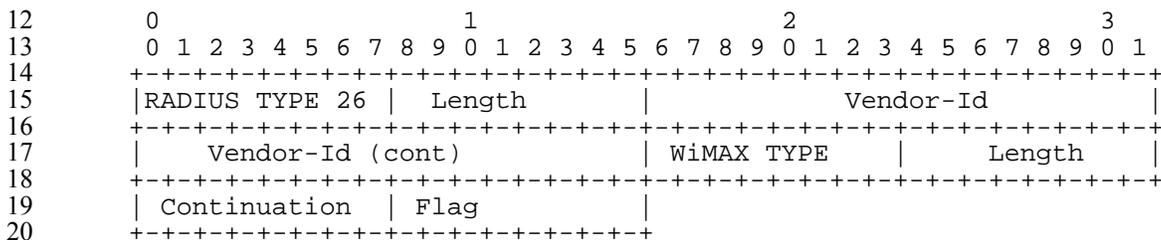
WType-ID	25 for Prepaid Indicator
Description	This attribute appears in Accounting messages and indicates to the backoffice that this session was associated with a prepaid user (on-line accounting). If the attribute is not present the session is deemed to be an offline (not prepaid) session.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. An enumerated value set to 1 indicates the session is an online session. A value of '0' indicates offline session.

22 **5.4.2.25 PDFID**

```
23       0                   1                   2                   3
24       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
25       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
26       |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
27       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
28       |     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
29       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
30       | Continuation  |    Unsigned Short             |
31       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
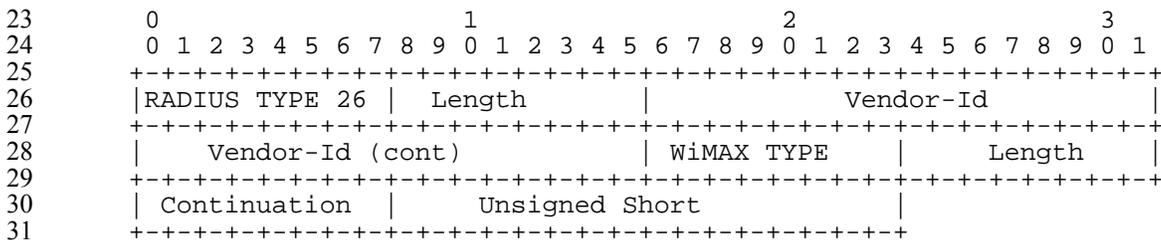
WType-ID	26 for PDFID
Description	This value of this attribute matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios.
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	Unsigned Short. Packet Data Flow Identifier. (Most significant bit first)

5.4.2.26 SDFID

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length     |              Vendor-Id        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |    Unsigned Short             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
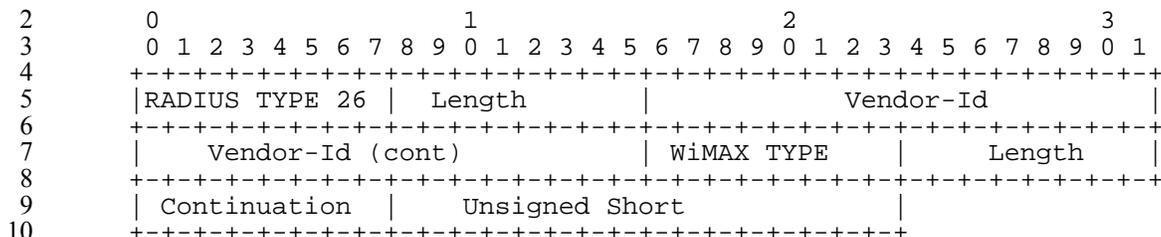
WType-ID	27 for SDFID
Description	The value of this attribute matches all records from the same packet data flow. SDFID is assigned by the CSN and remains constant through all handover scenarios.
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	Unsigned Short. Service Data Flow Identifier (Most significant bit first)

5.4.2.27 Packet-Flow Descriptor

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length     |              Vendor-Id        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |              TLV
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
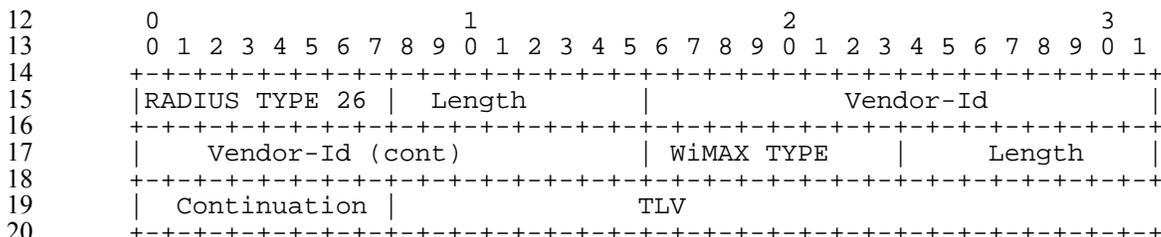
Type-ID	28 for Packet-Flow-Descriptor
Description	This attribute describes a packet flow. A packet flow may describe a uni-directional flow and bidirectional flow. The packet flow descriptor may be pre-provisioned. A packet flow descriptor references one or two QoS specifications.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	PacketDataFlowID	2+2	0	1	0	0
2	ServiceDataFlowID	2+2	0	0-1	0	0
3	ServiceProfileID	2+4	0	0-1[a]	0	0
4	Direction	2+1	0	0-1[b]	0	0
5	ActivationTrigger	2+1	0	0-1[b]	0	0
6	TransportType	2+1	0	0-1[b]	0	0
7	UplinkQosID	2+1	0	0-1 [c]	0	0
8	DownlinkQoSID	2+1	0	0-1 [d]	0	0
9	UplinkClassifier	2+Length	0	0-n[c]	0	0
10	DownlinkClassifier	2+Length	0	0-n[d]	0	0

1 **Notes:**

[a] If ServiceProfileID is provided then TLV IDs greater then 3 overrides the QoS parameter settings of the related ServiceProfile according to the TLV-value.

[b] If ServiceProfileID is not provided these RADIUS attributes are MANDATORY. If the RADIUS dius-attributes are missing then the NAS SHALL silently discard this RADIUS attribute and should reject the network entry of the MS. An accounting-stop message with an error reason should be generated.

[c] This attribute SHALL be present if SerivceProfileId is not present and:

Direction is Uplink or

Direction is bi-directional and the flow is symmetrical

If the attribute is missing then the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.

[d] This attribute SHALL be present if SerivceProfileID is not present and:

Direction is Downlink or

Direction is bi-directional and not symmetrical.

If the attribute is missing then the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.

2

TLV ID	1 for PacketDataFlow-ID
Description	This attributes identifies a packet data flow instance. The identifier is assigned by the home network and is unique per mobile session for the entire session. PacketDataFlow-IDs 1 to 20 are reserved for the packet data flow of the Initial Service Flow (ISF).
Length	2+2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid,

3

TLV ID	2 for ServiceDataFlow-ID
Description	This attribute is used to group of one or more packet data flows belonging to the same service instances (e.g., a combined voip/video call). The number is assigned by the home network and is unique per mobile session for the entire session. The same Service Data Flow ID may appear in more than one Packet Data Flow ID. ServiceDataFlow-ID of 1 is reserved for the Initial Service Flow.
Length	2+2.
Value	Unsigned Short representing the Service flow identifier (most significant bit first). This value is assigned by the home network and is unique per mobile session for the life of the session. A value of zero(0) is invalid.

1

TLV ID	3 ServiceProfileID
Description	This attribute identifies a pre-configure flow descriptor at the NAS.
Length	2+4.
Value	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.

2

TLV ID	4 for Direction
Description	The direction of the Packet Data Flow.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Uplink • 2 = Downlink • 3 = Bi-directional • 4 – FF = Reserved

3

TLV ID	5 for Activation Trigger
Description	This parameter specifies the trigger to be used for the activation of the service flow. For the ISF, Provisioned, Admit andActivate SHALL be set. The Activate SHALL be mandatorly supported by the ASN. All other states need not to be supported in Rel1.0 and should be interpreted as "Activate" if not supported.
Length	2+1
Value	Octet bit-map with the following values: • 0x00 = Reserved • 0x01 = Provisioned (SHALL be set in case of ISF) • 0x02 = Admit (SHALL be set in case of ISF) • 0x04 = Activate (SHALL be set in case of ISF) • 0x08 = Dynamically Changeable (not valid for ISF) • 0x1z to 0x8z = Reserved

1

TLV ID	6 for Transport Type
Description	Defines the transport type which might be IP (v4 or v6) as well as Ethernet. This parameter need to be mapped into "CS specification" as defined in IEEE802.16e [REF1].
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = IPv4-CS • 2 = IPv6-CS • 3 = Ethernet • 4 – 255 = Reserved

2

TLV ID	7 for UplinkQoSID
Description	The identifier of the QoS descriptor for the uplink direction or for bi-direction if the flow is bi-directional with symmetrical QoS. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.
Length	2+1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

3

TLV ID	8 for DownlinkQoSID
Description	The identifier of the QoS descriptor for the downlink direction. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.
Length	2+1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

4

TLV ID	9 for UpLinkClassifier
Description	The classifier to match for traffic flowing in the uplink direction. If the classifier cannot be parsed then the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.
Length	2+Length of string
Value	String containing an IP-Filter Rule as pre [48]. Action is set to "permit".

5

TLV ID	10 for DownLinkClassifier
Description	The classifier to match for traffic flowing in the downlink direction. If the classifier cannot be parsed then the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.

Length	2+Length of string
Value	String containing an IP-Filter Rule as pre [48]. Action is set to permit.

1 **5.4.2.28 QoS-Descriptor**

```
2      0                   1                   2                   3
3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5     |RADIUS TYPE 26 |   Length      |           Vendor-Id           |
6     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7     |      Vendor-Id (cont)         |  WiMAX TYPE   |    Length     |
8     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9     |  Continuation |              TLVs
10    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
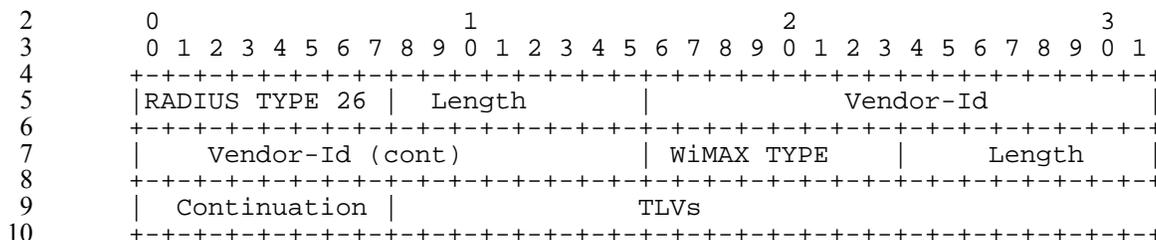
Type-ID	29 for QoS-Descriptor
Description	This attribute describes over the air QoS parameter that are associated with a flow. The QoS-Descriptor is only valid for the actual RADIUS transaction.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types are described below.

11

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	QoS ID	3	0	1	0	0
2	Global Service Class Name	2+6	0	0-1	0	0
3	Service Class Name	2+Length	0	0-1	0	0
4	Schedule Type	3	0	1	0	0
5	Traffic Priority	3	0	0-1[a][b]	0	0
6	Maximum Sustained Traffic Rate	6	0	0-1[a]		
7	Minimum Reserved Traffic Rate	6	0	0-1[a]	0	0
8	Maximum Traffic Burst	6	0	0-1[a]	0	0
9	Tolerated Jitter	6	0	0-1[a]	0	0
10	Maximum Latency	6	0	0-1[a]	0	0
11	Reduced Resource Code	3	0	0-1[a]	0	0
12	Media Flow Type	2+Length	0	0-1[a]	0	0
13	Unsolicited Grant Interval	4	0	0-1[a]	0	0
14	SDU Size	3	0	0-1[a]	0	0
15	Unsolicited Polling Interval	4	0	0-1[a]	0	0

12 **Notes:**

[a]   The inclusion of these attributes are as per the value of the Schedule-Type inaccordance to Table 5-11.

[b]   If omitted the traffic priority is assumed to be 0.

Table 5-11 – Showing Valid QoS Attributes for Each Schedule-Type

ID	QoS Parameter	BE	ERT-VR	UGS	RT-VR	NRT-VR
5	Traffic Priority.	0-1[a]	0-1[a]	0	0-1[a]	0-1[a]
6	Maximum sustained traffic rate.	0-1	0-1 [b]	0	0-1[b]	0-1[b]
7	Minimum reserved traffic rate.	0	1	1	1	1
8	Maximum Traffic burst.	0	0-1	0	0-1	0-1
9	Tolerated jitter	0	0-1[c]	0-1[c]	0	0
10	Maximum latency.	0	1	1	1	0
13	Unsolicited Grant Interval	0	1	1	0	0
14	SDU Size	0	0	0-1[d]	0	0
15	Unsolicited Polling Interval	0	0	0	1	0

Notes:

[a]   If omitted then traffic priority SHALL equals 0.

[b]   If absent SHALL default to Minimum Reserved Traffic Rate.

[c]   If omitted then jitter SHALL equal to maximum latency.

[d]   If omitted then SDU SHALL be variable.

TLV ID	1 for QoS ID
Description	A unique ID for this QoS specification in this packet. The ID is used in the Service Flow Descriptor attribute to reference a specific QoS Spec (see the UplinkQoSID and DownlinkQoSID TLVs)
Length	2+1
Value	Unsigned Octet representing an ID.

TLV ID	2 for Global Service Class Name
Description	This parameter represents the Global Service Class Name as defined in IEEE802.16e
Length	2+6
Value	String of length 6 octet containing the name of the global service class name. Values are defined in IEEE802.16e.

TLV ID	3 for Service Class Name
Description	This parameter represents the Service Class Name as defined in IEEE802.16e

Length	2+Length of Service Class String (>=1)
Value	String containing the name of the service class name. Values are defined in IEEE802.16e.

1

TLV ID	4 for Schedule Type
Description	The parameter specifies the Uplink Granted Scheduling Type as defined in IEEE802.16e.
Length	2+1
Value	Octet enumeration with the following values defined: • 0 = Reserved • 1 = Reserved • 2 = Best Effort • 3 = nrtPS • 4 = rtPS • 5 = Extended rtPS • 6 = UGS • 7 – 255 = Reserved

2

TLV ID	5 for Traffic Priority
Description	The value of this parameter specifies the priority assigned to a service flow. Given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.
Length	2+1
Value	0 to 7 – Higher numbers indicate higher priority. Default 0.

3

TLV ID	6 for Maximum Sustained Traffic Rate
Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Length	2+4
Value	Unsigned Integer specifying a rate in bits per second.

4

TLV ID	7 for Minimum Reserved Traffic Rate
Description	Represents the Minimum Reserved Traffic Rate as defined in IEEE802.16e. This parameter specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second and specifies the minimum amount of data to be transported on behalf of

	the service flow when averaged over time. The specified rate SHALL only be honored when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter SHALL be satisfied by assuring the available data is transmitted as soon as possible.
Length	2+4
Value	Unsigned Integer specifying the rate in bytes.

1

TLV ID	8 for Maximum Traffic Burst
Description	Represents the Maximum Traffic Burst as defined in IEEE802.16e. This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Length	2+4
Value	Unsigned Integer specifying the burst size in bytes per second as defined by IEEE802.16e.

2

TLV ID	9 for Tolerated Jitter
Description	Represents the Tolerated Jitter as defined in IEEE802.16e
Length	2+4
Value	Unsigned Integer representing the maximum delay variation (jitter) (in milliseconds).

3

TLV ID	10 for Maximum Latency
Description	Represents the Maximum Latency as defined in IEEE802.16e. Time period between the reception of a packet by the BS or MS on its network interface and the delivering the packet to the RF Interface of the peer device. If defined, this parameter represents a service commitment (or admission criteria) at the BS or MS and SHALL be guaranteed by the BS or MS. A BS or MS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Length	2+4
Value	Unsigned Integer specifying a maximum latency in units of milliseconds

4

TLV ID	11 for Reduced Resources Code
Description	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available.
Length	2+1
Value	Unsigned Octet: value of 0 is not allowed, value of 1 allowed. Other values are reserved.

5

TLV ID	12 for Media Flow Type
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.

Length	2+Length of String
Value	The first octet of the string represents an enumeration with the following values: • 0 = Reserved • 1 = Voice over IP • 2 = Robust Browser • 3 = Secure Browser/ VPN • 4 = Streaming video on demand • 5 = Streaming live TV • 6 = Music and Photo Download • 7 = Multi-player gaming • 8 = Location-based services • 9 = Text and Audio Books with Graphics • 10 = Video Conversation • 11 = Message • 12 = Control • 13 = Data • 14 – 254 = Reserved • 255 = Media Description in SDP format is included The 1st octet is always present in this TLV as an enumerator. Other fields presence and format depends on the code value set in the enumerator: If the 1st octet enumerator is set to indicate "Media Description in SDP format" (value 255), then variable-length SDP string is added: <SDP string> encoded as specified in IETF RFC 2327.

1

TLV ID:	13 for Unsolicited Grant Interval
Description:	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Length:	2+2
Value:	Unsigned Short measuring time in milliseconds.

2

TLV ID	14 for SDU Size
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec). If this attribute is absent then the SDU SHALL be variable.
Length	2+1
Value	8-bit unsigned integer. Default = 49

3

TLV ID	15 for Unsolicited Polling Interval

Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Length	2+2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).

5.4.2.29 Granted-QoS

This section intentionally left blank.

5.4.2.30 Control-Packets-In

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length     |             Vendor-ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |   WiMAX TYPE  |    Length      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |              Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |
+-+-+-+-+-+-+-+-+
```
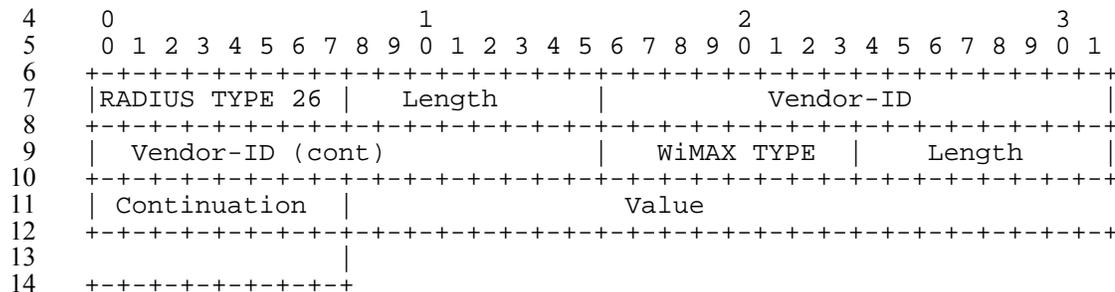
WType-ID	31 for Control-Packets-In
Description	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing packets count.

5.4.2.31 Control-Octets-In

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length     |             Vendor-ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |   WiMAX TYPE  |    Length      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |              Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |
+-+-+-+-+-+-+-+-+
```
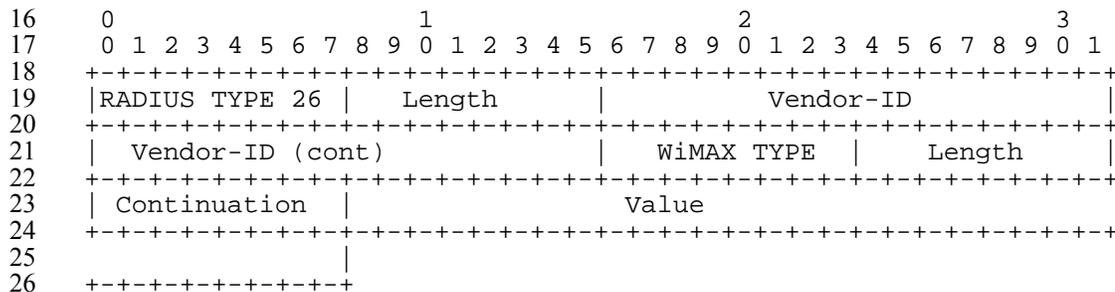
WType-ID	32 for Control Octets In
Description	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing octets.

1 **5.4.2.32 Control-Packets-Out**

```
2    0                   1                   2                   3
3    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5    |RADIUS TYPE 26 |   Length      |             Vendor-ID         |
6    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7    |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
8    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9    | Continuation  |               Value
10   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11                   |
12   +-+-+-+-+-+-+-+-+
```
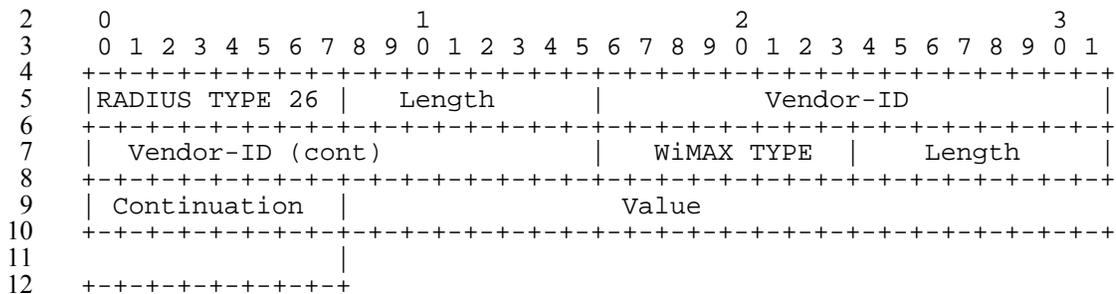
WType-ID	33 for Control-Packets-Out
Description	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing packets count.

13 **5.4.2.33 Control Octets Out**

```
14   0                   1                   2                   3
15   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
16   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17   |RADIUS TYPE 26 |   Length      |             Vendor-ID         |
18   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
20   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21   | Continuation  |               Value
22   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
23                   |
24   +-+-+-+-+-+-+-+-+
```
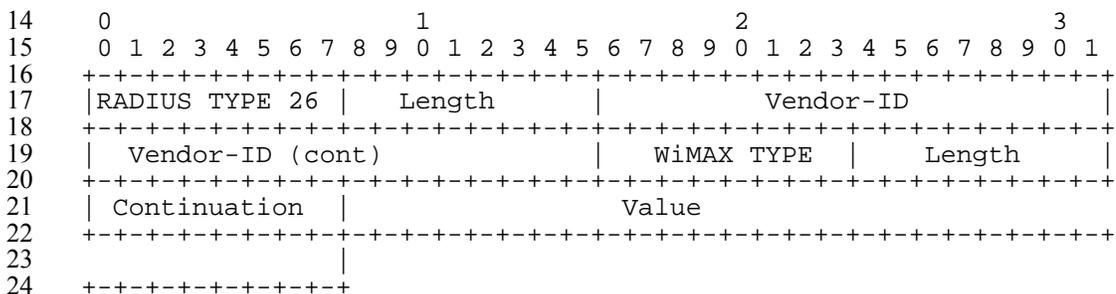
WType-ID	34 for Control Octets Out
Description	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing an octet count.

25 **5.4.2.34 PPAC**

```
26    0                   1                   2                   3
27    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
28    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
29    |RADIUS TYPE 26 |   Length      |             Vendor-Id         |
30    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
31    |     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
32    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
33    | Continuation  |         TLV
34    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
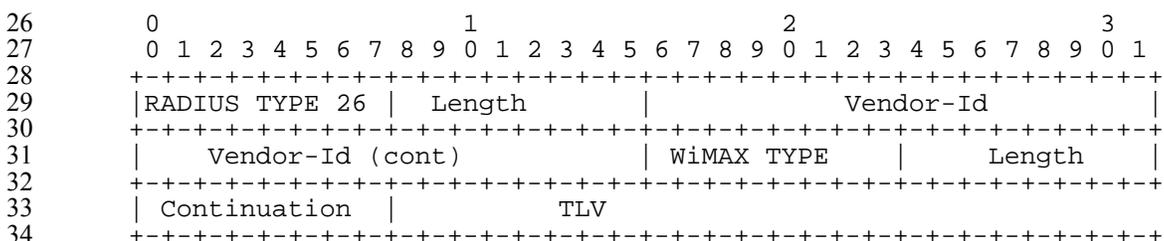
WType-ID	35 for PPAC
Description	The PrepaidAccountingCapability (PPAC) attribute is sent in the Access-Request message by a prepaid capable NAS and is used to describe the prepaid capabilities of the NAS.

Length	6 + 3 + TLVs
Continuation	C-bit = 0.
Value	The sub-types described below.

1

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	AvailableInClient (AiC)	2+4	1	0	0	0

2

TLV ID	1 for AvailableInClient (AiC)
Description	The optional AvailableInClient Subtype, generated by the PPC, indicates the metering capabilities of the NAS and SHALL be bitmap encoded. The possible values are as follows.
Length	2+4
Value	4 Octet String interpreted as a bit map with the following values: • 0x00000000 = Reserved • 0x00000001 = Volume metering supported • 0x00000002 = Duration metering supported • 0x00000004 = Resource metering supported • 0x00000008 = Pools supported • 0x00000010 = Rating groups supported • 0x00000020 = Multi-Services supported • 0x00000040 = Tariff Switch supported

3 **5.4.2.35 Session Termination Capability**

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length     |             Vendor-Id         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Vendor-Id (cont)          |   WiMAX TYPE  |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              4 Octet-String                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
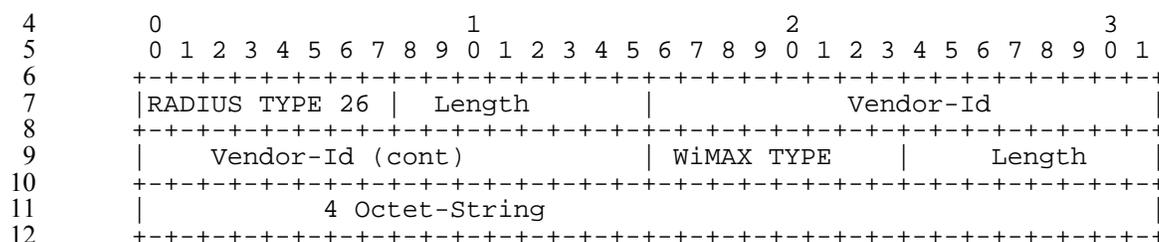
WType-ID	36 for Session Termination Capability
Description	This attribute is included in a RADIUS Access-Request message to the RADIUS server and indicates whether or not the NAS supports Dynamic Authorization.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	4 octet Bit Mask with the following values: • 0x00000000 = Reserved • 0x00000001 = Dynamic Authorization Extensions ([28]) is supported

1 **5.4.2.36 PPAQ Attribute**

```
 2      0                   1                   2                   3
 3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 4      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 5      |RADIUS TYPE 26 |   Length      |            Vendor-Id          |
 6      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 7      |     Vendor-Id (cont)          |  WiMAX TYPE   |    Length     |
 8      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 9      | Continuation  |       TLV
10      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	37 for PPAQ
Description	One or more PPAQ attributes are sent in an Access Request, Authorize- Only Access-Request and Access-Accept message. In an Access Request message, the PPAQ attribute is used to facilitate One-Time charging transactions. In Authorize-Only Access-Request messages it is used for One-Time charging, report usage and the request for further quota. It is also used in order to request prepaid quota for a new service instance. In an Access-Accept message it is used in order to allocate the (initial and subsequent) quotas. When multiple services are supported, a PPAQ is associated with a specific service as indicated by the presence of a Service-Id, a Rating-Group-Id, or the "Access Service" (as indicated by the absence of a Service-Id and a Rating-Group-Id).
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

11

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	Quota Identifier	2+Length	0-1[g]	0-1[m][n]	0	0
2	VolumeQuota	2+Variable	0-1[a][g]	0-1[a][k][n]	0	0
3	VolumeThreshold	2+4	0	0-1[a][m][n]	0	0
4	DurationQuota	2+4	0-1[b][g]	0-1[b][k][n]	0	0
5	DurationThershold	2+4	0	0-1[b][m][n]		
6	ResourceQuota	2+4	0-1[c][g]	0-1[c][k][n]	0	0
7	ResourceThreshold	2+4	0	0-1[c][m][n]	0	0
8	Update-Reason		0-1[d][g]	0	0	0
9	PrepaidServer		0-n[e][g]	0-n[e][m][n]	0	0
10	Service-ID	2+Length	0-1[g][h][j]	0-1[m][n]	0	0
11	Rating-Group-ID	2+4	0-1[g][h][j]	0-1[m][n]	0	0
12	Termination-Action	2+1	0	0-1[m][n]	0	0
13	Pool-ID	2+4	0	0-1[m][n]	0	0
14	Pool-Multiplier	2+	0	0-1[f][m][n]	0	0
15	Requested-Action	2+1	0-1[g]	0	0	0
16	Check-Balance-Result	2+1	0	0-1[k][m][n]	0	0

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
17	Cost-Information AVP	2+	0	0-1[n]	0	0

1 **Notes:**

[a]   SHALL be present if volume based charging is used. SHALL NOT be present otherwise. Volume Threshold is optional.

[b]   SHALL be present if duration-based charging is used. SHALL NOT be present otherwise. Duration threshold is optional.

[c]   SHALL be present if resource-based charging is used. SHALL NOT be present otherwise. Resource threshold is optional.

[d]   SHALL be present in an Authorize-Only Access-Request.

[e]   MAY be present in an Access-Accept. If present in Access Accept it SHALL be present in Access-Request (except for the first Access-Request)

[f]   Pool Multiplier SHALL be present when Pool-ID is present otherwise Pool Multiplier SHALL NOT be present in the PPAQ.

[g]   If Requested-Action is present then Service-ID SHALL also be present and all other attributes SHALL NOT be present.

[h]   PPAQ SHALL NOT contain both a Service-ID and a Rating-Group-ID.

[j]   A PPAQ that does not contain a Service-ID or a Rating-Group-Id refers to the "Access Service"(ISF).

[k]   If Balance-Check-Result is present and set to 0 then either VolumeQuota, DurationQuota or ResourceQuota SHALL be present.

[m]   If Balance-Check-Result is present then Service-ID SHALL also be present and other attributes(tagged with m) SHALL NOT be present.

[n]   The PPAQ in which a Cost-Information occurs SHALL NOT include a QID, because no quota is actually reserved by the PPS. The Service-ID SHALL be present with the Cost-Information for that Service-ID may not be present if the Cost-Information cannot be provided. All other attribute SHALL not appear.

2

TLV ID	1 for Quota Identifier
Description	It is generated by the PPS together with the allocation of new quota. The online quota update RADIUS Access-Request message that is sent from the SAD to the PPS includes a previously received QuotaIdentifier AVP.
Length	2+Length of Quota Identifier
Value	Octet String. The Quota Identifier value (most significant bit first)

3

TLV ID	2 for VolumeQuota
Description	The length of this AVP is 12 or 18 octets. In a RADIUS Access-Accept message (PPS to SAD direction), it indicates the volume (in octets) allocated for the session by the PPS. In an RADIUS Authorize-Only Access-Request message (SAD to PPS direction), it indicates the total used volume (in octets) for both inbound and outbound traffic.

Length	2+4
Value	The attribute is an unsigned Integer representing a volume measured in kilo-bytes(1024 bytes)

1

TLV ID:	3 for VolumeThreshold
Description:	This AVP is optionally present if VolumeQuota is present in a RADIUS Access-Accept message (PPS to SAD direction). It is generated by the PPS and indicates the volume (in octets) that SHALL be consumed before a new quota should be requested. This threshold should not be larger than the VolumeQuota.
Length:	2+4
Value:	The attribute is an unsigned Integer representing a volume measured in kilo-bytes(1024 bytes).

2

TLV ID	4 for DurationQuota
Description	This optional AVP is only present if duration-based charging is used. In RADIUS Access-Accept message (PPS to SAD direction), it indicates the duration (in seconds) allocated for the session by the PPS. It is encoded as an integer. In an on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total duration (in seconds) since the start of the accounting session related to the QuotaID of the PPAQ AVP in which it occurs.
Length	2+4
Value	Unsigned Integer representing seconds.

3

TLV ID	5 for DurationThreshold
Description	This AVP is optionally present if DurationQuota is present in a RADIUS Access-Accept message (PPS to SAD direction). It is generated by the PPS and indicates the duration (in seconds) that SHALL be consumed before a new quota should be requested. This threshold should not be larger than the DurationQuota.
Length	2+4
Value	Unsigned Integer representing seconds.

4

TLV ID	6 for ResourceQuota
Description	This optional AVP is only present if resource-based or one-time charging is used. In the RADIUS Access-Accept message (PPS to SAD direction) it indicates the resources allocated for the session by the PPS. In RADIUS Authorize-Only Access-Request message (SAD to PPS direction), it indicates the resources used in total, including both incoming and outgoing chargeable traffic. In one-time charging scenarios, the subtype represents the number of units to charge or credit the user.
Length	2+4
Value	The attribute is an unsigned Integer representing a resource measured in units.

5

TLV ID	7 for ResourceThreshold
Description	The semantics of this AVP follows those of the VolumeThreshold and DurationThreshold

	AVPs.
Length	2+4
Value	The attribute is an unsigned Integer representing a resource measured in units.

1

TLV ID	8 for Update-Reason
Description	This AVP SHALL be present in the Authorize-Only RADIUS Access-Request message (PPC to PPS direction). It indicates the reason for initiating the on-line quota update operation. Update reasons 6, 7, 8 and 9 indicate that the associated resources are released at the client side, and that therefore the PPS SHALL not allocate a new quota in the RADIUS Access Accept message.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Pre-initialization • 2 = Initial-Request • 3 = Threshold Reached • 4 = Quota Reached • 5 = TITSU Approaching • 6 = Remote Forced Disconnect • 7 = Client Service Termination • 8 = "Access Service" Terminated • 9 = Service not established • 10 = One-time Charging

2

TLV ID	9 for PrepaidServer
Description	This optional AVP indicates the address (IPv4 or IPv6) of the serving PPS. If present, the Home RADIUS server uses this address to route the message to the serving PPS. The attribute may be sent by the Home RADIUS server. Multiple instances of this subtype MAY be present in a single PPAQ AVP. If present in the incoming RADIUS Access-Accept message, the SAD SHALL send this attribute back without modifying it in the subsequent RADIUS Access-Request message, except for the first one. If multiple values are present, the SAD SHALL not change their order.
Length	2 + (4 (IPv4) or 16 (IPv6))
Value	The value of this AVP is encoded as an IPv4 address or an IPv6 address.

3

TLV ID	10 for Service-ID
Description	This value is handled as an opaque string that uniquely describes the service instance to which prepaid metering should be applied. A Service-Id could be an IP 5-tuple (source address, source port, destination address, destination port, protocol). If a Service-ID AVP is present in the PPAQ, the entire PPAQ refers to that service. If a PPAQ does not contain a Service-Id or Rating-Group-ID, then the PPAQ refers to the Access Service (ISF).

Length	2+Variable.
Value	The value field of this AVP is encoded as a string.

1

TLV ID	11 for Rating-Group-ID
Description	This AVP indicates that this PPAQ is associated with resources allocated to a Rating Group with the corresponding ID. This AVP is encoded as a string. A PPAQ SHALL NOT contain more than one Rating-Group-ID.
Length	2+4
Value	Unsigned Integer representing the value of the Rating Group ID.

2

TLV ID	12 for Termination-Action
Description	This AVP describes action to take when the PPS does not grant additional quota.
Length	2+1
Value	Octet Enumeration with the following values: • 0 = Reserved • 1 = Terminate • 2 = Request more quota • 3 = Redirect/Filter

3

TLV ID	13 for Pool-ID
Description	This AVP identifies the resource pool that the quota included in this PPAQ is associated with.
Length	2+4
Value	Unsigned Integer representing a Pool-ID.

4

TLV ID	14 for Pool-Multiplier
Description	The pool-multiplier determines the weight that resources are inserted into the pool that is identified by the accompanying Pool-ID AVP, and the rate at which resources are taken out of the pool by the relevant Service or Rating-Group.
Length	2+4
Value	The attribute consists of a unsigned integer.

5

TLV ID	15 for Requested-Action
Description	This AVP can only be present in messages sent from the PPC to the PPS. It indicates that the user or the PPC desires the PPS to perform the indicated action and to return the result. The PPAQ in which a Requested-Action AVP occurs SHALL NOT contain a QID, and SHALL contain a Service-Identifier that, possibly in combination with other AVPS, can be used by the PPS to uniquely identify the service for which the indicated action is requested.
Length	2+1

Value	Octet enumeration with the following values:
	• 0 = Reserved
	• 1 = Balance Check
	• 2 = Price Enquiry

1

TLV ID:	16 for Check-Balance-Result
Description:	This AVP can only be present in messages sent from the PPS to the PPC. It indicates the balance check decision of the PPS about a previously received Balance Check Request (as indicated in a Requested-Action AVP).
Length:	2+1
Value:	Octet enumeration with the following values:
	• 0 = Success
	• Any other value = Failure

2

TLV ID	17 Cost-Information AVP
Description	This AVP is used in order to return the cost information of a service as specified by the Service-ID, which the PPC can transfer transparently to the end user. This AVP is sent from the PPS to the PPC as a response to a "Price Enquiry", as indicated by the Requested-Action AVP. If Cost-Information is not available for the specified Service-ID, then theCost-Information AVP SHALL NOT appear in the response.
Length	2+9
Value	The value is encoded using fixed encoding and consists of the following fields:
	• 4 octets = Unsigned Integer representing the deci-units of the lowest unit of currency; e.g., a tenths of a cent when the currency is US dollars.
	• 4 octets = Currency code as defined in the ISO-4217 standard
	• 1 or more octets = Carries a UTF8String encoded human readable string that can be displayed to the end user. It specifies the applicable unit to the Cost-Information when the service cost is a cost per unit (e.g., cost of the service is $1 per minute). The Cost-Unit can be minutes, hours, days, kilobytes, megabytes, etc.

3   ## 5.4.2.37 Prepaid Tariff Switching Attribute (PTS)

```
4    0                   1                   2                   3
5    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
6   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7   |RADIUS TYPE 26 |   Length      |              Vendor-Id        |
8   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9   |    Vendor-Id (cont)           |  WiMAX TYPE   |     Length    |
10  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11  | Continuation  |      TLVs
12  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
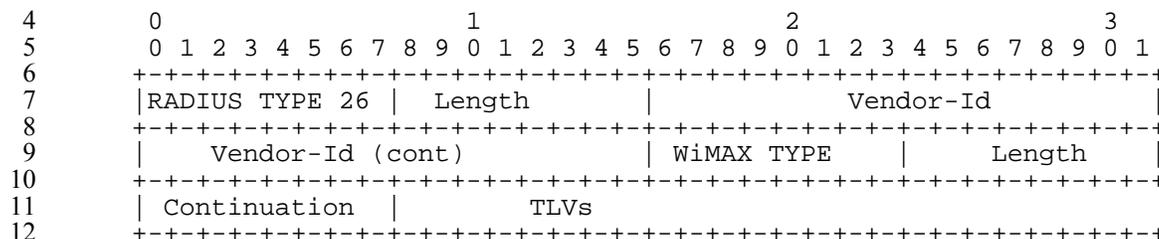
WType-ID	38 for Prepaid Tariff Switching (PTS)
Description	PTS attribute which allows for changeovers from one rate to another during service provision.
	Support for tariff switching is optional for both the PPC and the PPS. PPCs use the flag "Tariff Switching supported" of the PPAC attribute in order to indicate support for tariff

	switching.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

1

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	Quota Identifier	2+Length	1	1	0	0
2	VolumeUsedAfterTariffSwitch	2+4	1	0	0	0
3	TarrifSwitchInterval	2+4	0	0-1	0	0
4	TimeIntervalAfterTarriffSwitchUpdate	2+	0	0-1[a]	0	0

2   **Notes:**

[a]   The PPS SHALL include this AVP if there is another tariff switch period after the period that ends
        as indicated by the TSI attribute.

3

TLV ID	1 for Quota Identifier
Description	Quota Identifier SHALL be included. In an online RADIOUS Access-Request message sent from the PPC to the PPS the Quota Identifier AVP SHALL contain a quota identifier that was previously received from the PPS and SHALL be the same as a quota identifier of one fo the PPAQ attributes included in the same RADIUS message. It is through this Quota Identifier that the PTS attribute is associated with a particular PPAQ.
Length	2+Length of Quota Identifier
Value	Octet String. The Quota Identifier value (most significant bit first)

4

TLV ID	2 for VolumeUsedAfterTariffSwitch
Description	Indicates the volume (in octets) used during a session after the last tariff switch for the service specified via the QID subfield and the accompanying PPAQ attribute.
Length	2+4
Value	Unsigned Integer representing a number of kilo-octets (1024 octets)

5

| **TLV ID**	3 for TarrifSwitchInterval
Description	Indicates the interval (in seconds) between the value of Event-Timestamp RADIUS attribute (see [9]) of the corresponding RADIUS Access-Request message and the next tariff switch condition.
Length	2+4
Value	Unsigned Integer indicating a number of seconds.

6

TLV ID	4 for TimeIntervalAfterTarriffSwitchUpdate

Description	Contains the number of seconds of the tariff period that begins immediately after the period that ends as indicated by the TarriffSwitchInterval sub-TLV. If the TITSU attribute is not present, the PPC assumes that the tariff period which ends as indicated by the TSI attribute lasts until further notice. If TITSU is specified, the PPC SHALL send a quota update before the point in time specified by the TITSU attribute.
Length	2+Length of Quota Identifier
Value	Unsigned Integer measuring a number of seconds.

5.4.2.38 Active-Time

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Vendor-Id (cont)          |  WiMAX TYPE   |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |   Integer
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |
+-+-+-+-+-+-+-+-+
```
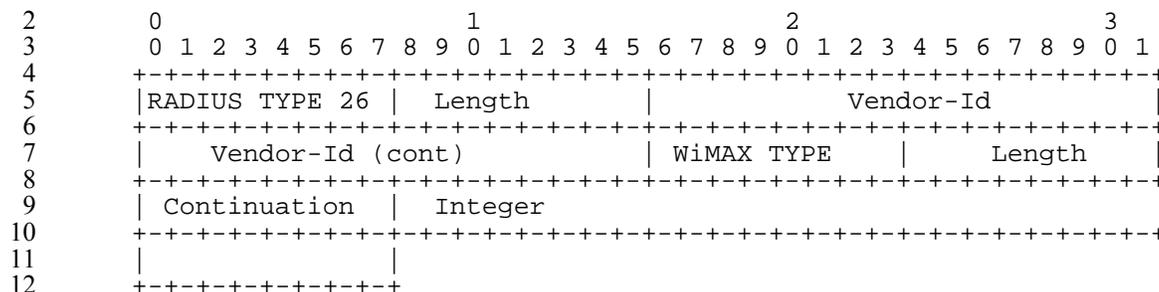
WType-ID	39 for Active-Time
Description	The amount of time the session was not in Idle state.
Length	6 + 3 +4
Continuation	C-bit = 0
Value	Unsigned Integer. The time in seconds.

5.4.2.39 DHCP-RK

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |             Vendor-ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |  WiMAX TYPE   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |     SALT                      |    String     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          String
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	40 for DHCP-RK
Description	The DHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted DHCP-RK.
Continuation	When following the procedures defined in [35] if the resulting encrypted string will be greater then 244 (255-11) octets then the plaintext SHALL be split into two attributes each encrypted separately with the C-bit of the second attribute set to 1 to indicate that this attribute is a fragment of the previous VSA. Otherwise, if no fragmentation is required, then the C-bit is set to '0' zero.
Value	The value consists of 2 octet SALT (see [35]) and String containing the encrypted DHCP-RK formulated as per [35].

1   **5.4.2.40 DHCP-RK-Key-ID**

```
2      0                   1                   2                   3
3      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5      |RADIUS TYPE 26 |     Length      |               Vendor-ID       |
6      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7      |   Vendor-ID (cont)              |    WiMAX TYPE |    Length     |
8      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9      | Continuation  |     Key ID of the DHCP-RK
10     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11                     |
12     +-+-+-+-+-+-+-+-+-+
```
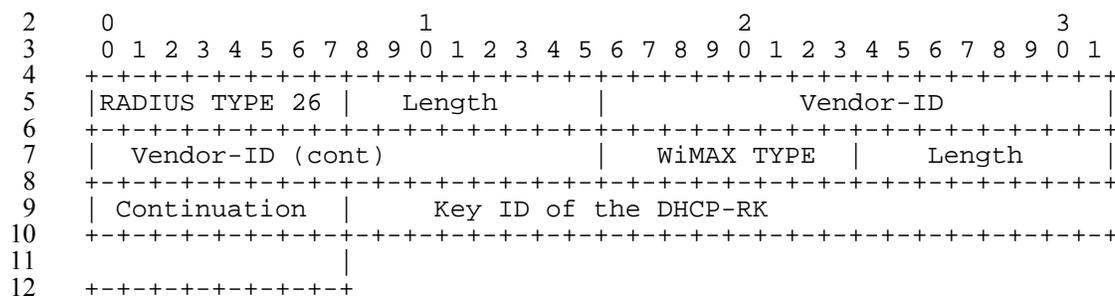
WType-ID	41 for DHCP-RK-Key-ID
Description	An integer number uniquely identifying the DHCP-RK within the scope of a single DHCP server.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

13   **5.4.2.41 DHCP-RK-Lifetime**

```
14     0                   1                   2                   3
15     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
16     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17     |RADIUS TYPE 26 |     Length      |               Vendor-ID       |
18     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19     |   Vendor-ID (cont)              |    WiMAX TYPE |    Length     |
20     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21     | Continuation  |     Lifetime of the DHCP-RK
22     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
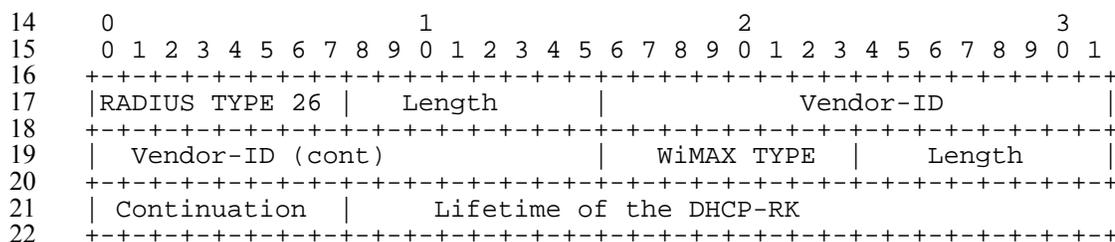
WType-ID	42 for DHCP-RK-Lifetime
Description	Lifetime of the DHCP-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

23   **5.4.2.42 DHCPMSG-Server-IP**

```
24     0                   1                   2                   3
25     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
26     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
27     |RADIUS TYPE 26 |     Length      |               Vendor-ID       |
28     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
29     |   Vendor-ID (cont)              |    WiMAX TYPE |    Length     |
30     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
31     | Continuation  |     DHCP server addr.
32     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
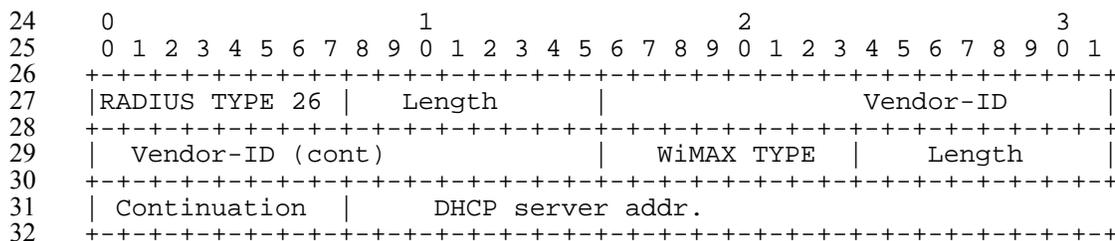
WType-ID	43 for DHCPMSG-Server-IP
Description	The IPv4 address of the DHCP server contained in the DHCPDISCOVER message.
Length	6 + 3 + 4

Continuation	C-bit = 0
Value	Octet string containing an IPv4 address of DHCP server (most significant bit first) to which the DHCPDISCOVER/DHCPREQUEST message was sent.

1 **5.4.2.43 Idle-Mode-Transition**

```
2     0                   1                   2                   3
3     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5    |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
6    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7    |   Vendor-ID (cont)            |  WiMAX TYPE   |    Length     |
8    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9    | Continuation  |    Value      |
10   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
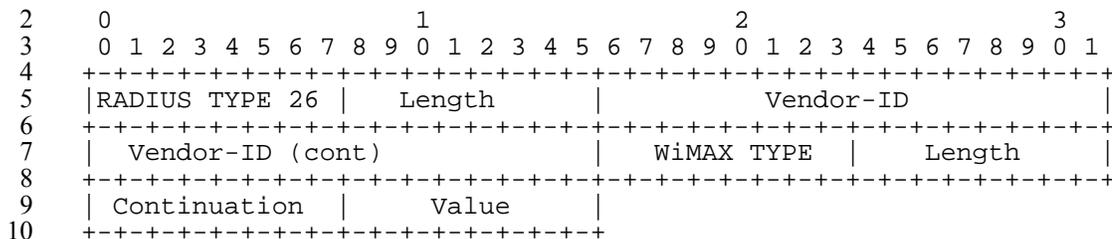
WType-ID	44 for Idle-Mode-Transition
Description	A flag indicating whether the mobile node is in idle or not.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. When set to (1) the MS is in idle mode. When set to (0) the MS is not in Idle mode.

11 **5.4.2.44 NAP-ID**

```
12    0                   1                   2                   3
13    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
14   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
16   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
17   |   Vendor-ID (cont)            |  WiMAX TYPE   |    Length     |
18   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
19   | Continuation  |           Operator ID                        |
20   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
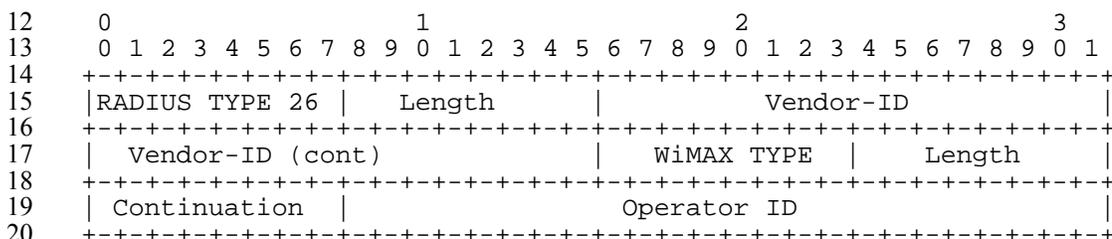
WType-ID	45 for NAP-ID
Description	Uniquely identifies the Network Access Provider.
Length	6 + 3 + 3
Continuation	C-bit = 0.
Value	Octet-String (3 Octets) representing an operator identifier.

21 **5.4.2.45 BS-ID**

```
22    0                   1                   2                   3
23    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
24   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
25   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
26   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
27   |   Vendor-ID (cont)            |  WiMAX TYPE   |    Length     |
28   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
29   | Continuation  |           Operator ID                        |
30   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
31   |                 BS - ID                      |
32   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
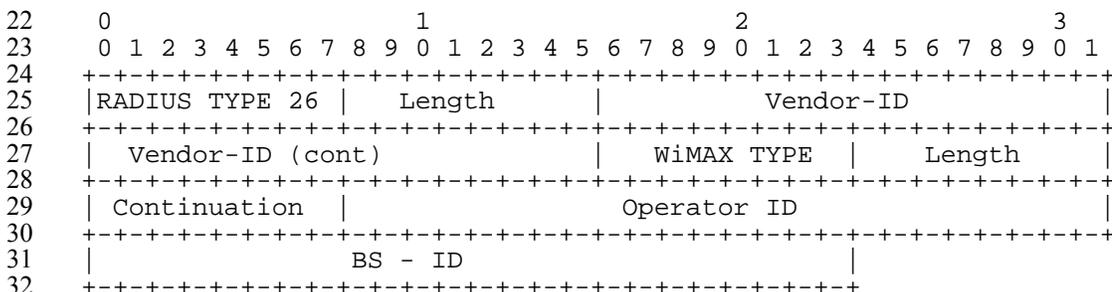
WType-ID	46 for BS-ID
Description	Uniquely identifies a NAP and a Base Station within that NAP.
Length	6 + 3 + 6
Continuation	C-bit = 0
Value	Octet-String (6 Octets). Representing NAP operator identifier (first 3 Octets) and the Base Station ID (next 3 Octets)

5.4.2.46 Location

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |            Vendor-ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |              Location
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
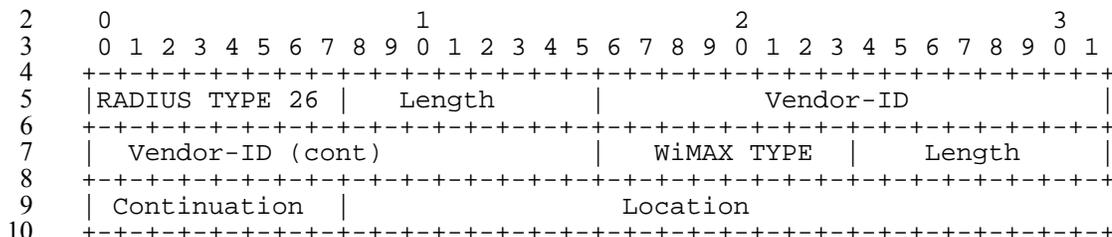
WType-ID	47 for Location
Description	Location of the ASN.
Length	6 + 3 + Length of Location (>0)
Continuation	C-bit = 0 or 1
Value	Octet-String representing location. Format is TBD

5.4.2.47 Acct-Input-Packets-Gigaword

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |            Vendor-ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |              Location
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
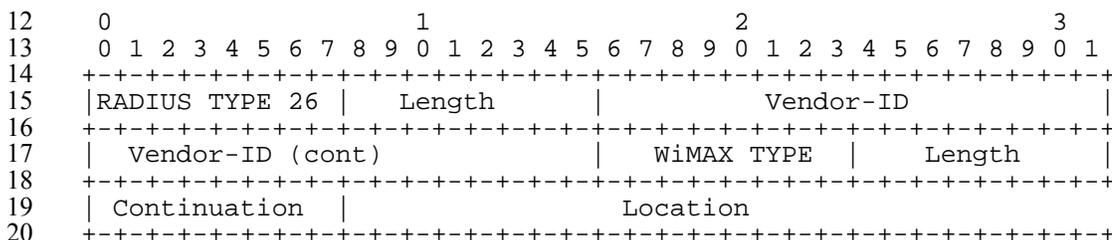
WType-ID	48 for Acct-Input-Packets-Gigaword
Description	Number of packets incremented each time Acct-Input-Packets(47) overflows.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing 2^{32} packets counts.

5.4.2.48 Acct-Output-Packets Gigaword

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |            Vendor-ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)            |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |              Location
```
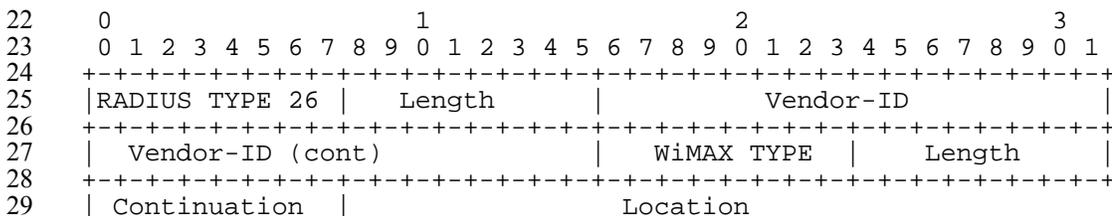
1
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	49 for Acct-Output-Packets-Gigaword
Description	Number of packets incremented each time Acct-Output-Packets(48) overflows.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing 2^{32} packets counts.

2 ### 5.4.2.49 Flow Description

```
3   0                   1                   2                   3
4   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
5   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
6   |RADIUS TYPE 26 |    Length     |             Vendor-ID         |
7   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
8   |   Vendor-ID (cont)            |   WiMAX TYPE  |    Length     |
9   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
10  | Continuation  |             Flow Description
11  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
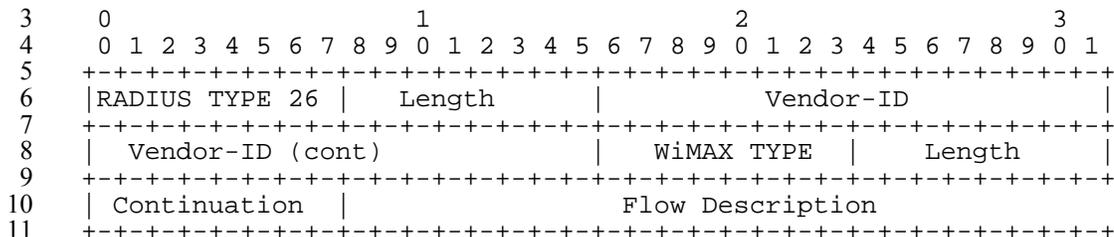
| WType-ID	50 for Flow Description
Description	Describes a flow classifier.
Length	6 + 3 + length of Flow Classifier (>0)
Continuation	C-bit = 0
Value	Octet-String formatted as per IPFilterRule (see [48]).

12 ### 5.4.2.50 BU-CoA-Ipv6

```
13  0                   1                   2                   3
14  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
15  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16  |RADIUS TYPE 26 |    Length     |             Vendor-ID         |
17  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
18  |   Vendor-ID (cont)            |   WiMAX TYPE  |    Length     |
19  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20  | Continuation  |             BU-CoA-IPv6
21  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
22
23  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
24
25  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
26
27  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
28                     |
29  +-+-+-+-+-+-+-+-+-+-+
```
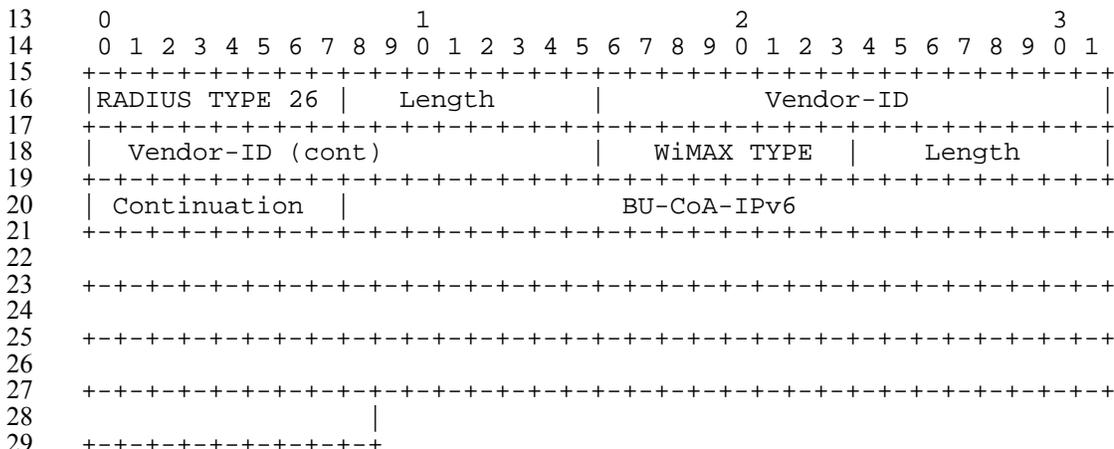
| WType-ID	51 for BU-CoA-IPv6
Description	The CoA from the BU message.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet-String representing an IPv6 address most significant octet first.

5.4.2.51 DNS

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length       |            Vendor-ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)              |   WiMAX TYPE  |    Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation   |                 DNS
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          |
+-+-+-+-+-+-+-+-+-+-+
```
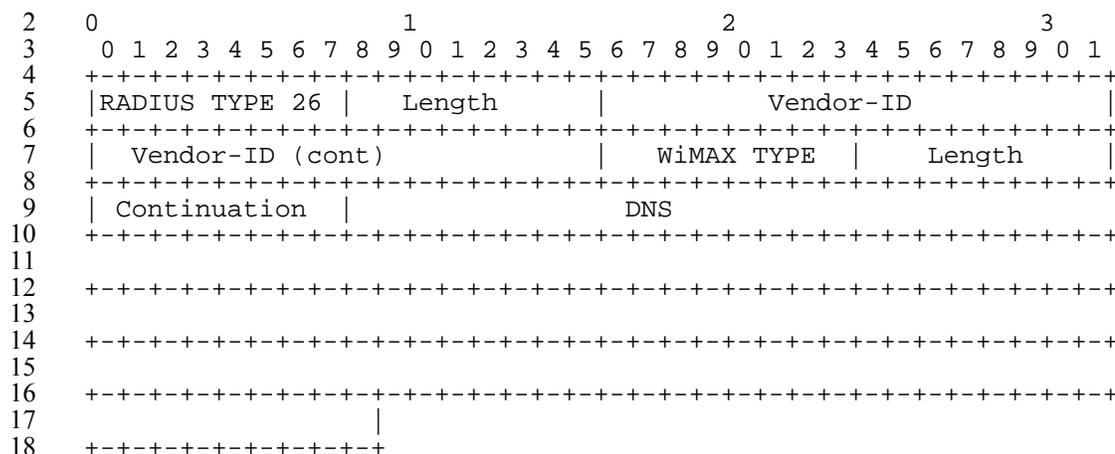
| WType-ID	52 for DNS
Description	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet-String representing an IPv4 or IPv6 address most significant octet first.

5.4.2.52 Hotline-Profile-ID

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length       |            Vendor-ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)              |   WiMAX TYPE  |    Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation   |                 String
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	53 for Hotline-Profile-ID
Description	A unique identifier (relative to the HCSN) of a hotline profile to be applied to this session.
Length	6 + 3 + length of octet-string.
Continuation	C-bit = 0
Value	String representing a hotline profile formatted as follows: realm + "/" + profile-id-string Where: • Realm is the Fully Qualified Domain Name of the operator that is asserting the Hotline profile; and • Profile-id-string is operator specific label for the hotline profile to be applied at the by the hotlining device.

1 **5.4.2.53 HTTP-Redirection-Rule**

```
2   0                   1                   2                   3
3   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5   |RADIUS TYPE 26 |    Length       |            Vendor-ID        |
6   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7   |   Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
8   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9   | Continuation  |                   string
10  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11
```
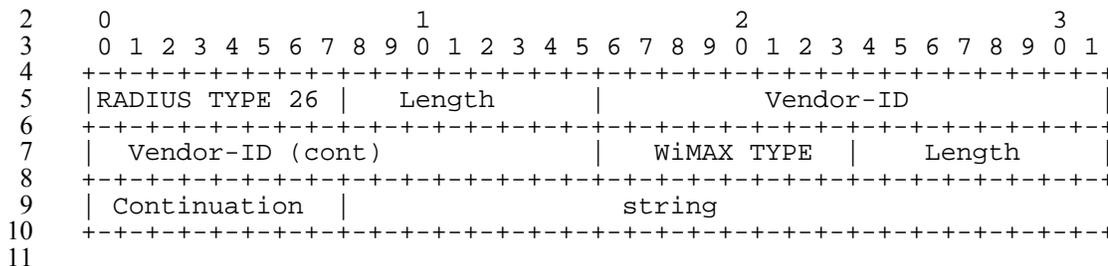
WType-ID	54 for HTTP-Redirection-Rule
Description	An HTTP redirection rule. When the classifier matches the NAS responds back with the specified URL causing the client's browser to be redirected to that URL.
Length	6 + 3 + length of rule.
Continuation	C-bit = 0
Value	An string formatted as per IPFilterRule specified by [48] with the following exception: The action portion of the rule SHALL follow the following:

| Action Keyword	Description
"redirect" url	If the rule matches then redirect packets that match the rule to the specified URL encoded as per RFC2396
"pass"	If the rule matches then the HTTP request is allowed to continue through. The is no url.
"flush"	Has no other elements in the rule. The hotlining device SHALL flush all HTTP-Redirection rules received from the HAAA.

12 **5.4.2.54 IP-Redireciton-Rule**

```
13  0                   1                   2                   3
14  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
15  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16  |RADIUS TYPE 26 |    Length       |            Vendor-ID        |
17  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
18  |   Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
19  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20  | Continuation  |                   string
21  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
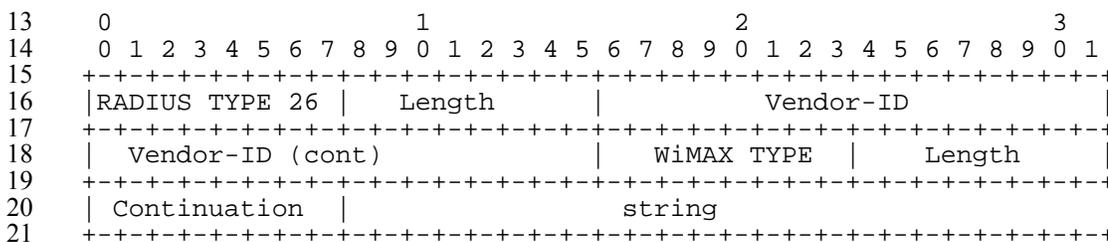
WType-ID	55 for IP Redirection Rule.
Description	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.
Length	6 + 3 + length of rule
Continuation	C-bit = 0
Value	An string formatted as per IPFilterRule specified by [48] with the following exception: The action portion of the rule SHALL follow the following:

Action Keyword	Description
"redirect" IP[port]	If the rule matches then redirect packets that match the rule to the specified IP address and optional port.

|	"flush"	Has no other elements in the rule. The hotlining device SHALL flush all HTTP-Redirection rules received from the HAAA.

5.4.2.55 Hotline-Session-Timer

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length         |              Vendor-ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)                |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |            unsigned integer
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |
+-+-+-+-+-+-+-+-+
```

| WType-ID	56 for Hotline-Session-Timer
Description	The length of time in seconds the session can remain hotlined. If not specified the length of time the session is hotlined is determined by the Session-Time and Termination-Action attributes. Session-Time with Termination-Action set to Default(0) SHALL override this timer. If Session-Time with Termination-Action is set to RADIUS-Request(1), the NAS SHALL reauthenticate without resetting the value of Hotline-Session-Timer. Upon successful reauthentication, if the NAS receives a new Hotline-Session-Timer value, the NAS SHALL terminate the session based on the value specified by the received attribute.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing a time in seconds. A value of zero means infinity.

5.4.2.56 NSP-ID

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |    Length         |              Vendor-ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Vendor-ID (cont)                |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |            Operator ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
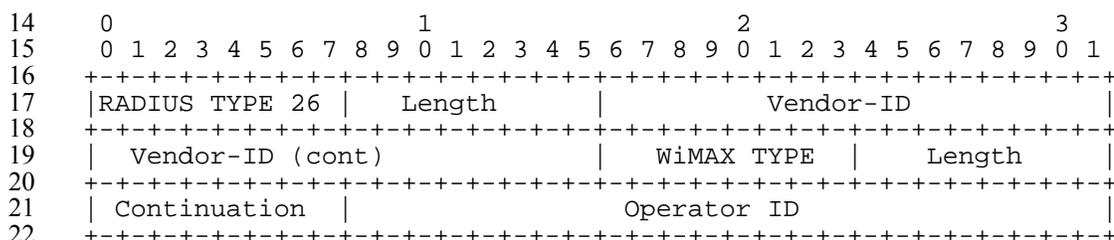
WType-ID	57 for NSP-ID
Description	Uniquely identifies the Network Service Provider.
Length	6 + 3 + 3
Continuation	C-bit = 0.
Value	Octet-String (3 Octets) representing an operator identifier.

1 **5.4.2.57 HA-RK-Key-Requested**

```
2    0                   1                   2                   3
3    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
4    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
5    |RADIUS TYPE 26 |    Length     |            Vendor-ID          |
6    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
7    |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
8    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
9    | Continuation  |            Integer
10   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11   |               |
12   +-+-+-+-+-+-+-+-+
```
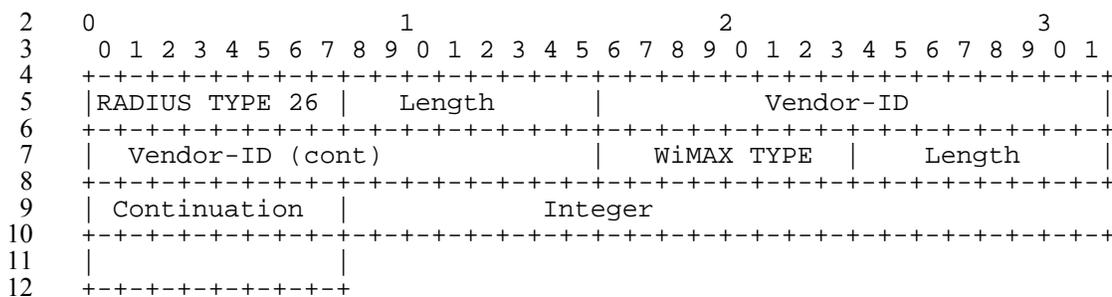
WType-ID	58 for HA-RK-Key-requested
Description	The amount of time the session was not in Idle state.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer. The enumeration is defined as follows : 0 = don't need HA-RK-key 1 = need HA-RK-key

13

14 **5.4.2.58 x FA-RK-SPI**

```
15   0                   1                   2                   3
16   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
17   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
18   |RADIUS TYPE 26 |    Length     |            Vendor-ID          |
19   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
21   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
22   | Continuation  |               TLV
23   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
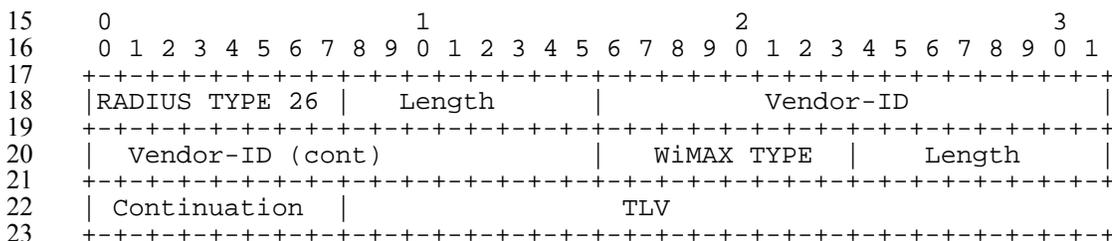
WType-ID	x for FA-RK-SPI
Description	The SPI used for the FA-RK.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

24

1 6. Data Plane

2 The data plane consists of the transport encapsulation of the user payload within the mobile WiMAX network. Basic
3 considerations are provided in chapter 7.11 of the Stage 2 documentation. Stage 3 section 6 amends the Stage 2
4 description by providing detailed information on the applied protocols.

5 Release 1.0.0 of the mobile WiMAX network specification assumes a routed transport infrastructure for all of the
6 exposed network reference points. Therefore user payload packets are encapsulated within IP packets when they are
7 carried over the reference points R3, R4 and R6. User payload packets are encapsulated in 802.16 MAC frames
8 when carried over R1.

9
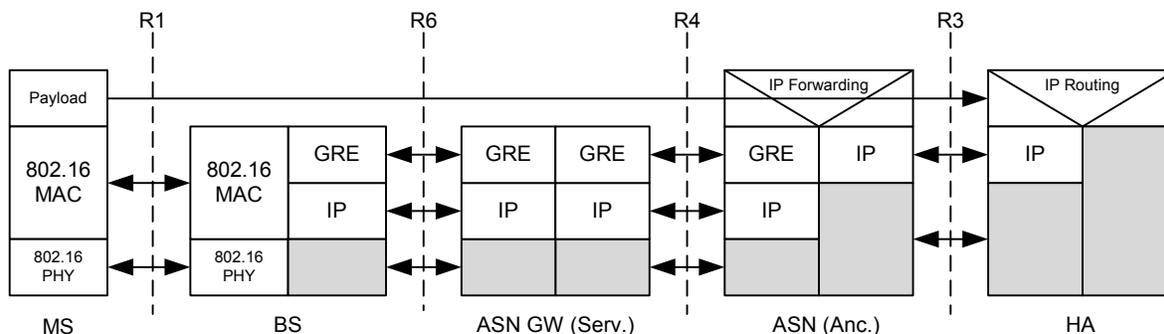
10 **Figure 6-1 – Data Plane with R4 and R6**

11 If the payload contains Ethernet framing, Ethernet frames coming from R1 SHALL NOT be terminated before the
12 (anchor) ASN.

13 No dedicated data plane protocol is specified for R2 or R5. User payload is transferred without any encapsulation
14 according to the source and destination addresses in the user payload packets.

15 6.1 Encapsulation on R3

16 6.1.1 IP in IP Encapsulation

17 According to [15] IP-in-IP encapsulation SHALL be applied for transport of user payload over the reference point
18 R3. The encapsulation SHALL be done in accordance to RFC2003. Reverse tunneling SHALL be done according to
19 RFC3024.

20 6.1.2 GRE Encapsulation

21 As an option in [15], GRE (Generic Route Encapsulation) encapsulation MAY be applied for transport of user
22 payload over the reference point R3. GRE is specified in RFC2784 and extended in RFC2890 by the Key option as
23 well as the Sequence Number option. Neither the Key option nor the Sequence Number options SHALL be applied
24 in Release 1.0.0 but MAY be used in later releases. Therefore the 'Sequence Number Present' bit as well as the 'Key
25 Present' bit in the GRE header is set to 0 in Release 1.0.0.

26 6.2 GRE Encapsulation on R4 and R6

27 GRE as specified by RFC2784 and extended by RFC2890 SHALL be used as the tunneling protocol for the data
28 plane over the reference points R4 and R6. GRE allows for tunneling of IP packets, Ethernet frames as well as
29 WiMAX specific payload frames over an IP-based transport infrastructure. The same encapsulation protocol is
30 applied on R4 and R6, regardless of the type of user payload, i.e. IPv4, IPv6, IPv4oETH, IPv6oETH, plain Ethernet
31 or WiMAX specific payload frames, and regardless of the granularity of the tunnels, i.e. per MS granularity or per
32 service flow granularity.

1
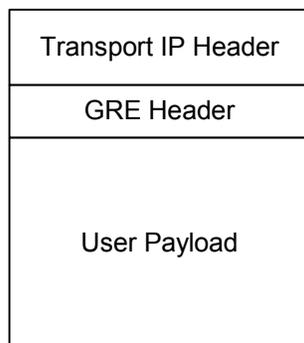
2   **Figure 6-2 – GRE Encapsulation**

3   The GRE protocol according to RFC2784 SHALL be used without the Checksum option. Therefore the Checksum
4   Present bit is set to zero.

5   RFC2890 provides two optional extensions, the Key option as well as the Sequence Number option. While the Key
6   option SHALL be applied on R4 and R6 for providing the Data Path ID of the tunnel, the Sequence Number option
7   MAY be provided for handover optimizations. When present, the Sequence Number field is signaled by the
8   'Sequence Number Present' bit in the GRE header.

```
9         0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
10       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
11       |0|0|1|S| Reserved0       |0 0 0|            Protocol Type       |
12       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
13       |                        Key = Data Path ID                     |
14       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
15       |                    Sequence Number (Optional)                 |
16       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
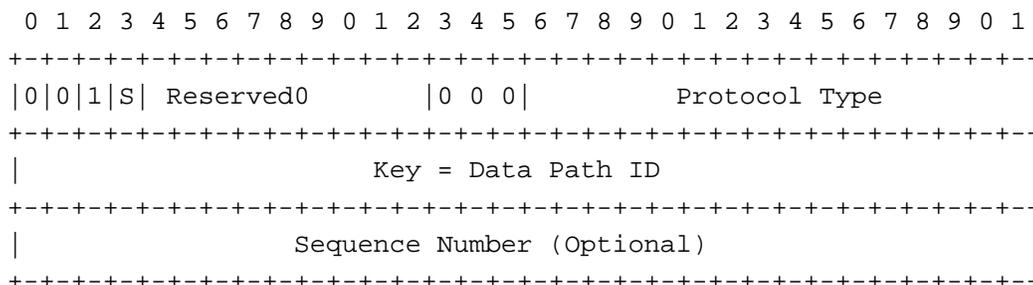
17   **Figure 6-3 – GRE Header Format**

18   **Table 6-1 – GRE Header Field Definitions**

Field	Type	Description
Protocol Type	16bit ETHER TYPE	Defines protocol type of user payload. The following values are assigned according to http://www.iana.org/assignments/ethernet-numbers: • IPv4: 0x0800 • IPv6: 0x86DD • Ethernet: 0x6558 • For the WiMAX Payload Type, 0xFFFF SHALL be used.
Data Path ID	32bit UNSIGNED	Value assigned by the Data Path Function uniquely identifies a particular tunnel for user payload Granularity of tunnels is defined and handled by the DPF.
Sequence Number	32bit UNSIGNED	Optional value for enumerating sequence of user payload packets; may be used for handover enhancements. If the Sequence Number is present in the GRE header, the S-Bit is set to '1'

1   WiMAX Payload Type may be used to indicate if the upper protocol is PHS suppressed, ROHC compressed or
2   uncompressed IP packet..

6.3   Convergence Sublayer on R1

4   IEEE802.16 convergence sublayers SHALL be applied to the particular user payload for encapsulation and transport
5   over R1. In the BS, the Data Path ID in the GRE header and optionally the packet classification process are used to
6   determine the addressed MSID as well as the particular SFID.

7   If classification is taking place in the ASN-GW, the BS maps each Data Path ID into a particular MSID and SFID.
8   In this case the mapping table in the BS is established and maintained by the Data Path Function.

6.3.1   IP-CS

10   IP datagrams going upstream over R1 are encapsulated in the BS as user payload in GRE packets and transferred
11   over R6 and eventually R4 to the anchor ASN-GW/ASN. IP datagrams send downstream from the anchor ASN-GW
12   within the payload of GRE packets are extracted in the BS out of the GRE packet and forwarded over R1 to the MS.
13   All datagrams transferred upstream over R1 SHOULD be forwarded over R6, and all packets transferred
14   downstream over R6 SHOULD be forwarded over R1.

6.3.2   IPoETH-CS

16   Ethernet frames going upstream over R1 are encapsulated in the BS as user payload in GRE packets and transferred
17   over R6 and eventually R4 to the anchor ASN-GW/ASN. Ethernet frames send downstream from the anchor ASN-
18   GW within the payload of GRE packets are extracted in the BS out of the GRE packet and forwarded over R1 to the
19   MS. All Ethernet frames transferred upstream over R1 SHOULD be forwarded over R6, and all frames transferred
20   downstream over R6 SHOULD be forwarded over R1.

21   Ethernet behavior in the user plane SHALL be realized by a multiport bridge in the anchor ASN-GW/ASN with a
22   single port for each of the MSs. Ethernet frames are extracted out of the GRE packets before forwarding the frames
23   into the particular bridge port. To allow DataPathID based identification of particular port. the granularity of the
24   GRE tunnels over R4 or R6 SHALL NOT be per-BS. The MSs are connected to radio side ports of the bridge while
25   the FA/Access Router is connected to a network side port of the bridge.

26   Downstream Ethernet frames coming out of bridge ports are encapsulated as user payload in GRE packets and
27   forwarded over R6 or R4 towards the MS belonging to the port of the bridge. If multiple CIDs exist in downstream
28   for a particular MS, classification SHALL be performed in the scope of the CIDs belonging to the MS.
29   Classification takes place in the (anchor) ASN/GW before encapsulating the Ethernet frames in GRE packets in the
30   case of per-SF granularity, or in the BS in the case of per-MS granularity of the GRE tunnels. After a handover the
31   tunnels MAY be extended over R4 from the anchor ASN-GW/ASN to the serving ASN-GW/ASN.

32   Forwarding and processing of the Ethernet frames in the bridge SHALL be performed according to [IEEE802.1D]
33   ammended by [IEEE802.16k]. All multicast and multicast control messages SHALL be processed in the bridge
34   according to [RFC4541]. Broadcasting messages to all radio side ports of the bridge and direct host-to-host
35   communication between radio side ports of the bridge SHOULD be prevented.

36   Further information about processing of multicast and broadcast messages in such a bridge can be found in [draft-
37   ietf-16ng-ip-over-ethernet-over-802.16-xx.txt]."

38   Figure 6-4 shows the adoption of the IPoETH-CS link model for the mobile WiMAX network architecture.
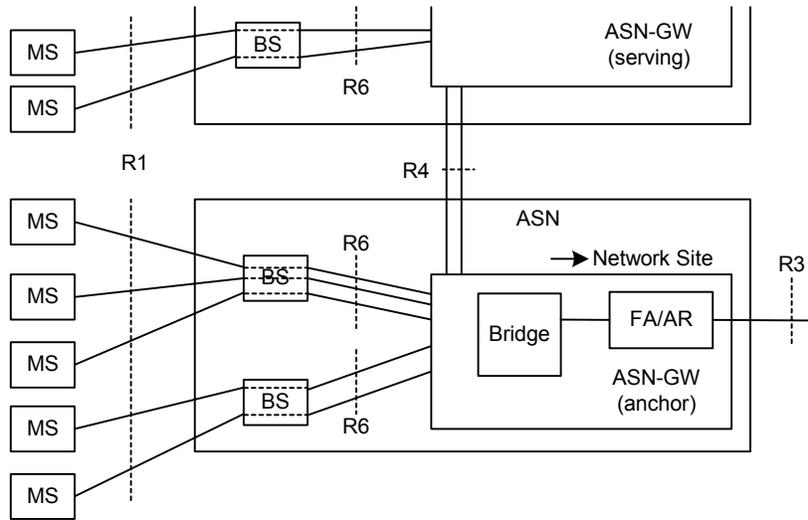
1

2   **Figure 6-4 – IPoETH-CS Link Model in the WiMAX Architecture**

1 # 7. ASN Profile Mappings

2 ## 7.1 ASN Profile A

3 In the Profile A, ASN GW SHALL control the overall HO procedure. HO Control functions can be located at either
4 Serving ASN GW or Anchor ASN GW.

5 For more detailed information about Profile A specification, refer to Sec 8.1 of Stage 2 WiMAX Network
6 Specification.

7 ### 7.1.1 RRM

8 #### 7.1.1.1 R6: Per-BS Spare Capacity Reporting Procedure

9 This procedure MAY be used by a Serving ASN-GW to retrieve information about the current load of all the Base
10 Stations in the ASN which are reporting to that Serving ASN-GW and which MAY become candidate Target BSs
11 (TBSs) for Handover decisions.

12
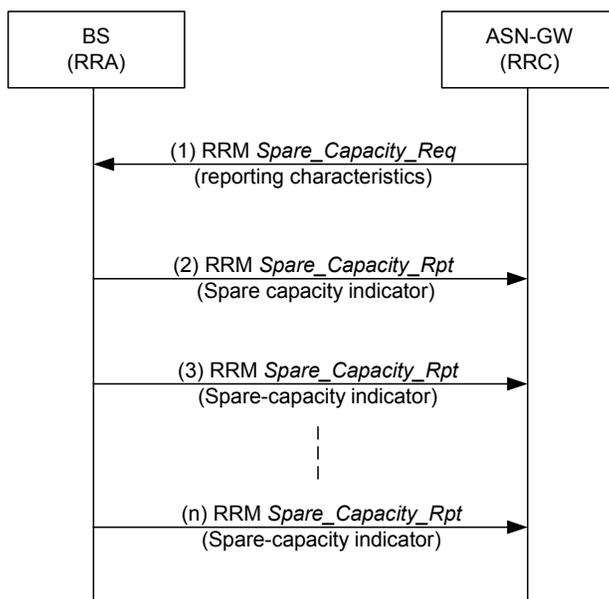
13 **Figure 7-1 – Per-BS Spare Capacity Reporting Procedure**

14 **STEP 1**

15 ASN-GW sends an RRM R6 *Spare_Capacity_Req* to the BS, requesting it to indicate its available radio resources
16 once, or periodically, or event driven.

17 **STEP 2, 3, …, n**

18 BS sends RRM R6 *Spare_Capacity_Rpt* to ASN-GW, either in direct response to the Request, or subsequently in
19 response to predefined events.

20 #### 7.1.1.1.1 R6 Messages for Per-BS Spare Capacity Reporting Procedure

21 The message definition for the RRM R6 *Spare_Capacity_Req* message is the same as the corresponding R4 message
22 definition as specified in section 4.9.3.1.1 – except that on R6, the RRM R6 *Spare-Capacity-Req* message sent from
23 ASN GW to a BS can include a single BS only.

1   **Table 7-1 – RRM R6 Spare_Capacity_Req, Profile A**

IE	Reference	M/O	Notes
RRM Spare Capacity Report Type	5.3.2.164	M	
BS ID	5.3.2.25	M	Identifier of the BS whose Spare Capacity SHALL be reported. In the message from ASN GW to a BS, a single BS only can be included.
RRM Reporting Characteristics	5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. If the optional reporting characteristics field is not included, then the *Spare_Capacity_Rpt* SHALL be sent only once by the reporting entity. – TLV may be included based on local RRC policy. Decision to include this TLV is implementation specific.
RRM Averaging Time T	5.3.2.158	O	The Time T is used by BS (RRA) as the measurement interval for producing the information requested by RRC. – If omitted, the BS SHALL apply a default value.
RRM Reporting Period P	5.3.2.158	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at $T + P$, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
RRM Absolute Threshold Value J	5.3.2.157	O	The threshold value J is used by BS (RRA) as the absolute threshold for reporting.
RRM Relative Threshold RT	5.3.2.161	O	The threshold value RT is used by BS (RRA) to keep track of the threshold from the last measurement period.

2   The message definition for the RRM R6 *Spare_Capacity_Rpt* message is the same as the corresponding R4 message
3   definition as specified in section 4.9.3.1.1.

4   **7.1.1.2   R6: Per-MS PHY Channel Measurement Procedure**

5   This procedure MAY be used by an ASN-GW to retrieve information about the radio resources used by a specific
6   MS. The information MAY help the ASN-GW to detect the necessity of taking actions for resource efficiency
7   improvement, e.g.

8   •   QoS parameter adjustment for certain Service Flows, or

9   •   Triggering a handover.

10   Note: This procedure MAY also be used for conveying neighbor BS information from BS to ASN GW which has
11   been reported from MS to BS in the MOB_SCN-REPORT ([802.16e-2006], section 6.3.2.3.50.)

1
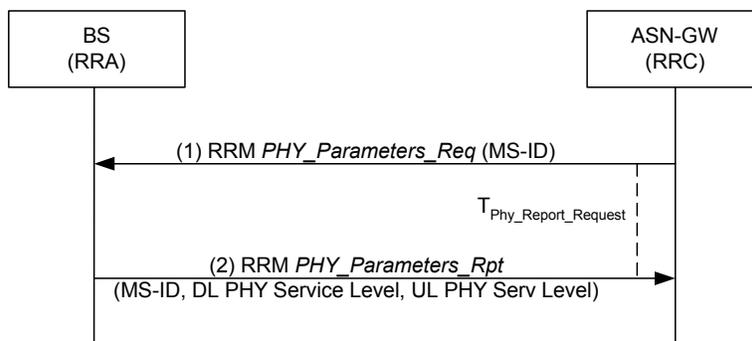
2 **Figure 7-2 – Per-MS PHY Channel Measurement Procedure**

3 **STEP 1**

4 ASN-GW (RRC) sends an RRM R6 *PHY-Parameters_Req* to the BS, requesting it to report the PHY Service Level
5 (bit/Hz) and other link quality parameters for a specific MS which is currently in active state. This procedure
6 SHALL be associated with a timer as specified in section 7.1.1.2.2.

7 **STEP 2**

8 BS sends an RRM R6 *PHY_Parameters_Rpt* to the ASN-GW, reporting the PHY Service Level (bit/Hz) and other
9 link quality parameters for a specific MS.

10 **7.1.1.2.1   R6 Messages for Per-MS PHY Channel Measurement Procedure**

11 This section provides the message definitions for the R6 messages in support of the Per-MS PHY Channel
12 Measurement Procedure. See sections 5.2.6.6 and 5.3 for message and TLV definitions.

13 **Table 7-2 – RRM R6 PHY_Parameters_Req**

IE	Reference	M/O	Notes
VOID			This message has no procedure specific TLVs. The MSID in the message header SHALL be used.

14 **Table 7-3 – RRM R6 PHY_Parameters_Rpt**

IE	Reference	M/O	Notes
MSID	5.3.2.102	O	
RRM BS-MS PHY Quality Info	5.3.2.160	M	
>Serving/Target Indicator	5.3.2.181	M	Set to Serving
>Round Trip Delay	5.3.2.156	M	Round Trip Delay (RTD) between the MS and the Serving BS
>DL PHY Quality Info	5.3.2.60	M	Downlink PHY Quality between the MS and the Serving BS
>DL PHY Service Level (DL PSL)	5.3.2.61	M	Channel rate available for the MS calculated as a multiple of 1/32 of nominal bandwidth in the correspondent direction assuming 1 bit/Hz. PSL = 1 means 1/32 bit/Hz; PSL = 32 means 1 bit/Hz; PSL = 96 means 3 bit/Hz. For example, if channel

IE	Reference	M/O	Notes
			bandwidth is 10 MHz, value PSL=4 means 4*1/32*10 Mbps = 1.25 Mbps. - (Number of subchannels in different OFDMA modes is multiple of 16 or 32; highest modulation (QAM64) provides 3 bits/Hz).
>UL PHY Quality Info	5.3.2.197	M	
>UL PHY Service Level (UL PSL)	5.3.2.198	M	Channel rate available for the MS calculated as a multiple of 1/32 of nominal bandwidth in the correspondent direction assuming 1 bit/Hz. PSL = 1 means 1/32 bit/Hz; PSL = 32 means 1 bit/Hz; PSL = 96 means 3 bit/Hz. For example, if channel bandwidth is 10 MHz, value PSL=4 means 4*1/32*10 Mbps = 1.25 Mbps. - (Number of subchannels in different OFDMA modes is multiple of 16 or 32; highest modulation (QAM64) provides 3 bits/Hz).
BS Info (Target, one or more)	5.3.2.26	O	Number of Neighbor BSs reported by the mobile in the scanning report
>Serving/Target Indicator	5.3.2.181	O	Set to Target
>DL PHY Quality Info	5.3.2.60	O	Downlink PHY Quality between the MS and the Neighbor BS. Included based on local BS policy. Decision to include this TLV is implementation specific.
Failure Indication	5.3.2.69	O	"Failure Indication" is to be used for exceptional cases; e.g., the indicated BS ID does not exist, RRC cannot route the request to the indicated BS ID, the indicated BS is out of service for the time being.

1 **7.1.1.2.2 PHY Parameter Report Timers and Timing Considerations**

2 This section identifies timer entities defined for PHY Parameter Reporting procedure.

3 The parameter reporting procedure shown in Figure 7-2 employs one timer that is defined as follows:

4 • PHY Report Timer ($T_{Phy\_Report\_Timer}$) – This timer is maintained by the RRC to monitor PHY Report. It
5 monitors the period PHY Parameter request and the PHY Parameter response by the radio resource agent.

6 Table 7-4 shows the default value of timers and also indicates the range of the recommended duration of these
7 timers. Note that these values are provisioned in Release 1.0.0.

8 **Table 7-4 – Timer Values**

Timer	Default Value (ms)	Criteria	Maximum Timer Value (ms)
PHY Parameters Req Period ($T_{Phy\_Report\_Timer}$)	TBD	TBD	TBD

9 Table 7-5 shows the details on timer expiry causes, reset triggers and corresponding actions.

1

Table 7-5 – Timer Max Retry Conditions

Timer	Entity	Reset(s)	Cause(s)	Action(s)
T$_{Phy\_Report\_Timer}$	RRC	RRM: PHY Parameters	Message gets lost due to congestion in the backhaul Badly formatted *Spare_Capacity_Req* Base station overloaded to process the PHY Parameter Request message	If the last retry fails, the RRC takes an action based on the local policy

2   **7.1.1.3   R6: RRM Neighbor BS Resource Status Update Procedure**

3   This procedure MAY be used by an ASN-GW to inform a BS about the current load situation of its neighbor BSs.
4   The BSs can use this, among others, to update the "Available Radio Resource" indicator which is an optional
5   parameter in the MOB_NBR-ADV broadcast message (as specified in Draft Amendment 802.16g).

6   **Entities:**

7   BS (RRA), ASN-GW (RRC)
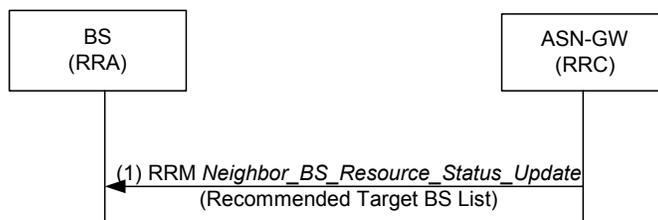
8

9   **Figure 7-3 – Neighbor BS Resource Status Update Procedure**

10   **STEP 1**

11   ASN-GW sends an RRM R6 *Neighbor_BS_Resource_Status_Update* to the BS.

12   **7.1.1.3.1   R6 Messages for RRM Neighbor BS Resource Status Update Procedure**

13   This section provides the message definitions for the R6 messages in support of the RRM Neighbor BS Resource
14   Status Update Procedure. See sections 5.2.6.6 and 5.3 for message and TLV definitions.

15   **Table 7-6 – RRM R6 Neighbor_BS_Resource_Status_Update**

IE	Reference	M/O	Notes
RRM BS Info (Target, one or more)	5.3.2.159	M	Number of Neighbor BSs which SBS SHOULD include in MOB_NBR-ADV message.
> Serving/Target Indicator	5.3.2.181		Set to Target
>BS ID	5.3.2.25	M	
>Available Radio Resource DL	5.3.2.22	M	
>Total Slots DL	5.3.2.191	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Available Radio	5.3.2.23	M	

IE	Reference	M/O	Notes
Resource UL			
>Total Slots UL	5.3.2.192	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>DCD Configuration Change Count	5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>UCD Configuration Change Count	5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>DCD Settings	5.3.2.49	O	This TLV may be used only while DCD configuration change count is presented. This IEEE802.16e-2005 defined TLV. The DCD_settings is a TLV value that encapsulates a DCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. The DCD settings fields SHALL contain only neighbor's DCD TLV values that are different from the serving BS corresponding values. For values that are not included, the MS SHALL assume they are identical to the corresponding values of the serving BS. The duplicate TLV encoding parameters within a Neighbor BS SHALL not be included in DCD setting. *Note 1
>UCD Settings	5.3.2.195	O	This TLV may be used only while UCD configuration change count is presented. This IEEE802.16e-2005 defined TLV. The UCD_settings is a compound TLV value that encapsulates a UCD message that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS uplink. The UCD settings fields SHALL contain only neighbor's UCD TLV values that are different from the serving BS's corresponding values. For values that are not included, the MS SHALL assume they are identical to the serving BS's corresponding values. *Note 1

Note 1: See reference: 802.16e-2005, the TLV definition of section 6.3.2.3.47 (MOB_NBR-ADV message).

7.1.1.4   R6: Per-BS Radio Configuration Update Reporting Procedure

This procedure MAY be used by a BS to report some critical radio resource configuration update to the serving GW(RRC), such as DCD, UCD burst profile changes.

1
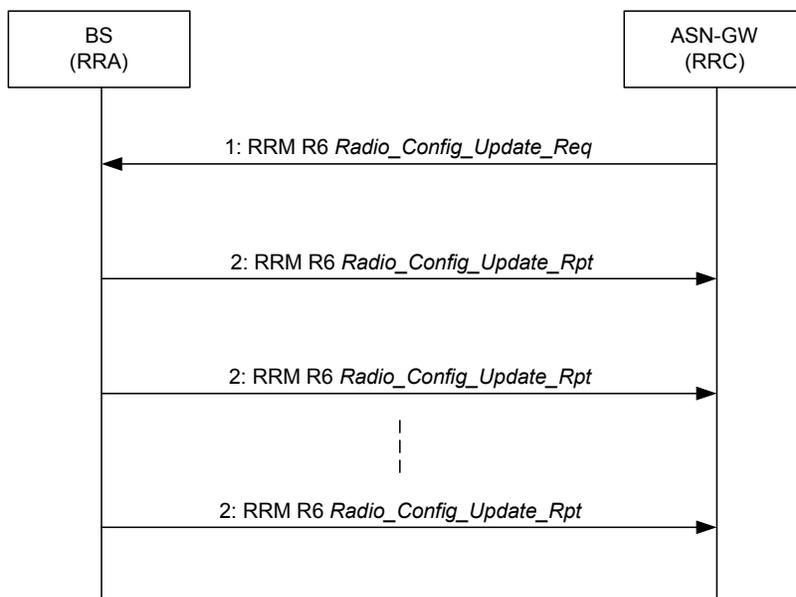
Figure 7-4 – Per-BS Radio Configuration Update Reporting Procedure

3 **STEP 1**

4 ASN-GW sends an RRM R6 *Radio_Config_Update_Req* to the one or multiple BS(s), requesting it to indicate its
5 available radio configuration changes by event driven.

6 **STEP 2 …, n**

7 BS sends RRM R6 *Radio_Config_Update_Rpt* to ASN-GW, either in direct response to the Request, or
8 subsequently in response to predefined events.

9 **7.1.1.4.1 R6 Messages for Per-BS Radio Configuration Update Procedure**

10 The message definition for the RRM R6 *Radio_Config_Update_Req* messages is the same as the corresponding R4
11 message definition as specified in section 4.9.3.2.1 – except that on R6, the RRM R6 *Radio_Config_Update_Req*
12 message sent from ASN GW to a BS can include a single BS only.

13 **Table 7-7 – RRM R6 Radio_Config_Update_Req**

IE	Reference	M/O	Notes
BS ID (one or more)	5.3.2.25	M	Identifier of the BS whose Radio-Configuration SHALL be reported. In the message from ASN GW to a BS, a single BS only can be included.
RRM Reporting Characteristics	5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. In this message, only Bit#0 (periodic reporting) and Bit#1 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset. If *Radio_Config_Update_Rpt* needs to be sent based on multiple events, then the corresponding bits have to be set to 1. If the optional reporting characteristics field is not specified, then the *Radio_Config_Update_Rpt* SHALL be sent only once. – This TLV is included based on local RRC policy.

IE	Reference	M/O	Notes
			Decision to include this TLV is implementation specific.
RRM Reporting Period P	5.3.2.163	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.

1 The message definition for the RRM R6 *Radio_Config_Update_Rpt* messages is the same as the corresponding R4
2 message definition as specified in section 4.9.3.2.1.

7.1.2   R6 ASN Anchored Mobility

7.1.2.1   HO Preparation Phase

5 In section 4.7.2.1, there are several scenarios of handoff preparation. This section of profile A HO preparation is
6 based on 4.7.2.1, and is integrated into the following scenarios:

7 Scenario 1 corresponding to scenario 1, 2 and 3 in section 4.7.2.1;

8 Scenario 2 corresponding to scenario 4 in section 4.7.2.1;

9 Scenario 4 corresponding to scenario 5 and 6 in section 4.7.2.1.

7.1.2.1.1   Handoff Preparation Scenario 1: Data Path Pre-establishment flows separating from HO Request / Response procedures.

12 In the HO Preparation Phase, if Serving ASN is not collocated with Anchor ASN, the *HO_Req* message will not go
13 through Anchor ASN and no data path pre-establishment info can be sent with *HO_Req* to the Target ASN. So the
14 data path establishment procedure will be initiated by Target BS separately.

1
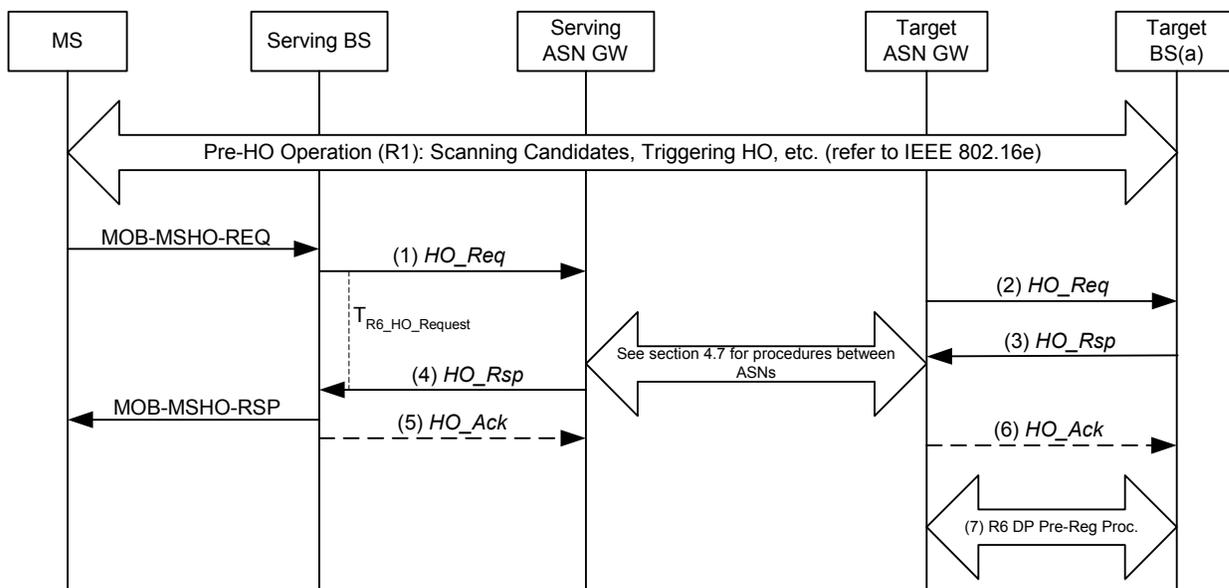
2 **Figure 7-5 – Preparation Phase for MS-triggered Handover - Scenario 1**

3 **STEP 1**

4 When the Serving BS receives MOB_MSHO-REQ from the MS, it sends R6 *HO_Req* message to Serving ASN GW
5 with the list of Candidate BSs selected by MS and other contexts. Upon sending out R6 *HO_Req*, the Serving BS
6 SHALL start timer $T_{R6\_HO\_Req}$.

7 Serving GW selects a set of BSs from the Candidate BS list received in the R6 *HO_Req*, by its local decision
8 criteria, and transmits R4 *HO_Req* message with the related context maintained by it according to section 5.7.1.1, to
9 each selected candidate BS. In case the Serving ASN GW cannot send the message directly to the Target BS, it
10 SHALL send the message to the Target ASN GW first.

11 **STEP 2**

12 When to Target ASN GW receives the R4 *HO_Req* message, it send separately R6 *HO_Req* to the candidate BSs
13 which are specified in the R4 *HO_Req* message. Upon sending out every R6 *HO_Req*, the Target ASN GW SHALL
14 start timer $T_{R6\_HO\_Req\_Target}$ for the Target BS. If it doesn't receive response messages from some BSs before their
15 $T_{R6\_HO\_Req\_Target}$ timers expire, it SHALL discard the corresponding request attempt to these BSs and exclude these
16 BSs from the recommended BS list in R4 *HO_Rsp* message.

17 **STEP 3**

18 Each candidate BS tests the acceptability of the requested HO by comparing its amount of available resources and
19 the required BW/QoS parameters in the R6 *HO_Req* message received from the ASN GW. Each BS transmits R6
20 *HO_Rsp* message, which includes the Success/Failure code for the corresponding *HO_Req*.

21 **STEP 4**

22 The Serving ASN GW decides recommended BSs for the HO, based on the information in R4 *HO_Rsp* messages
23 sent from candidate BSs. The ASN GW transmits the recommended BS list to the Serving BS by R6 *HO_Rsp*
24 message. The Serving BS stops the timer $T_{R6\_HO\_Req}$ when receives R6 *HO_Rsp* and sends MOB_BSHO-RSP which
25 conveys the list of recommended BSs to MS.

26 **STEP 5**

27 The Serving BS transmits R6 *HO_Ack* to the serving ASN GW as the acknowledgement of the R6 *HO_Rsp*
28 message. The serving ASN GW may send out this message to the recommended BSs. In case the Serving ASN GW

1   cannot send the message directly to the Target BS, it SHALL send the message to the Target ASN GW first using
2   R4 *HO_Ack* message format. This step may be optional and it can be used to indicate TBS that the MS might initiate
3   network re-entry at any time.

4   **STEP 6**

5   The Target ASN GW sends the R6 *HO_Ack* message to the BSs which are specified in the received R4 *HO_Ack*
6   from the Serving ASN GW.

7   **STEP 7**

8   The Data Path Pre-Registration procedure is employed to pre-register the data path with Anchor ASN. Note that this
9   procedure can be initiated upon the target BS receives the R6 *HO_Req* message, but the *HO_Rsp* does not depend
10 on the completion or success of this data path pre-registration procedure. And if Anchor ASN is collocated with
11 Serving ASN, the Data path Pre-Registration procedure can be initiated by Anchor/Serving ASN along with HO
12 Request procedure. Otherwise, it is initiated by Target BS.

13 **7.1.2.1.2   Handoff Preparation Scenario 2: Anchor ASN Collocated with Serving ASN, and R6 Path**
14 **Pre-Registration messages piggybacked onto R6 HO_Req**

15 In the HO Preparation Phase, if Serving ASN is collocated with Anchor ASN, the *HO_Req* message may piggyback
16 data path pre-establishment info to the Target ASN to pre-registration data path for MS.
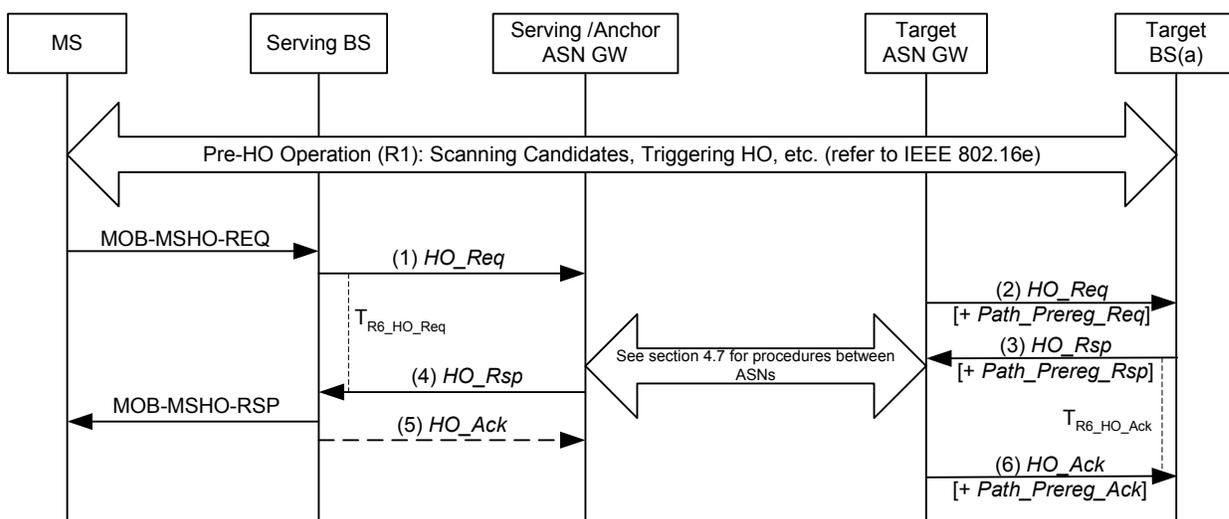
17

18 **Figure 7-6 – HO Preparation Phase for MS-triggered Handover - Scenario 2**

19 **STEP 1**

20 When the Serving BS receives MOB_MSHO-REQ from the MS, it sends R6 *HO_Req* message to Serving ASN GW
21 with the list of Candidate BSs selected by MS and other contexts. Upon sending out R6 *HO_Req*, the Serving BS
22 SHALL start the $T_{R6\_HO\_Req}$ timer.

23 The Serving/Anchor GW selects a set of BSs from the Candidate BS list received in the R6 *HO_Req*, by its local
24 decision criteria, and transmits R4 *HO_Req* message with data path pre-registration information according to section
25 5.7, to each selected candidate BS. In case the Serving/Anchor ASN GW cannot send the message directly to the
26 Target BS, it SHALL send the message to the Target ASN GW first.

27 **STEP 2**

28 When to Target ASN GW receives the R4 *HO_Req* message, it send separately R6 *HO_Req* to the candidate BSs
29 which are specified in the R4 *HO_Req* message. Upon sending out every R6 *HO_Req*, the Target ASN GW SHALL
30 start a $T_{R6\_HO\_Req\_Target}$ timer for the Target BS. If it doesn't receive response messages from some BSs before their

1   $T_{R6\_HO\_Req\_Target}$ timers expire, it SHALL discard the corresponding request attempt to these BSs and exclude these
2   BSs from the recommended BS list in R4 *HO_Rsp* message. The R6 *HO_Req* message includes the R6
3   *Path_Prereg_Req* information to initiate the pre-establishment of the data path for the MS.

STEP 3

5   Each candidate BS tests the acceptability of the requested HO by comparing its amount of available resources and
6   the required BW/QoS parameters in the R6 *HO_Req* message received from the ASN GW. If the BS can accept the
7   HO, it then deal with the Data Path pre-establishment according to the Path Pre-Registration information received
8   from R6 *HO_Req*. Each BS transmits R6 *HO_Rsp* message, which includes the Success/Failure code for the
9   corresponding *HO_Req*. If the Data Path Pre-Registration is supported,the R6 Data Path Pre-Registration info
10 should be included in the message and a timer $T_{R6\_HO\_Ack}$ should be started.

STEP 4

12 The Serving ASN GW decides recommended BSs for the HO, based on the information in R4 *HO_Rsp* messages
13 sent from candidate BSs. The ASN GW transmits the recommended BS list to the Serving BS by R6 *HO_Rsp*
14 message. The Serving BS stops the timer $T_{R6\_HO\_Req}$ when receives R6 *HO_Rsp* and sends MOB-BSHO-RSP which
15 conveys the list of recommended BSs to MS.

STEP 5

17 The Serving BS transmits R6 *HO_Ack* to the serving ASN GW as the acknowledgement of the R6 *HO_Rsp*
18 message. The serving ASN GW may send out this message to the recommended BSs. In case the Serving ASN GW
19 cannot send the message directly to the Target BS, it SHALL send the message to the Target ASN GW first using
20 R4 *HO_Ack* message format. This step may be optional and it can be used to indicate target BS that the MS might
21 initiate network re-entry at any time.

STEP 6

23 The Target ASN GW sends the R6 *HO_Ack* message with R6 *Path_Prereg_Ack* info to the BSs which are specified
24 in the received R4 *HO_Ack* from the Serving ASN GW. The BS stops the timer $T_{R6\_HO\_Ack}$ when it receives this
25 message.

7.1.2.1.3   Handoff Preparation Scenario 3: Anchor Controlled HO

27 The following call flow describes a successful handover preparation scenario where the MS may perform Pre-HO
28 operation, such as scanning or associating with the neighbor BSs before deciding on handover and transmitting
29 MOB_MSHO-REQ. For detailed procedures, refer to the related section of IEEE 802.16e
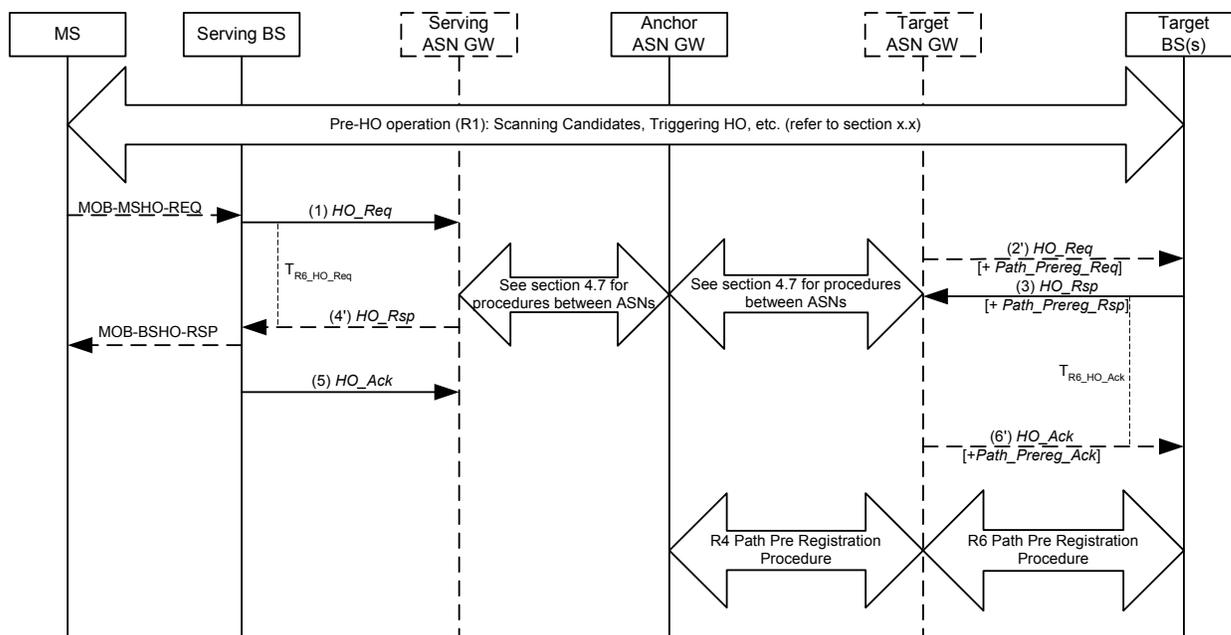
* Target ASN GW is inserted for illustration of Inter ASN HO case.
Serving ASN GW may be collocated with Anchor ASN GW in some areas.
* T5 - If HO Request is sent to multiple Target BS(s), all the Target BSs are
expected to respond to the Target ASN GW with in T5.

1

2 **Figure 7-7 – Handoff Preparation Scenario 3: Anchor Controlled HO**

3 Note: Please refer to section 7.1.2.1.6 for Path Pre registration procedure.

4 **STEP 1**

5 When the Serving BS receives *MOB_MSHO-REQ* from the MS, it sends R6 *HO_Req* message to Serving ASN GW
6 with the list of Candidate BSs selected by MS and other parameters.

7 In case the Anchor ASN GW has the HO control function and the Serving BS cannot send the message directly to
8 the Anchor ASN GW, the Serving ASN GW SHALL relay *HO_Req* message to the Anchor ASN GW.

9 The Serving BS SHALL start the $T_{R6\_HO\_Request}$ timer after sending R6 *HO_Req*.

10 **STEP 2**

11 Anchor which has HO control functionality selects a set of BSs from the Candidate BS list received in the list
12 received in the R6 *HO_Req* based on it's local decision criteria, and then transmits R6 *HO_Req* message. This R6
13 *HO_Req* message has MS session information associated with each selected candidate BS. In case the Anchor or
14 Serving ASN GW cannot send the message directly to the Target BS, it SHALL send the message to the Target
15 ASN GW which then relays this message to the Target BS.

16 Upon sending out each R6 *HO_Req*, the Anchor ASN GW SHALL start a $T_{R6\_HO\_Req}$ timer.

17 In the *HO_Req* message sent by Anchor ASN GW, the IEs for Data path Pre-registration may be optionally included
18 in order to accelerate the data path re-establishment.

19 **STEP 3**

20 Each candidate BS tests the acceptability of the requested HO by comparing its amount of available resources and
21 the required BW/QoS parameters in the R6 *HO_Req* message received from the ASN GW. Each BS transmits R6
22 *HO_Rsp* message, which includes the Success/Failure code for the corresponding *HO_Req*, to the Anchor ASN GW
23 who initially sends *HO_Req*. In case the Target BS cannot send the message directly to the Anchor ASN GW, it

1 SHALL send the message to the Target ASN GW. Then the Target ASN GW relays this message to the Anchor
2 ASN GW.

3 When a candidate BS receives HO_Requst message with IEs for DataPath Pre-registration, it SHALL append IEs
4 for *Path_Prereg_Rsp* or Pre-Reg_Failure_Reason TLV to its *HO_Rsp* message. The support of Path Pre-registration
5 feature at BS is optional, but sending Pre-Reg_Failure_Reason TLV when the feature is not supported by BS is
6 mandatory.

7 **STEP 4**

8 The Anchor ASN GW decides recommended BSs for the HO, based on the information in R6 *HO_Rsp* messages
9 sent from candidate BSs. The ASN GW transmits the recommended BS list to the Serving BS by R6 *HO_Rsp*
10 message. In case the Anchor ASN GW cannot send the message directly to the Serving BS, it SHALL send the
11 message to the Serving ASN GW. Then the Serving ASN GW relays this message to the Serving BS.

12 **STEP 5**

13 The Serving BS transmits R6 *HO_Ack* to the ASN GW who initiates R6 *HO_Req* as the acknowledgement of the R6
14 *HO_Rsp* message. In case the Anchor ASN GW has the HO control functionality and the Serving BS cannot send
15 the message directly to the Anchor ASN GW, it SHALL send the message to the Serving GW. Then the Serving
16 ASN GW relays this message to the Anchor ASN GW.

17 **STEP 6**

18 If Anchor-initiated Path Pre-registration is used, the Anchor ASN GW transmits R6 *HO_Ack* to Target BS as the
19 acknowledgement of the R6 *HO_Rsp* message and its related *Path_Prereg_Rsp*. In case the Anchor ASN GW
20 cannot send the message directly to the Target BS, it SHALL send the message to the Target GW. Then the Target
21 ASN GW relays this message to the Target BS.

22 If Anchor-initiated Path Pre-registration feature is not employed, Step 6 is optional. They can be used to indicate
23 Target BS that the MS might initiate network re-entry at any time.

24 **7.1.2.1.4 Handoff Preparation Scenario 4: Network initiated**

25 Network can initiate HO procedure according to the current status of network, such as the payload of different BSs,
26 the data throughput of reference points. Network initiated HO can be used to balance payload between network
27 entities. Different entities can trigger HO procedure. In profile A, ASN GW should initiate HO of MSs under its
28 control.

1
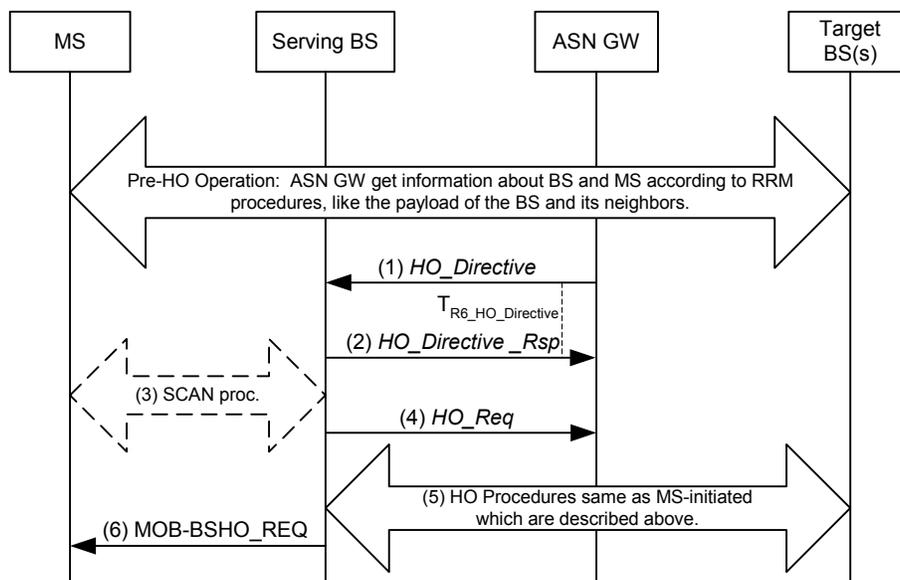
2 **Figure 7-8 – Preparation Phase for Network-triggered Handover - Scenario 3**

3 Before sending *HO_Directive* to trigger HO procedure, the ASN GW (Serving) can get informations of BS and MS
4 about their payload or signal quality through RRM procedures. According these informations, ASN GW can decide
5 if a network initiated HO is need.

6 When Network triggered HO, the network side(ASN GW) sends HO trigger message to Serving HO Function
7 located in Serving BS, then the Serving BS will conduct MS HO operation like MS initiated HO case.

8 **STEP 1**

9 If the ASN GW (refer as Serving ASN) determines to initiate a HO for various reasons, such as balancing payload, it
10 SHALL transmit R6 *HO_Directive* message to the specific BS (refer as Serving BS) to indicate the BS to handover
11 some MSs to other BSs, and transmits the recommended BS list. The ASN GW may indicate the BS to migrate how
12 many payload to other BSs for balancing payload. The ASN GW will start the timer $T_{R6\_HO\_Directive}$ when it sends out
13 this messag

14 The ASN GW may also give the recommend MSs which need be handed over.

15 **STEP 2**

16 After receiving the R6 *HO_Directive* message from Serving ASN-GW, the Serving BS acknowledges the R6
17 *HO_Directive* from the Serving ASN GW with R6 *HO_Directive_Rsp* at once. And upon receiving this message,
18 the GW stops the timer $T_{R6\_HO\_Directive}$.

19 **STEP 3**

20 The Serving BS selects some candidate MSs for HO based on information maintained by Serving BS and received
21 from *HO_Directive* message. In order to guarantee the success of HO, the SBS may request some candidates to
22 execute SCAN procedure to get their neighbors information.

23 **STEP 4**

24 Based on the above information, the SBS selects some suitable MSs for HO and transmits R6 *HO_Req* message to
25 the Serving ASN-GW separately for each MS. Upon sending out R6 *HO_Req*, the Serving BS SHALL start the
26 $T_{R6\_HO\_Req}$ timer for each MS.

1 **STEP 5**

2 The following procedure is the same as the process of MS initiated HO which is described above sections.

3 **STEP 6**

4 After network deals with the process of HO preparation, the Serving BS sends MOB-BSHO_REQ message to each
5 MS to request MS to handover to the target BS(s). The Serving BS sends MOB_BSHO_REQ which conveys the list
6 of recommended BSs to MS. After this, the network and MS will deal the HO process as described in HO action
7 phase.

8 **7.1.2.1.5 R6 Message Definitions for HO Preparation Phase**

9 This section describes the R6 message definitions for the HO Preparation Phase

10 The *HO_Req* message sent from Serving BS to Serving ASN GW is show in Table 7-8.

11 **Table 7-8 – R6 HO_Req Message Format (SBS→ Serving ASN GW)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>SBC Context	5.3.2.174	O	802.16e related MS session context.
>PKM Context	5.3.2.131	O	802.16e related MS session context.
>REG Context	5.3.2.144	O	802.16e related MS session context.
>SF Info (one or more)	5.3.2.185	O	Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	O	Service Flow ID
>SDU Info (one or more)	5.3.2.176	O	Each element in the list contains context of an SDU affected by the Data Integrity Operations. For Type-2 Data Path.
>Block SN	Not defined in Release 1.0.0	O	Sequence Number of the last transmitted ARQ block context for Data Integrity. Relevant only for DL U-Cast SF. If Type-2 DP is used, this TLV is included.
>SA Descriptor	5.3.2.170	O	TEK related Context info. This IE is sent by the serving BS. If Path Pre-registration is used, then this TLV SHALL be forwarded.
>SAID	.5.3.2.169	O	Security association identifier - GSAID for multicast or broadcast service.
Serving BS Info	5.3.2.26	O	Contains Serving BS context in the nested Ies.
>BS ID	5.3.2.25	O	Serving BS ID
>Round Trip Delay	5.3.2.156	O	Round Trip Delay (RTD) between the MS and the Serving BS
>DL PHY Quality Info	5.3.2.60	O	Downlink PHY Quality between the MS and the Serving BS

IE	Reference	M/O	Notes
>UL PHY Quality Info	5.3.2.197	O	Uplink PHY Quality between the MS and the Serving BS
Target BS Info (one or more)	5.3.2.26	M	Each IE in the list contains Target BS context in the nested Ies.
>BS ID	5.3.2.25	M	Target BS ID
>Relative Delay	5.3.2.146	O	Indicates the delay of neighbor DL signals relative to the serving BS, as measured by the MS for the particular BS.
>DL PHY Quality Info	5.3.2.60	O	Downlink PHY Quality between the MS and the Target BS
>UL PHY Quality Info	5.3.2.197	O	Uplink PHY Quality between the MS and the Target BS

1   The *HO_Req* sent from Target ASN GW to Target BS is shown in Table 7-9.

2   **Table 7-9 – R6 HO_Req Message Format (Target ASN GW → TBS)**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	Describes type of the HO (FBSS, MDHO, HHO) This information may be extracted from ASN GW based on subscriber policy information
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>Anchor GW ID	5.3.2.10	O	Identifies the Anchor ASN GW
>Authenticator ID	5.3.2.20	O	Identifies the Authenticator ASN GW
>AK Context	5.3.2.6	O	Authentication Key related Context info If Path Pre-registration is used, this TLV SHALL be included
>SBC Context	5.3.2.174	O	802.16e related MS session context.
>PKM Context	5.3.2.131	O	802.16e related MS session context.
>REG Context	5.3.2.144	O	802.16e related MS session context.
>Data Path Info	5.3.2.45	O	Data Path Info for per-BS or per-MS granularity tunnel
>SF Info (one or more)	5.3.2.185	O	Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	M	SFID associated with the Service Flow
>>QoS Info	5.x.x	M	QoS Parameters associated with the Service Flow
>>QoS Parameters	5.3.2.141	M	IEEE 802.16 QoS Parameters
>>SAID	5.3.2.169	O	SAID associated with the Service Flow. If Path Pre-registration is used, then this TLV SHALL be included.

IE	Reference	M/O	Notes
>>SA Descriptor	5.3.2.170	O	TEK related Context info.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>Packet Classification Rule (one or more)	5.3.2.114	O	Each IE in the list contains IEEE 802.16e Packet Classification Rule.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>>Classifier Rule Priority	5.3.2.32	O	IEEE 802.16e Classifier Rule Priority.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>SAID	5.3.2.169	O	SAID associated with the Service Flow.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>>Classifiers	5.3.2.30	O	Set of IEEE 802.16e Classifiers associated with the Classifier Rule.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>Data Path Info	5.3.2.45	O	Data Path Info for per-flow granularity tunnel
>>>Data Path Encapsulation Type	5.3.2.42	O	The type of the Data Path Encapsulation (e.g. GRE). Relevant for DL SF only.
			If Path Pre-registration is used, then this TLV SHALL be included.
>>>Data Path Type	5.3.2.47	O	The type of Data Path Function; possible value is Type 1 or Type 2.
>>>Data Path Establishment Option	5.3.2.43	O	A flag indicating whether or not Data Path should be established before responding to the *HO_Req*.
>>>Tunnel Endpoint	5.3.2.194	O	IP address of the ASN GW.
			If Path Pre-registration and per-BS data path granularity is used, this TLV SHALL be included
>>>Data Path ID	5.3.2.44	O	Path ID for the corresponding SF.
			If Path Pre-registration and per-flow data path granularity is used, then this TLV SHALL be included.
>>SDU Info (one or more)	5.3.2.176	O	Each element in the list contains context of an SDU affected by the Data Integrity Operations.
			For Type-2 Data Path.
>>Block SN	Not defined in Release 1.0.0	O	Sequence Number of the last transmitted ARQ block context for Data Integrity. Relevant only for DL U-Cast SF.
			If Type-2 DP is used, this TLV is included.
>>>Tunnel Endpoint	5.3.2.194	O	IP@ of the ASN GW.
			If Path Pre-registration and per-BS data path granularity is used, this TLV SHALL be included

IE	Reference	M/O	Notes
Target BS Info (one or more)	5.3.2.26	M	Each IE in the list contains Target BS context in the nested Ies.
>BS ID	5.3.2.25	M	Target BS ID

1   The *HO_Rsp* sent from Target BS to Serving ASN GW appears as shown in Table 7-10:

2   **Table 7-10 – R6 HO_Rsp Message Format (TBS → Serving ASN GW)**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	Describes type of the HO (FBSS, MDHO, HHO)
Result Code	5.3.2.154	M	This TLV indicates the acceptance or failure of the *Path_Prereg_Req* at the TBS. When the requested Path Pre-registration fails at the Target BS, this code SHALL include the appropriate reason code. Possible values are: Success: The request of the Pre-registration was accepted at the TBS. No_Resource: Not enough resource available at the Target BS Not_Supported: Pre-Reg is not supported by the Target BS
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>Anchor GW ID	5.3.2.10	O	Identifies the Anchor ASN GW
>Data Path Info	5.3.2.45	O	Data Path Info for per-MS or per-BS granularity tunnel
>SF Info (one or more)	5.3.2.185	O	Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	M	SFID associated with the Service Flow
>>Result Code	5.3.2.154	M	Indication whether this SF can be supported
>>QoS Info	5.x.x	M	Supported QoS Information for each Service flow at Candidate BS
>>>QoS Parameters	5.3.2.141	M	IEEE 802.16 QoS Parameters
>>CID	5.3.2.29	O	CID replacement. If Pre-registration and Type-2 Data Path is used or if HO Type is FBSS or MDHO,, this TLV SHALL be included.
>>>Data Path Info	5.3.2.45	O	Data Path Info for per-flow granularity tunnel
Target BS Info (one or more)	5.3.2.26		Contains relevant Target BS context in the nested Ies.
>BS ID	5.3.2.25	M	Target BS ID

IE	Reference	M/O	Notes
>HO ID	Defined in [2]	O	ID assigned for use in initial ranging to the target BS once this BS is selected as the target BS
>Service Level Prediction	5.3.2.180	M	Service Level Prediction code.
>Preamble Index / Sub-channel Index	5.3.2.137	O	Preamble Index / Sub-channel Index code
>HO Process Optimization	5.3.2.78	M	HO Process Optimization code
>HO Authorization Policy Support	Defined in [2]	O	Bit #0: RSA authorization Bit #1: EAP authorization Bit #2: Authenticated-EAP authorization Bit #3: HMAC supported Bit #4: CMAC supported Bit #5: 64-bit Short-HMAC Bit #6: 80-bit Short-HMAC Bit #7: 96-bit Short-HMAC
>HO Authorization Policy Indicator	Defined in [2]	O	To indicate if authorization negotiation is used in HO procedure. 0: EAP authorization and the value of the MAC mode field in the current BS (default) 1: The authorization policy for the target BS is negotiated.
>Action Time	5.3.2.4	M	802.16e parameter
>Resource Retain Type	Defined in [2]	O	802.16e parameter
>Resource Retain Time	Defined in [2]	O	802.16e parameter
>Result Code	5.3.2.154	O	Indicate whether the preparation phase was successful or not for easier processing at the GW

HO_Rsp format sent from Serving ASN GW to Serving BS is shown on the Table 7-11.

Table 7-11 – R6 HO_Rsp Message Format (Anchor/Serving ASN GW → SBS)

IE	Reference	M/O	Notes
HO Operation Mode	Defined in [2]	M	802.16e parameter
Resource Retain Flag	Defined in [2]	M	802.16e parameter
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
Target BS Info (one or more)	5.3.2.26	M	Contains relevant Recommended BS context in the nested Ies.
>BS ID	5.3.2.25	M	Recommended BS ID
>HO ID	Defined in [2]	O	ID assigned for use in initial ranging to the BS once this BS is selected as the target BS

IE	Reference	M/O	Notes
>Service Level Prediction	5.3.2.180	M	Service Level Prediction code.
>Preamble Index / Sub-channel Index	5.3.2.137	O	Preamble Index / Sub-channel Index code
>HO Process Optimization	5.3.2.78	M	HO Process Optimization code
>HO Authorization Policy Support	Defined in [2]	O	Bit #0: RSA authorization Bit #1: EAP authorization Bit #2: Authenticated-EAP authorization Bit #3: HMAC supported Bit #4: CMAC supported Bit #5: 64-bit Short-HMAC Bit #6: 80-bit Short-HMAC Bit #7: 96-bit Short-HMAC
>HO Authorization Policy Indicator	Defined in [2]	O	To indicate if authorization negotiation is used in HO procedure. 0: EAP authorization and the value of the MAC mode field in the current BS (default) 1: The authorization policy for the target BS is negotiated.
Action Time	5.3.2.4	M	802.16e parameter
Resource Retain Type	Defined in [2]	O	802.16e parameter
Resource Retain Time	Defined in [2]	O	802.16e parameter
Result Code	5.3.2.154	M	Indicate whether the preparation phase was successful or not to the BS

1   *HO_Ack* sent from SBS to Serving ASN GW is shown in Table 7-12.

2   **Table 7-12 – R6 HO_Ack Message Format (SBS → Serving ASN GW)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
Target BS Info	5.3.2.26	O	Contains relevant Target BS context in the nested Ies.
>BS ID	5.3.2.25	O	Target BS ID

3   The content of the R6 *HO_Ack* message from Target ASN GW to Target BS is specified in Table 7-13.

4   **Table 7-13 – R6 HO_Ack Message Format (Target ASN GW → TBS)**

IE	Reference	M/O	Notes
Target BS Info	5.3.2.26	O	Contains relevant Target BS context in the nested Ies.
>BS ID	5.3.2.25	O	Target BS ID

1   The content of R6 *HO_Directive* message is shown on the Table 7-14.

2   **Table 7-14 – R6 HO_Directive Message Format**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	Describes type of the HO (FBSS, MDHO, HHO)
Network Assisted HO Supported	Defined in [2]	M	Indicator for network assisted HO
HO Reason	Not defined in Release 1.0.0	M	The reason why the ASN GW initiates the HO process.
HO Ratio of Payload	Not defined in Release 1.0.0	O	Indicate HO Ratio of Payload for this BS
Target BSD Info (one or more)	5.3.2.26	O	The BSs which the ASN GW recommends the serving BS to handover MS to.
>BS ID	5.3.2.25	M	
MS Info	5.3.2.103	O	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)

3   The content of R6 *HO_Directive_Rsp* message is shown in Table 7-15.

4   **Table 7-15 – R6 HO_Directive_Rsp Message Format**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Indicate if the serving BS successfully received the *HO_Directive* message and is ready to deal with it.

5   **7.1.2.1.6 R6 Data Path Pre-Registration Procedure**

6   The following call flow describes the R6 Data Path Pre-Registration procedure during handovers between target BS
7   and target ASN GW. Data Path pre-establishment is initiated by the target BS.
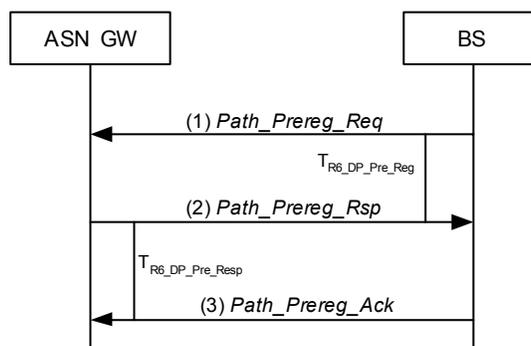
8

9   **Figure 7-9 – R6 Data Path Pre-Registration Procedure, Scenario 2**

10   **STEP 1**

11   The target BS sends an R6 *Path_Prereg_Req* message to the target ASN GW to pre-establish the data path for a MS
12   and starts the timer $T_{R6\_DP\_Pre\_Reg.}$

1 **STEP 2**

2 The target ASN GW deals with the request message and sends back an R6 *Path_Prereg_Rsp* message to the target
3 BS and starts the timer $T_{R6\_DP\_Pre\_Rsp}$. The target BS stops the timer $T_{R6\_DP\_Pre\_Reg}$ when receives this message.

4 **STEP 3**

5 The target BS sends an R4 *Path_Prereg_Ack* message to the target ASN GW to confirm the pre-establishment of the
6 data path. When the target ASN GW receives this message, it stops the timer $T_{R6\_DP\_Pre\_Rsp}$.

7 **7.1.2.1.7 R6 Data Path Registration Procedure (initiated by Target BS)**

8 R6 Data Path Registration procedure takes place between the Target BS and the Target ASN GW immediately after
9 the MS has arrived at the Target BS.
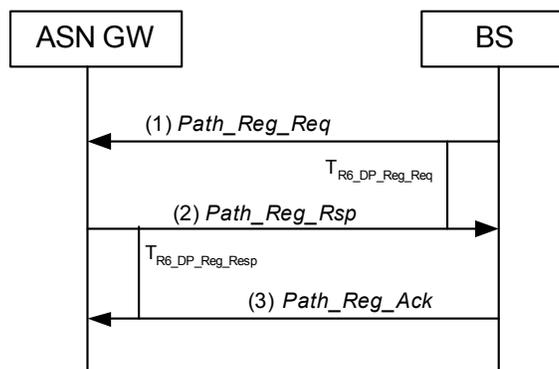
10

11 **Figure 7-10 – R6 Data Path Registration**

12 **STEP 1**

13 BS initiates Data Path Registration procedure by sending an R6 *Path_Reg_Req* message to the ASN GW connected
14 to it and starting the timer $T_{R6\_DP\_Reg\_Req}$.

15 **STEP 2**

16 The ASN GW deals with the message and sends back an R6 *Path_Reg_Rsp* message to the BS and starts the timer
17 $T_{R6\_DP\_Reg\_Rsp}$ when it expects the R6 *Path_Reg_Ack* message returned from the BS. The BS stops the timer
18 $T_{R6\_DP\_Reg\_Req}$ when it receives this message. R6 *Path_Reg_Rsp* message sent by the Anchor ASN GW SHALL
19 contain the updated R6 data path information for uplink traffic.

20 **STEP 3**

21 If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then
22 the BS sends an R6 *Path_Reg_Ack* message to ASN GW to trigger the data transmission. When receiving this
23 message, the ASN GW stops the timer $T_{R6\_DP\_Reg\_Rsp}$.

24 **7.1.2.1.8 R6 Data Path Registration Procedure (initiated by Anchor ASN GW)**

25 R6 Data Path Registration procedure takes place between the Target BS and the Target ASN GW immediately after
26 the MS has arrived at the Target BS. In case the Target BS or Anchor ASN GW cannot send the message directly to
27 the corresponding Anchor ASN GW or Target BS, it SHALL send the message to the Target ASN GW. Then the
28 Target ASN GW relays this message to the relevant recipient.
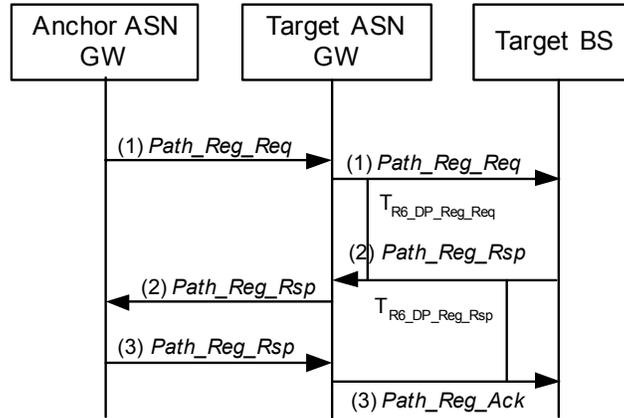
**Figure 7-11 – R6 Data Path Registration**

STEP 1

Anchor ASN GW initiates Data Path Registration procedure by sending an R6 *Path_Reg_Req* message to the Target BS and start the timer $T_{R6\_DP\_Reg\_Req}$.

STEP 2

Target BS processes the message and sends back an R6 *Path_Reg_Rsp* message to the Anchor ASN GW and starts the timer $T_{R6\_DP\_Reg\_Rsp}$ when it expects the R6 *Path_Reg_Ack* message returned from the Anchor ASN GW. The BS stops the timer $T_{R6\_DP\_Reg\_Req}$ when it receives this message. R6 *Path_Reg_Rsp* message sent by the Target BS SHALL contain the updated R6 data path information for downlink traffic.

STEP 3

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then the Anchor ASN GW sends an R6 *Path_Reg_Ack* message to Target BS to trigger the data transmission. After receiving this message, the Target BS stops the timer $T_{R6\_DP\_Reg\_Rsp}$.

7.1.2.1.9 R6 Data Path De-Registration Procedure (initiated by Serving BS)

R6 Data Path De-Registration Procedure appears below. The R6 data path de-registration initiated by serving BS.
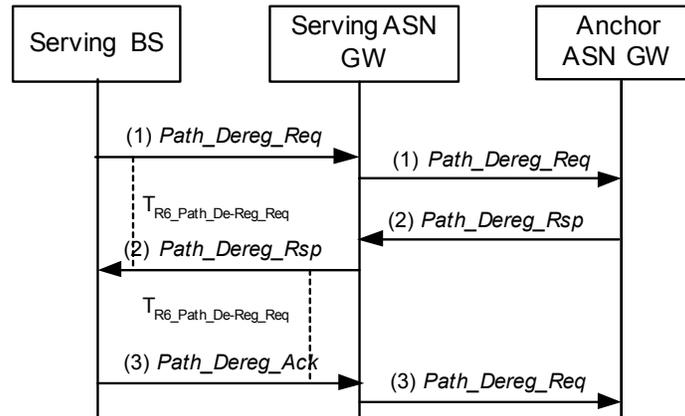
Figure 7-12 – Data Path De-Registration

1 **STEP 1**

2 The Serving BS initiates Data Path Registration procedure by sending an R6 *Path_Dereg_Req* message to the
3 Anchor ASN GW and starts the timer $T_{R6\_DP\_De-Reg\_Req}$. If the Serving BS can not send the message directly to the
4 Anchor ASN GW, it sends it to the Serving ASN GW. Then the serving ASN GW relays this message to the Anchor
5 ASN GW.

6 **STEP 2**

7 The Anchor ASN GW processes the message and releases the Data Path, then sends back R6 *Path_Dereg_Rsp* to the
8 Serving BS, with starting the timer $T_{R6-Path\_De-Reg\_Rsp}$. Upon receiving this message, the Serving BS stops the timer
9 $T_{R6\_Path\_De-Reg\_Req}$.

10 **STEP 3**

11 The Serving BS sends back R6 *Path_Dereg_Ack* message to the Anchor ASN GW. Upon receiving this message,
12 the Anchor ASN GW stops the timer $T_{R6-Path\_De-Reg\_Rsp}$.

13 **7.1.2.1.10 R6 Data Path De-Registration Procedure (initiated by Serving / Anchor ASN GW)**

14 R6 Data Path De-Registration Procedure appears below. The R6 data path de-registration initiated by serving /
15 Anchor ASN GW.
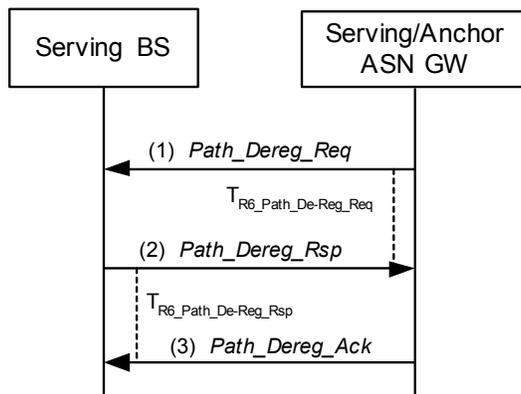
16

17 **Figure 7-13 – R6 Data Path De-Registration**

18 **STEP 1**

19 The Serving or Anchor ASN GW initiates Data Path Registration procedure by sending an R6 *Path_Dereg_Req*
20 message to the Serving BS and starts the timer $T_{R6\_DP\_De-Reg\_Req}$. If the Anchor ASN GW can not send the message
21 directly to the Serving BS, it sends it to the Serving ASN GW. Then the Serving ASN GW relays this message to the
22 Serving BS.

23 **STEP 2**

24 The Serving BS processes the message and releases the Data Path, then sends back R6 *Path_Dereg_Rsp* to the
25 Anchor ASN GW. Upon receiving this message, the Serving or Anchor ASN GW stops the timer $T_{R6\_Path\_De-Reg\_Req}$.

26 **STEP 3**

27 The Serving or Anchor ASN GW sends back R6 *Path_Dereg_Ack* message to the Serving BS. Upon receiving this
28 message, the Serving BS stops the timer $T_{R6\_Path\_De-Reg\_Rsp}$

29 **7.1.2.1.11 R6 CMAC Key Count Update Procedure**

30 CMAC Key Count Update procedure within ASN appears below.

1
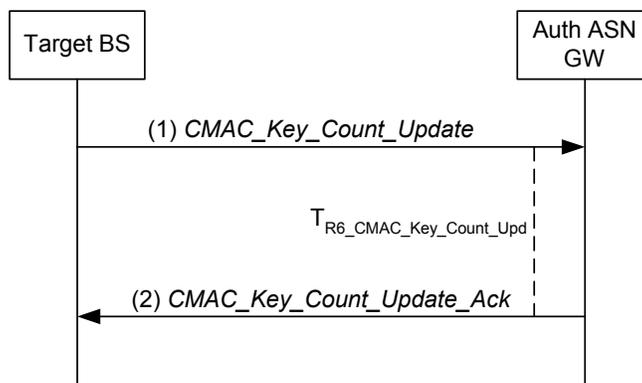
2 **Figure 7-14 – R6 CMAC Key Count Update**

3 **STEP 1**

4 The Target BS initiates CMAC Count Update procedure by sending an R6 *CMAC_Key_Count_Update* message to
5 the Target ASN GW which will route this message to the Authenticator and starts the timer $T_{R6\_CMAC\_Key\_Count\_Upd}$.

6 **STEP 2**

7 The Target ASN GW returns an R6 *CMAC_Key_Count_Update_Ack* message to the Target BS to confirm the
8 updating. Upon receiving this message, the BS stops the timer $T_{R6\_CMAC\_Key\_Count\_Upd}$.

9 **7.1.2.2   R6 Path De-Registration Procedure (initiated by the unselected Target BS)**

10 R6 Data Path De-Registration Procedure appears below. The R6 data path de-registration initiated by Unselected
11 Target BS.

12
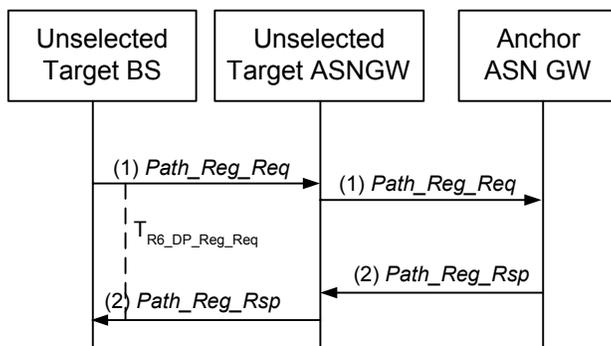
13 **Figure 7-15 – R6 Path De-Registration Procedure (initiated by the unselected Target BS) Profile A**

14 **STEP 1**

15 The Target BS that was previously selected by the MS initiates Data Path Registration procedure by sending an R6
16 *Path_Dereg_Req* message to the Anchor ASN GW and starts the timer $T_{R6\_DP\_Dereg\_Req}$. If the Target BS can not send
17 the message directly to the Anchor ASN GW, it sends it to the Target ASN GW. Then the serving ASN GW relays
18 this message to the Anchor ASN GW.

19 **STEP 2**

20 The Anchor ASN GW processes the message and releases the Data Path, then sends back R6 *Path_Dereg_Rsp* to the
21 Target BS. Upon receiving this message, the Target BS stops the timer $T_{R6\_DP\_Dereg\_Req}$.

1   **7.1.2.3   HO Action Phase**

2   In section 5.7.1.2 HO Action Phase, there are several scenarios of handoff action. This section of profile A HO
3   action is based on 5.7.2.1, and is integrated into the following scenarios:

4   Scenario 2 corresponding to scenario 1 and 4 in section 5.7.2.1;

5   Scenario 3 corresponding to scenario 2 in section 5.7.2.1;

6   Scenario 4 corresponding to scenario 3 and 6 in section 5.7.2.1.

7   **7.1.2.3.1   Handover Action Scenario 1: HO Control at the Anchor GW**

8   The following call flow describes a successful handover action scenario in which the HO control exists at the
9   Anchor ASN GW.
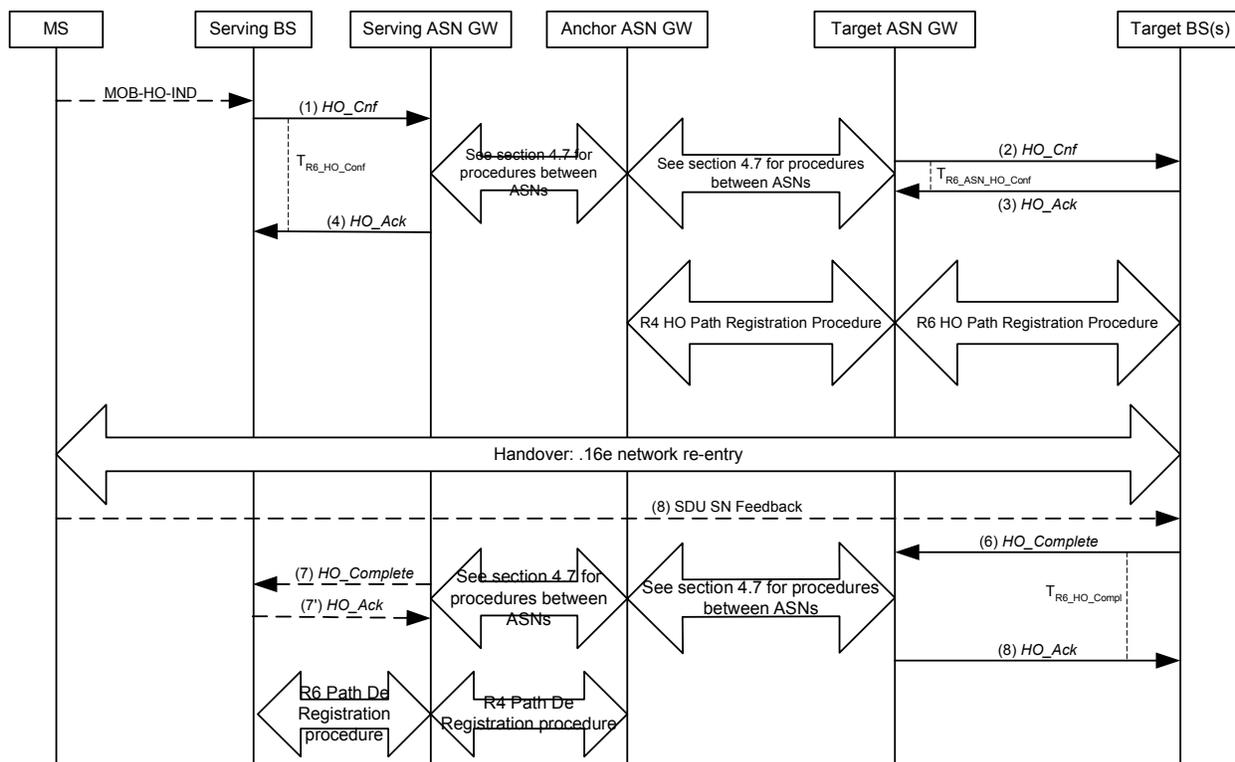
10   * Path setup transactions can be done in parallel with .16e network re-entry procedure.

11   **Figure 7-16 – HO Action Phase Scenario 1 – HO Control in Anchor GW**

12   Note: Please refer to section 7.1.2.1.7 for R6 Path Registration procedure.

13   Please refer to section 7.1.2.1.9 for R6 Data Path De-Registration procedure.

14   **STEP 1**

15   Upon receiving MOB_HO-IND message from MS, the Serving BS SHALL transmit R6 *HO_Conf* message to notify
16   the Anchor ASN GW, which has the HO control functionality, of the start of actual MS HO to the Target BS which
17   is selected by MS.

18   The R6 *HO_Cnf* message may include Data Integrity during HO and information about each MS service flow. In
19   case the Serving BS cannot send the message directly to the Anchor ASN GW, it SHALL send the message to the
20   Serving ASN GW. Then the Serving ASN GW relays this message to the Anchor ASN GW.

1 **STEP 2**

2 The Anchor ASN GW transmits R6 *HO_Cnf* to inform the Target BS of the upcoming MS HO. If Path Pre-
3 registration was not employed during the HO Preparation phase, the R6 *HO_Cnf* message SHALL include MS
4 Session Information elements, such as SBC context, REG context, AK context, SF Info, etc.

5 In case the Anchor ASN GW cannot send the message directly to the Target BS, it SHALL send the message to the
6 Target GW. Then the Target ASN GW relays this message to the Target BS.

7 **STEP 3**

8 The Target BS transmits R6 *HO_Ack* message to the Anchor or Serving ASN GW which initiated R6 *HO_Req*
9 message.

10 In case the Target BS cannot send the message directly to the Anchor or Serving ASN GW, it SHALL send the
11 message to the Target ASN GW. Then the Target ASN GW relays this message to the Anchor ASN GW.

12 **STEP 4**

13 The Anchor ASN GW sends R6 *HO_Ack* to the Serving BS as an acknowledgement to the R6 *HO_Cnf*.

14 In case the Anchor ASN GW cannot send the message directly to the Serving BS, it SHALL send the message to the
15 Serving GW. Then the Serving ASN GW relays this message to the Serving BS.

16 Note: Step 5 SHALL be conditionally executed depending on the existence of Path Pre-registration. Those Steps
17 will be skipped if the Path Pre-registration is used in the HO Preparation phase.

18 **STEP 5**

19 If Path Pre-registration is not employed in the HO Preparation phase, the Target BS or Anchor ASN GW SHALL
20 transmit R6 *Path_Reg_Req* message. See sections 7.1.2.1.7 and 7.1.2.1.8 for path registration procedure initiated by
21 Target BS and Anchor ASN GW respectively.

22 **STEP 6**

23 MS sends SDU SN Feedback Header with the last SDU SN on the uplink to the Target BS optionally.

24 **STEP 7**

25 Upon completion of MS Network Re-entry, the Target BS transmits R6 *HO_Complete* message to notify the Anchor
26 or Serving ASN GW, which has the HO control functionality, of the result of MS Re-entry. In case the Target BS
27 cannot send the message directly to the Anchor or Serving ASN GW, it SHALL send the message to the Target
28 ASN GW. Then the Target ASN GW relays this message to the Anchor or Serving ASN GW.

29 **STEP 8**

30 On receiving R6 *HO_Complete* message, the Anchor or Serving ASN GW may transmit R6 *HO_Complete* message
31 to the Serving BS. If the Serving BS receives this message it SHALL release the resources associated to this MS, as
32 it is considered that network re-entry succeeded, and further moves will require new HO procedures.

33 In case the Anchor ASN GW cannot send the message directly to the Serving BS, it SHALL send the message to the
34 Serving GW. Then the Serving ASN GW relays this message to the Serving BS.

35 **STEP 9**

36 The *HO_Ack* message is transmitted back from Serving BS to Target BS (via GW)

37 **STEP 10**

38 Upon expiry of the MS context retain timer or optionally upon reception of the R6 *HO_Complete* message, the
39 Serving BS initiates Path De-Registration procedure see section 9.1.4.2.3.

7.1.2.3.2 Handover Action Scenario 2: R4 HO_Cnf sent to the Target BS before MS Network Re-entry from the Target BS

The following call flow describes a successful handover action scenario where the Target BS receives the R6 *HO_Cnf* message from the Serving ASN, and received the Data Path Establishment Option TLV in the R4 *HO_Req* message.
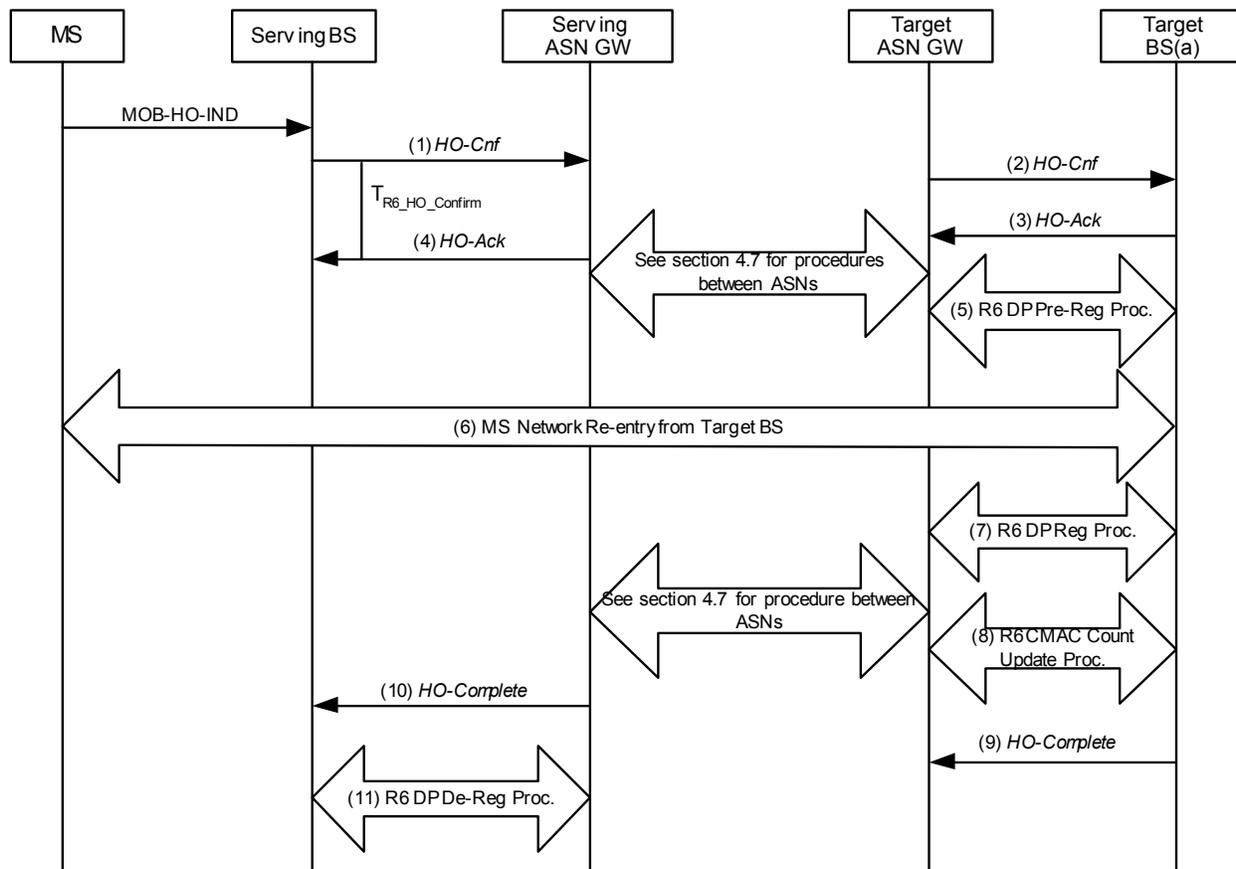

Figure 7-17 – Handover Action Scenario 2 Profile A

STEP 1

Upon receiving MOB_HO-IND message from MS, the Serving BS SHALL transmit R6 *HO_Cnf* message to notify the Serving ASN GW of the start of actual MS HO to the Target BS which is selected by MS and start the timer $T_{R6\_HO\_Conf}$. The R6 *HO_Cnf* message may include Data Integrity during HO. Information about each MS service flow. If Path Pre-registration was not employed during the HO Preparation phase, the R6 *HO_Cnf* message SHALL include MS Session Information elements, such as SBC context, REG context, AK context, SF Info, etc.

The message is routed to the Target ASN GW per the procedures described in section 5.7.1.2.

STEP 2

When the Target ASN GW receives the R4 *HO_Cnf* message, it transmits R6 *HO_Cnf* to inform the Target BS of the upcoming MS HO. If Path Pre-registration was not employed during the HO Preparation phase, the R6 *HO_Cnf* message SHALL include MS Session Information elements, such as SBC context, REG context, AK context, SF Info, etc.

1 **STEP 3**

2 The Target BS transmits R6 *HO_Ack* message to the Target ASN GW to confirm the receiving of R6 *HO_Cnf*
3 message. When the Target ASN GW receives the message, it will transmit R4 *HO_Ack* message to the Serving ASN
4 according to section 5.7.

5 **STEP 4**

6 The Serving ASN sends R6 *HO_Ack* to the Serving BS to acknowledge the HO_Comfirm message. Upon the
7 Serving ASN receives this message, it stops the timer $T_{R6\_HO\_Conf.}$

8 **STEP 5**

9 If Path Pre-registration was not employed during the HO Preparation phase, the Target BS may initiates the Data
10 Path pre-establishment for the MS by sending R6 *Path_Prereg_Req* to the Target ASN GW.

11 **STEP 6**

12 The MS initiates network re-entry with the Target BS.

13 **STEP 7**

14 If not already pre-established, the Target BS initiates Data Path Registration procedure with the Target ASN. Note:
15 This procedure may take place even if data path was pre-established and will follow the two-way handshake
16 process.

17 **STEP 8**

18 Simultaneously with starting the Data Path Registration procedure, the Target BS initiates CMAC Key Count
19 Update procedure by sending R6 *CMAC_Key_Count_Update* message to the Target ASN GW with the latest
20 CMAC Key Count value received from MS.

21 **STEP 9**

22 Upon completion of network re-entry, the Target BS may send an R6 *HO_Complete* message to the Target ASN to
23 notify the completion of the handover.

24 **STEP 10**

25 When the Serving ASN receives the R4 *HO_Complete* message from the Target ASN, it sends R6 *HO_Complete*
26 message to the Serving BS and releases the MS context.

27 **STEP 11**

28 The Data Path between the Serving BS and the Serving ASN GW is released.

29 **7.1.2.3.3 Handover Action Scenario 3: R6 HO_Cnf not received at the Target BS, or MS network
30   re-entry comes before R6 HO_Cnf at the Target BS**

31 The following call flow describes a successful Handover Action scenario where the R4 *HO_Cnf* message sent by the
32 Serving ASN to the Target BS was either delayed or not received. The MS completes network re-entry at one of the
33 Target BSs selected by the Serving ASN during the Handover Preparation phase. This scenario also applies to the
34 case that the MOB-HO_IND message is lost at air link and no *HO_Cnf* received at target BS. See also section
35 4.7.2.2.3

1
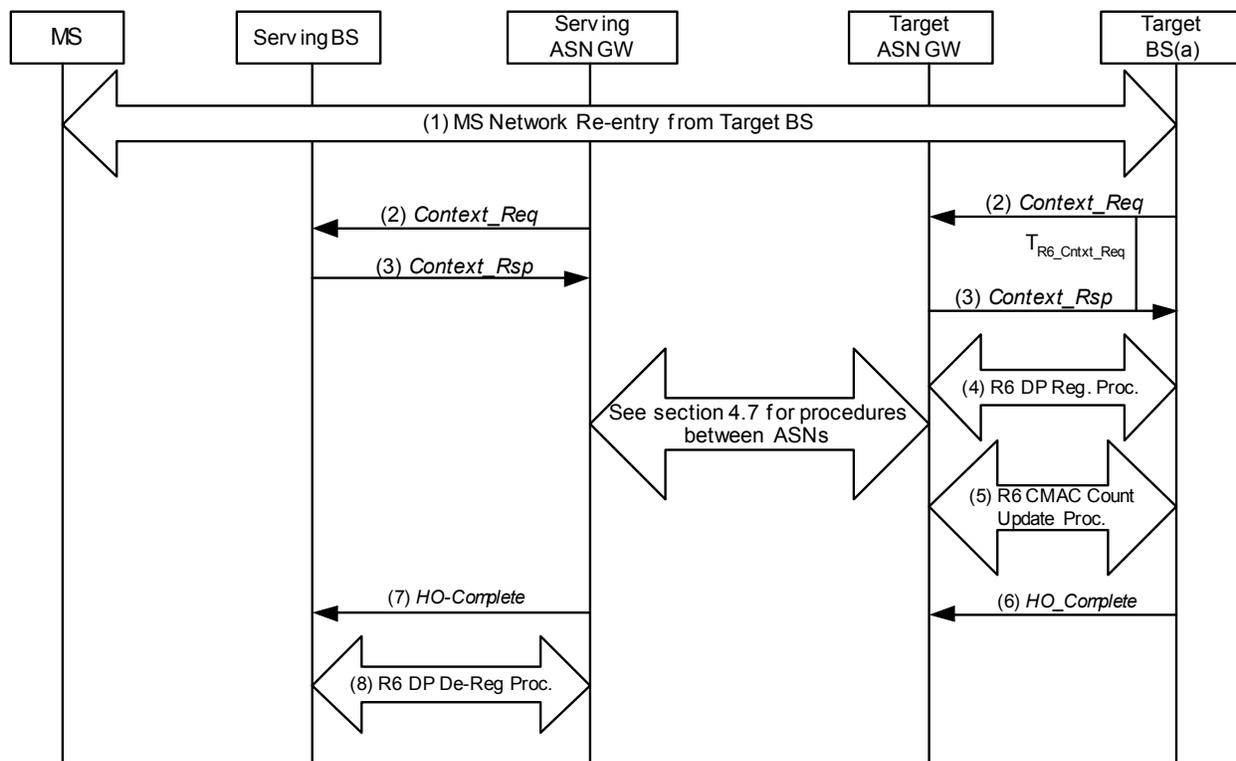
2 **Figure 7-18 – Handover Action Scenario 3 Profile A**

3 **STEP 1**

4 The MS completes network re-entry at Target BS selected by the Serving ASN during the Handover Preparation
5 phase.

6 **STEP 2**

7 The Target BS initiates a Context Request procedure with the Serving ASN GW to retrieve the latest MAC context
8 for the MS, by sending R6 *Context_Req* message to the Target ASN and starts the timer $T_{R6\_Cntxt\_Req}$. When the
9 Serving ASN receives the message, if it has not enough information requested, it may request the Serving BS for the
10 latest info by sending R6 *Context_Req* to the Serving BS.

11 Note that the Target BS may send more than one R6 *Context_Req* to different entity, such as authenticator, to
12 request information it needs. For more details see section 4.7.

13 **STEP 3**

14 The Serving BS and the Serving ASN GW return *Context_Rpt* message to the Target BS. The Target BS stops the
15 timer $T_{R6\_Cntxt\_Req}$ upon receiving this message.

16 **STEP 4**

17 If not already pre-established, the Target BS initiates Data Path Registration procedure with the Target ASN. Note:
18 This procedure may take place even if data path was pre-established and will follow the two-way handshake
19 process.

STEP 5

Simultaneously with starting the Data Path Registration procedure, the Target BS initiates CMAC Key Count Update procedure by sending R6 *CMAC_Key_Count_Update* message to the Target ASN GW with the latest CMAC Key Count value received from MS.

STEP 6

The Target BS may send an R6 *HO_Complete* message to the Target ASN to notify the completion of the handover.

STEP 7

When the Serving ASN receives the R4 *HO_Complete* message from the Target ASN, it sends R6 *HO_Complete* message to the Serving BS and releases the MS context.

STEP 8

The Data Path between the Serving BS and the Serving ASN GW is released.

7.1.2.3.4   Handover Action Scenario 4: MOB_HO-IND not received at Serving ASN

The following call flow describes a successful Handover Action scenario where the MOB_HO-IND sent by the MS to the Serving ASN was lost over the air and not received by the Serving ASN. The MS completes network re-entry at one of the target BSs selected by the Serving ASN during the Handover Action phase or a target BS which wasn't selected and notified of a an impending handover from the MS during the handover preparation but was notified later upon detection of the lost MOB_HO-IND message from the mobile, e.g a target BS which was included in the MOB_MSHO-REQ message sent by the MS but wasn't included in the MOB_BSHO-RSP message sent by the serving BS. See also section 5.7.2.1.6 HO Action Scenario 3.

1
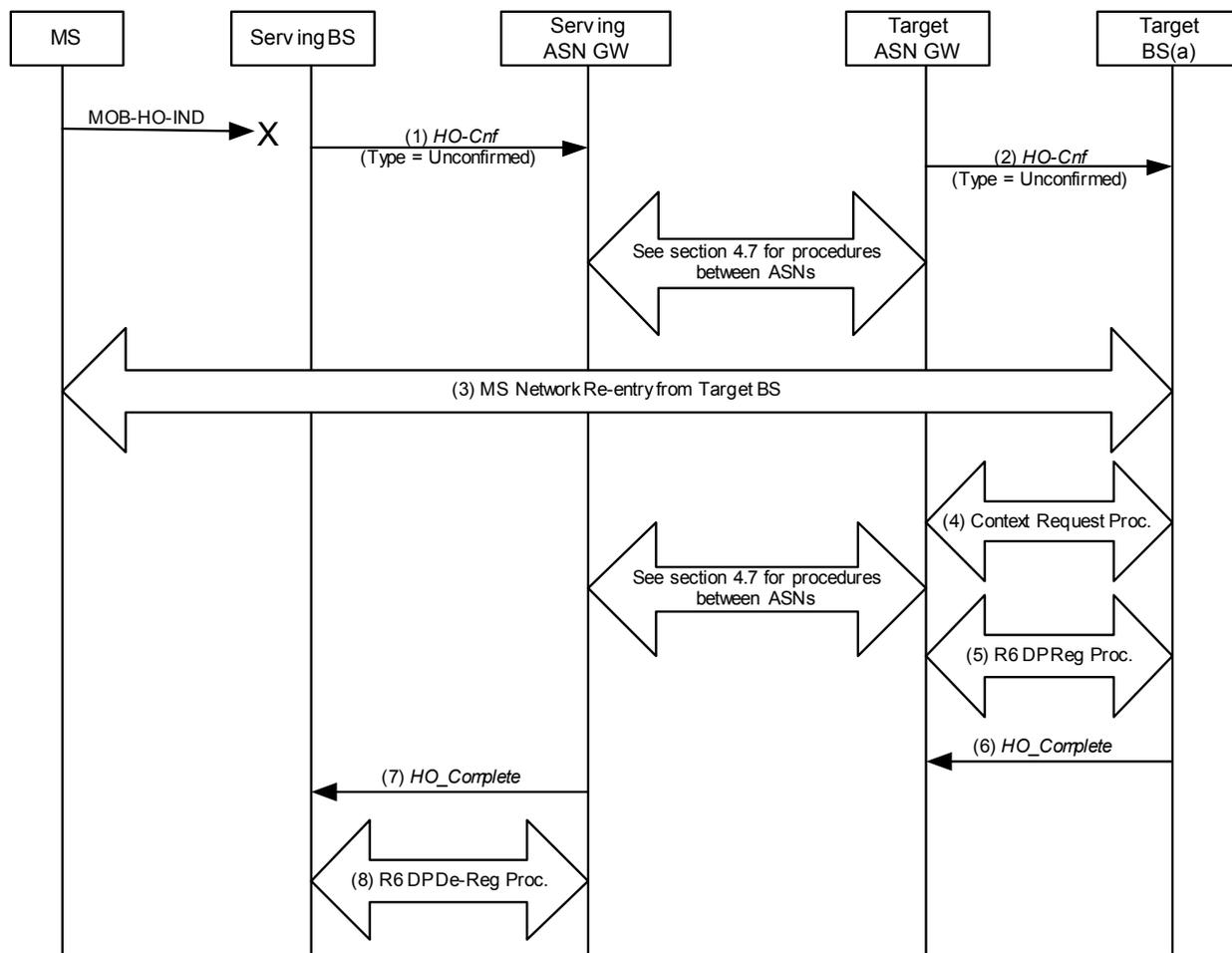
2 **Figure 7-19 – Handover Action Scenario 4 Profile A**

3 **STEP 1**

4 The MOB_HO-IND sent by the MS to the Serving BS is lost over the air and not received by the Serving BS. Upon
5 expiration of internal timer at the Serving BS, the Serving BS sends an R6 *HO_Cnf* message(s) with "Unconfirmed"
6 type to the set of the Serving ASN which will forward to the Target ASN(s) controlling the candidate Target BSs
7 which were indicated in the MOB_BSHO-RSP or MOB_BSHO-REQ and starts the $T_{R6\_HO\_Conf}$ timer. The R6
8 *HO_Cnf* message may also be sent to Target ASN(s) that were not notified of a potential impending handover from
9 the MS during the preparation phase and were not included in the MOB_BSHO-REQ or MOB_BSHO-RSP
10 messages.

11 **STEP 2**

12 The Target ASN(s) sends R6 *HO_Cnf* message to the candidate Target BSs selected in step 1. The R6 *HO_Cnf*
13 message contains the HO_Indication Type set to "Unconfirmed", AK context, and latest MAC context information.

14 **STEP 3**

15 The MS completes network re-entry at one of the target BSs selected by the Serving ASN during the Handover
16 Action phase, or at a target BS controlled by a target ASN notified of an impending handover from the MS after the
17 serving BS detects the loss of communication with the MS due to loss of the MOB_HO-IND message.

1 **STEP 4**

2 According to its obtained context of the MS, the Target MS may require to some entities (e.g. Authenticator) to get
3 some context by Context Request procedure.

4 **STEP 5**

5 The Data Path registration procedure will be initiated to establish the data path towards Anchor DPF.

6 **STEP 6**

7 The Target BS may send an R6 *HO_Complete* message to the Target ASN GW to expedite release of MS context
8 information. The Target ASN will forward this message to the Serving ASN.

9 **STEP 7**

10 The Serving ASN GW send R6 *HO_Complete* message to the Serving BS. Upon receipt of this message, the Serving
11 BS stops timer $T_{R6\_HO\_Conf}$ if it was started and releases MS context.

12 **STEP 8**

13 If the data path is still maintained, upon completing Data Path Registration procedure with the Target ASN, the
14 Anchor ASN SHALL initiate Data Path De-Registration procedure with the old Serving ASN. Also the Data Path
15 between the Serving ASN GW and Serving BS of the MS is de-registered.

16 **7.1.2.3.5 R6 Message Definitions for HO Action Phase**

17 This section describes the R6 message definitions for the HO Action Phase

18 The content of *HO_Cnf* message from Serving BS to Serving ASN GW appears in Table 7-16.

19 **Table 7-16 – R6 HO_Cnf Message Format (SBS → Serving ASN GW)**

IE	Reference	M/O	Notes
HO Confirm Type	5.3.2.76	M	802.16e mandatory parameter . Possible values are: Confirm, Unconfirm, Cancel, (resume old connection) Reject (Target BS proposed not accepted).
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
Target BS Info (One or more)	5.3.2.26	M	Contains relevant Target BS context in the nested Ies. If HO Confirm Type = Unconfirm, the Serving BS sends HO Confirm with all the candidate Target BS(s) which were indicated in the MOB_BSHO-RSP or MOB_BSHO-REQ.
>BS ID	5.3.2.25	M	ID of the selected Target BS
>Estimated HO Start	Defined in [2]	O	If MS include this information in its HO-indication message, this TLV SHALL be included

IE	Reference	M/O	Notes
>HO ID	Defined in [2]	O	ID assigned for use in initial ranging to the target BS once this BS is selected as the target BS.
			If MS include this information in its HO-indication message, this TLV SHALL be included
>SF Info (one or more)	5.3.2.185	O	Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	O	SFID associated with the Service Flow
>>SA Descriptor	5.3.2.170	O	TEK related Context info.
			TEK context might be included if there is a desire to share TEKs between the Serving and Target BS upon HO.
			If it is already sent in the HO Preparation phase, this IE can be omitted.
>>SDU Info (one or more)	5.3.2.176	O	Each element in the list contains context of an SDU affected by the Data Integrity Operations.
			For Type-1 and Type-2 Data Path.
>>>Block SN	Not defined in Release 1.0.0	O	Sequence Number of the last transmitted ARQ block context for Data Integrity. Relevant only for DL U-Cast SF.
			For both Type 1 DP and Type-2 DP is used, this TLV is included.
>ARQ Context	Not defined in Release 1.0.0	O	The dynamic state variable and the outstanding ARQ blocks may be required to be transferred over from the serving BS to the target BS via the ASN-GW to ensure the data integrity of the ARQ operation even for type-1 data path.

1

2   The content of R6 *Path_Reg_Req* message appears in Table 7-17. If Pre-Registration took place prior to
3   Registration, none of the optional TLVs specified below needs to be included in the message.

4   **Table 7-17 – R6 Path_Reg_Req Message Format**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration (HO, Initial Entry, etc.)
MS Info	5.3.2.103		Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>Anchor GW ID	5.3.2.10	O	Identifies the Anchor ASN GW
>Data Path Info	5.3.2.45	M	Data Path Info for per-MS or per-BS granularity tunnel
>SF Info (one or more)	5.3.2.185		Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	M	SFID associated with the Service Flow

IE	Reference	M/O	Notes
>>CID	5.3.2.29	O	New CID associated with the Service Flow. If Type-2 Data Path is used, this TLV SHALL be included. Otherwise, it is optional. It is included only in the message originated from the BS.
>>Data Path Info	5.3.2.45	M	Data Path Info for per-flow granularity tunnel
Target BS Info	5.3.2.26	M	Contains relevant Target BS context in the nested Ies.
>BS ID	5.3.2.25	M	Target BS ID

1 The content of *Path_Reg_Rsp* message is shown in Table 7-18. If Pre-Registration took place prior to Registration,
2 none of the optional TLVs specified below SHALL be included in the message.

3 **Table 7-18 – R6 Path_Reg_Rsp Message Format**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration (HO, Initial Entry, etc.)
MS Info	5.3.2.103		Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>Anchor GW ID	5.3.2.10	O	Identifies the Anchor ASN GW
>Data Path Info	5.3.2.45	O	Data Path Info for per-flow granularity tunnel
>SF Info (one or more)	5.3.2.185		Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	M	SFID associated with the Service Flow
>>Data Path Info	5.3.2.45	M	Data Path Info for per-flow granularity tunnel
Target BS Info	5.3.2.26	M	Contains relevant Target BS context in the nested Ies.
>BS ID	5.3.2.25	M	Target BS ID

4 The content of *Path_Reg_Ack* message is shown in Table 7-19.

5 **Table 7-19 – R6 Path_Reg_Ack Message Format**

IE	Reference	M/O	Notes
MS Info	5.3.2.103		Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>Data Path Info	5.3.2.45	O	Data Path Info for per-MS or per-BS granularity tunnel
>SF Info (one or more)	5.3.2.185		Each IE of the list contains context of a particular SF.
>>SFID	5.3.2.184	O	SFID associated with the Service Flow
>>Result Code	5.3.2.154	O	Indication whether this SF can be supported

IE	Reference	M/O	Notes
>>>Data Path Info	5.3.2.45	O	Data Path Info for per-flow granularity tunnel

1　The content of HO_Complete message from Target BS to Target ASN GW is shown in Table 7-20.

2　**Table 7-20 – R6 HO_Complete Message Format (TBS → Target ASN GW)**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Result of the HO
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
>SDU Info (one or more)	5.3.2.176	O	Each element in the list contains context of an SDU affected by the Data Integrity Operations. For Type-1 Data Path.
>>SDU SN	5.3.2.178	O	Last transmitted SDU sequence number

3　The content of HO_Complete message from Serving ASN GW to Serving BS is shown in Table 7-21.

4　**Table 7-21 – R6 HO_Complete Message Format (Serving ASN GW → SBS)**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Result of the HO
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)
Serving BS Info	5.3.2.26	M	Contains Serving BS context in the nested Ies.
>BS ID	5.3.2.25	M	Serving BS ID

5　The content of R6 *Path_Dereg_Req* message is shown in Table 7-22.

6　**Table 7-22 – R6 Path_Dereg_Req Message Format**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration (HO, Initial Entry, etc.)
MS Info	5.3.2.103		Contains HO-related MS context in the nested Ies.
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)

7　The content of R6 *Path_Dereg_Rsp* message is shown in Table 7-23.

8　**Table 7-23 – R6 Path_Dereg_Rsp Message Format**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Describes type of the Registration (HO, Initial Entry, etc.)
MS Info	5.3.2.103		Contains HO-related MS context in the nested Ies.

IE	Reference	M/O	Notes
>MSID	5.3.2.102	O	6 octet MSID (MAC Address)

1 **7.1.2.4 HO Cancellation Procedure**

2 **7.1.2.4.1 HO Cancellation Scenario 1: Serving and Anchor ASN GW are not co-located and the**
3 **"Unselected Target ASN GW" receives the R4 HO_Cnf from the Serving ASN GW.**
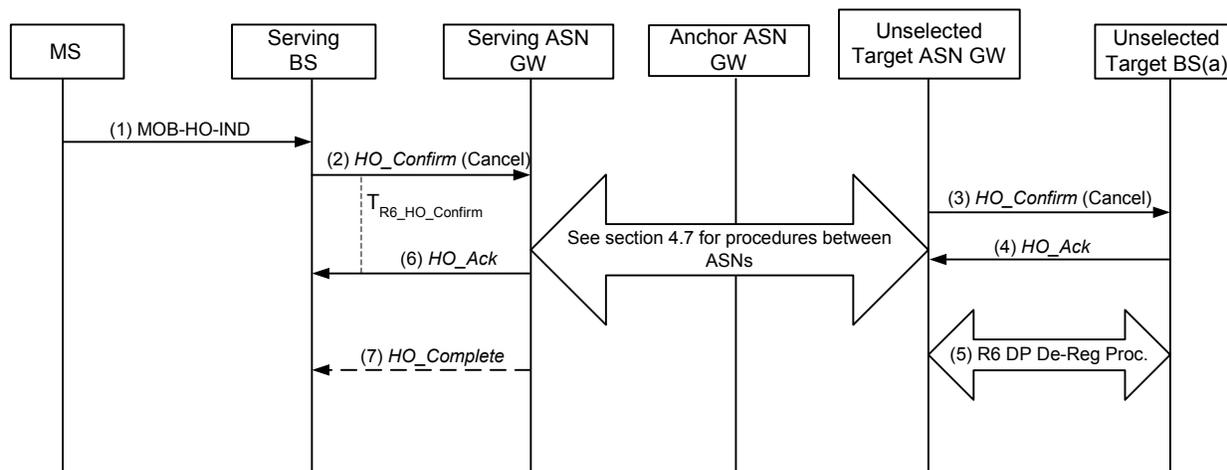

4

5 **Figure 7-20 – HO Cancellation Scenario 1 Profile A**

6 **STEP 1**

7 The MS sends MOB_HO-IND to the Serving BS. In the MOB_HO-IND, the MS can indicate to the Serving BS
8 with either of the following two possibilities:

9   a. The selected target BS that the MS chooses to perform the handover, or

10   b. The MS decides to cancel the handover procedure. In this case, the selected target BS is the Serving BS

11 **STEP 2**

12 Upon receiving MOB_HO-IND message with HO_IND_type set to 0b01: HO Cancel from MS, the Serving BS
13 SHALL transmit R6 *HO_Cnf* message to notify the Serving ASN GW which in turn notifies the previously selected
14 potential Target BSs which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP message to de-allocate the
15 reserved system resources that are prepared for the MS to handover. After sending the message, the Serving BS
16 awaits *HO_Ack* by starting the T_{HO_Conf}. If the timer expires, the Serving BS may re-send the R4 *HO_Cnf*. After a
17 pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf*. The Target BS SHALL
18 perform the local clean up if R4 *HO_Cnf* is never received from the Serving BS. The message is routed to the Target
19 ASN GW by the Serving ASN GW per the procedures described in section 4.7.

20 **STEP 3**

21 Target ASN GW routes the R4 *HO_Cnf* message to the Target BSs.

22 **STEP 4**

23 Target BS receives the R4 *HO_Cnf* with HO_Indication type set to "Cancel". Target BS sends R4 *HO_Ack* to the
24 Serving BS and may release the system resources that were pre-allocated to support the MS handover.

1 **STEP 5**

2 The Target BS may initiate Path Deregistration procedure. Refer to section 7.1.2.2 for more details.

3 **7.1.2.4.2 HO Cancellation Scenario 2: Serving and Anchor ASN GW are co-located and the**
4 **"Unselected Target ASN GW" receives the R4 HO_Cnf from the Serving ASN GW**

5
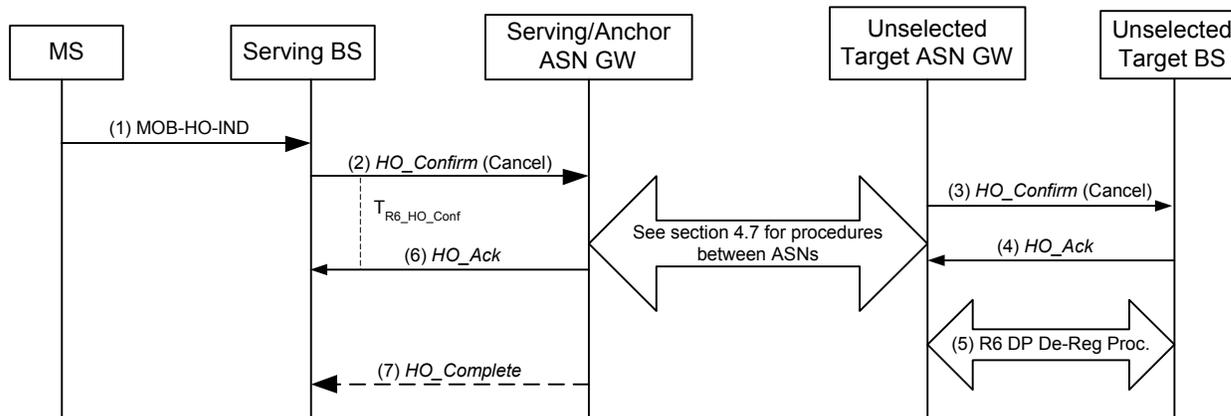
6 **Figure 7-21 – HO Cancellation Scenario 2 Profile A**

7 **STEP 1**

8 The MS sends MOB_HO-IND to the Serving BS. In the MOB_HO-IND, the MS can indicate to the Serving BS
9 with either of the following two possibilities:

10   a.   The selected target BS that the MS chooses to perform the handover, or

11   b.   The MS decides to cancel the handover procedure. In this case, the selected target BS is the Serving BS

12 **STEP 2**

13 Upon receiving MOB_HO-IND message with HO_IND_type set to 0b01: HO Cancel from MS, the Serving BS
14 SHALL transmit R6 *HO_Cnf* message to notify the Serving or Anchor ASN GW which in turn notifies the
15 previously selected potential Target BSs which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP
16 message to de-allocate the reserved system resources that are prepared for the MS to handover. After sending the
17 message, the Serving BS awaits *HO_Ack* by starting the T_{HO_Conf}. If the timer expires, the Serving BS may re-send
18 the R4 *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf*.
19 The Target BS SHALL perform the local clean up if R4 *HO_Cnf* is never received from the Serving BS. The
20 message is routed to the Target ASN GW by the Serving / Anchor ASN GW per the procedures described in section
21 4.7.

22 **STEP 3**

23 Target ASN GW routes the R4 *HO_Cnf* message to the Target BSs.

24 **STEP 4**

25 Target BS receives the R4 *HO_Cnf* with HO_Indication type set to "Cancel". Target BS sends R4 *HO_Ack* to the
26 Serving BS via Target ASN GW, Anchor / Serving ASN GW. Target BS may release the system resources that were
27 pre-allocated to support the MS handover.

28 **STEP 5**

29 The Target BS may initiate Path Deregistration procedure. Please refer to R6 Path Deregistration (section 7.1.2.2)
30 for more details.

1 **7.1.2.4.3 HO Cancellation Scenario 3: Serving and Anchor ASN GW are co-located and the**
2 **"Unselected Target ASN GW" does not receive the R4 HO_Cnf from the Serving ASN**
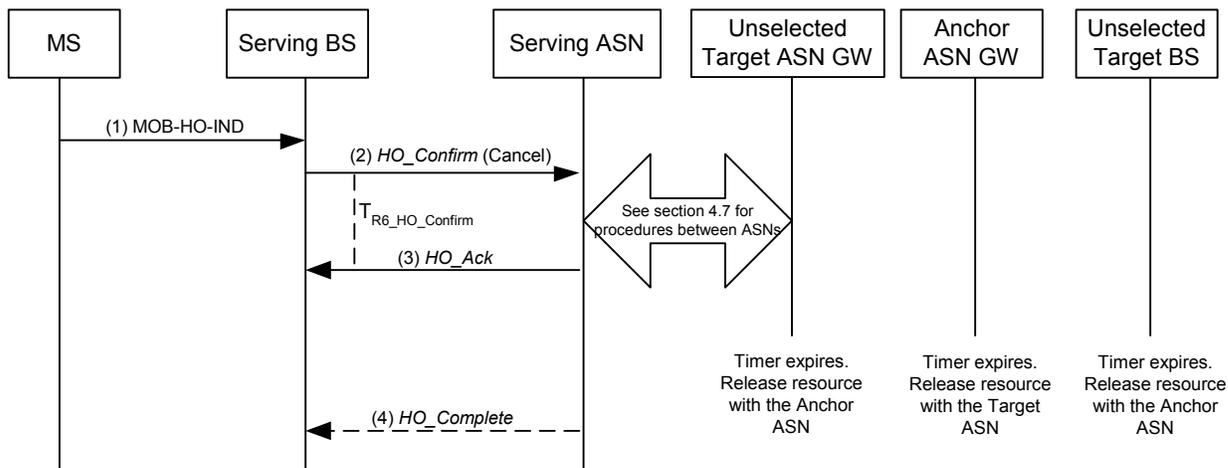
3

4 **Figure 7-22 – HO Cancellation Scenario 3 Profile A**

5 **STEP 1**

6 The MS sends MOB_HO-IND to the Serving BS. In the MOB_HO-IND, the MS can indicate to the Serving BS
7 with either of the following two possibilities:

8   a.   The selected target BS that the MS chooses to perform the handover, or

9   b.   The MS decides to cancel the handover procedures, in this case, the selected target BS is the Serving BS

10 **STEP 2**

11 Upon receiving MOB_HO-IND message with HO_IND_type set to 0b01: HO Cancel from MS, the Serving BS
12 SHALL transmit R6 *HO_Cnf* message to notify the Serving or Anchor ASN GW which in turn notifies the
13 previously selected potential Target BSs which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP
14 message to de-allocate the reserved system resources that are prepared for the MS to handover. After sending the
15 message, the Serving BS awaits *HO_Ack* by starting the T_{HO_Conf}. If the timer expires, the Serving BS may re-send
16 the R4 *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the R4 *HO_Cnf*.

17 **STEP 3**

18 The Target BS does not receive the R4 *HO_Cnf*. Target BS releases the system resources that were pre-allocated to
19 support the MS handover.

20 **STEP 4**

21 After the timer associated with the pre-registered DP expires, the Target BS may initiate the R4 Path De Registration
22 procedure. Please refer to section x.x.x.x for more details.

1 **7.1.2.5 Uncontrolled HO**
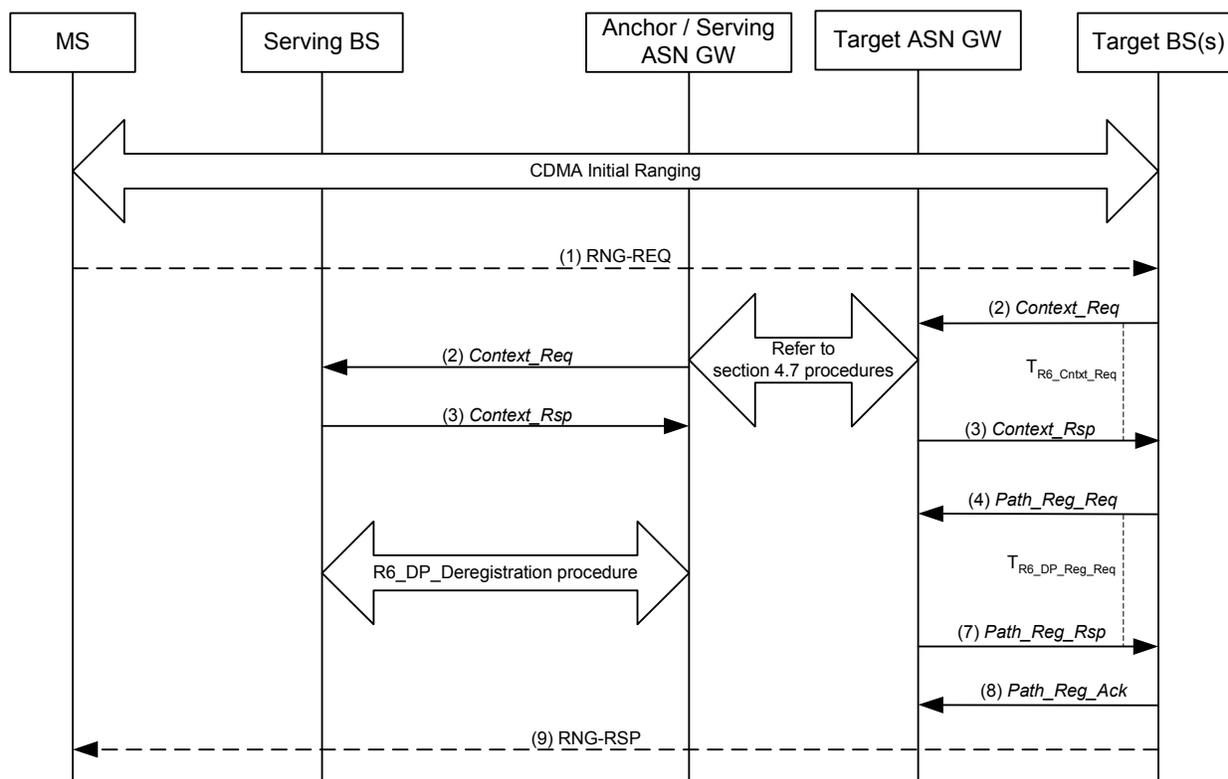
2

3 **Figure 7-23 – Uncontrolled HO Profile A**

4 Note: Please refer to section 7.1.2.2 for R6 Path Deregistration procedure.

5 **STEP 1**

6 MS sends RNG_REQ message to the selected Target BS. The RNG_REQ message SHALL have the information
7 about the old BS to which it was communicating before the HO.

8 **STEP 2**

9 Upon receiving RNG_REQ message from MS, the new (Target) BS SHALL transmits R6 *Context_Req* message to
10 notify the Anchor ASN GW that an uncontrolled HO of MS has taken place.

11 **STEP 3**

12 The ASN GW transmits R6 *Context_Rpt* to the Target BS. The message SHALL contain MS session information
13 (such as SBC context, REG context, SF context, TEK context etc) necessary to set up a data path (or paths) for MS.
14 ASN GW obtains TEK context from the serving BS.

15 **STEP 4**

16 The Target BS transmits R6 *Path_Reg_Req* message via Target ASN GW to Anchor ASN GW, to request setup of a
17 data path for HO. The message SHALL include the updated MS session context, such as SFID/CID mapping
18 information.

19 **STEP 5**

20 The ASN GW transmits R6 *Path_Dereg_Req* message. The message forces the Serving BS to stop forwarding the
21 downlink traffic of the specified MS, and to report the buffer status to the Anchor ASN GW.

STEP 6

The Serving BS reports the last buffer status to the Anchor ASN GW by transmitting R6 *Path_Dereg_Rsp* message.

STEP 7

The ASN GW transmits R6 *Path_Reg_Rsp* message which contains the updated R6 data path information.

STEP 8

On receiving R6 *Path_Reg_Rsp* message, the Target BS transmits R6 *Path_Reg_Ack* to the Anchor ASN GW to trigger the downlink data transmission.

STEP 9

Finally, the Target BS sends RNG_RSP to MS. The message SHALL contain the HO optimization flag to skip the unnecessary network re-entry transactions.

7.1.2.6   R6 HO Timer and Timing

This section identifies the timer entities participating in the R6 HO procedures. The following timers are defined over R6:

- $T_{R6\_DP\_Pre\_Reg}$: is started by the Target BS initiating pre-establishment of the data path for an MS, upon sending the R6 *Path_Prereg_Req* message and is stopped upon receiving a corresponding R6 *Path_Prereg_Rsp* message.

- $T_{R6\_DP\_Pre\_Rsp}$: is started by the Target ASN GW responding to pre-establishment of the data path for an MS, upon sending the R6 *Path_Prereg_Rsp* message to the Target BS and is stopped upon receiving a corresponding R6 *Path_Prereg_Ack* message.

- $T_{R6\_HO\_Req}$: is started by a serving BS upon sending the R6 *HO_Req* message for an MS to the Serving ASN GW and is stopped upon receiving a corresponding R6 *HO_Rsp* message from the Serving ASN GW.

- $T_{R6\_HO\_Ack}$: is started by target BS upon sending the R6 *HO_Rsp* message for an MS to the Target ASN GW and is stopped upon receiving a corresponding R6 *HO_Ack* message from the Target ASN GW.

- $T_{R6\_DP\_Reg\_Req}$: is started by the Target BS to initiate establishment or provide confirmation of the data paths for an MS, upon sending the R6 *Path_Reg_Req* message, and is stopped upon receiving a corresponding R6 *Path_Reg_Rsp* message.

- $T_{R6\_DP\_Reg\_Rsp}$: is started by the Target ASN GW upon sending the R6 *Path_Reg_Rsp* message if no data path has been pre-established for the MS, and is stopped upon receiving a corresponding R6 *Path_Reg_Ack* message.

- $T_{R6\_DP\_Dereg\_Req}$: is started by the Serving ASN GW after completion of the Data Path Registration procedure for an MS, upon sending the R6 *Path_Dereg_Req* message to the Serving BS, and is stopped upon receiving a corresponding R6 *Path_Dereg_Rsp* message from the Serving BS.

- $T_{R6\_CMAC\_Key\_Count\_Upd}$: is started by the Target (now new Serving) BS after MS completes network re-entry, upon sending the R6 *CMAC_Key_Count_Update* message to the Target ASN GW, and is stopped upon receiving a corresponding R6 *CMAC_Key_Count_Update_Ack* message from the Target ASN GW.

- $T_{R6\_HO\_Cnf}$: is started by the Serving BS after receiving MS_HO_IND message, upon sending the R6 *HO_Cnf* message to the Serving ASN GW, and is stopped upon receiving a corresponding R6 *HO_Ack* message from the Serving ASN GW.

- $T_{R6\_Cntxt\_Req}$: is started by the Target BS requesting context for a specific MS, upon sending the R6 *Context_Req* message to the Target ASN GW and is stopped upon receiving a corresponding R6 *Context_Rpt* message.

- $T_{R6\_HO\_Req\_Target}$: is started by the Target ASN GW upon sending all the R6 *HO_Req* messages to the candidates BSs. When this timer expires, the Target ASN GW sends R4 *HO_Rsp* message to the Serving ASN according to the R6 *HO_Rsp* messages received and discards those BSs whose responses messages are not received.

1 • T$_{R6\_ASN\_HO\_Conf}$: is started by the Target ASN GW upon sending the R6 *HO_Cnf* message provide
2 confirmation of the HO for an MS. It is stopped upon receiving a corresponding R6 *HO_Ack* message from
3 the Target BS.

4 • T$_{R6\_HO\_Complete}$: is started by the Target BS upon sending *HO_Complete* message to Target ASN GW to
5 complete the handoff procedure. It is stopped upon receiving the corresponding *HO_Ack* message.

6 • T$_{R6\_Path\_Modification\_Req}$: is started by the Anchor / Serving ASN GW upon initiating *Path_Modification_Req* to
7 the Serving BS. It is stopped after receiving *Path_Modification_Rsp*.

8 • T$_{R6\_Cntxt\_Req}$: is started by the Target BS upon initiating *Context_Req* to the Anchor ASN GW. It is stopped
9 after receiving *Context_Rpt* from the Anchor ASN GW.

10 Table 7-24 shows the default value of timers and also indicates the range of the recommended duration of these
11 timers.

12 **Table 7-24 – HO Timer Values for R6**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T$_{R6\_DP\_Pre\_Reg}$	TBD		TBD
T$_{R6\_DP\_Pre\_Rsp}$	TBD		TBD
T$_{R6\_HO\_Req}$	TBD		TBD
T$_{R6\_HO\_Ack}$	TBD		TBD
T$_{R6\_DP\_Reg\_Req}$	TBD		TBD
T$_{R6\_DP\_Reg-Rsp}$	TBD		TBD
T$_{R6\_Path\_De-Reg\_Req}$	TBD		TBD
T$_{R6\_Path\_De-Reg\_Rsp}$	TBD		TBD
T$_{R6\_CMAC\_Key\_Count\_Upd}$	TBD		TBD
T$_{R6\_HO\_Conf}$	TBD		TBD
T$_{R6\_Cntxt\_Req}$	TBD		TBD
T$_{R6\_HO\_Req\_Target}$	TBD		TBD
T$_{R6\_HO\_Directive}$	TBD		TBD
T$_{R6\_ASN\_HO\_Conf}$	TBD		TBD
T$_{R6\_HO\_Complete}$	TBD		TBD
T$_{R6\_Path\_Modification\_Req}$	TBD		TBD

13 **7.1.2.7   R6 HO Error Condition**

14 **7.1.2.7.1 Timer Expiry**

15 The following table shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each
16 timer expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
17 should be performed as indicated in Table 7-29.

18 **Table 7-25 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T$_{R6\_DP\_Pre\_Reg}$	Target BS	No action required.

Timer	Entity where Timer Started	Action(s)
T$_{R6\_DP\_Pre\_Rsp}$	Target ASN GW	No action required.
T$_{R6\_HO\_Req}$	Serving BS	If no Target BS can be reached, the Serving BS SHALL send MS a MOB_BSHO-RSP with Mode set to 0b111
T$_{R6\_HO\_Ack}$	Target BS	No action required.
T$_{R6\_DP\_Reg\_Req}$	Target BS	The Target BS SHALL force MS to perform initial network entry
T$_{R6\_DP\_Reg-Rsp}$	Target ASN GW	ASN GW shall defer sending the downlink packets until it receives any packets for MS from Target (new Serving) BS. ASN GW shall reset data paths for MS if no packets are received until a pre-specified system timer expires.
T$_{R6\_Path\_De\_Reg\_Req}$	Serving ASN GW	No action required
T$_{R6\_Path\_De\_Reg\_Rsp}$		
T$_{R6\_CMAC\_Key\_Count\_Upd}$	Target BS	BS shall force MS to perform initial network entry
T$_{R6\_HO\_Conf}$	Serving BS	No action required
T$_{R6\_Cntxt\_Req}$	Target BS	BS shall force MS to perform initial network entry.
T$_{R6\_HO\_Req\_Target}$	Target ASN GW	No action required.
T$_{R6\_HO\_Directive}$	ASN GW sending out *HO_Directive* message	The ASN GW may retry HO to another Target BS.
T$_{R6\_ASN\_HO\_Conf}$	Target ASN GW	No action required
T$_{R6\_HO\_Complete}$	Target BS(s)	No action required
T$_{R6\_Path\_Modification\_Req}$	ASN GW	No action required
T$_{R6\_Path\_Reg\_Rsp}$	ASN GW	No action required

7.1.2.7.2 R6 Path_Reg_Rsp Error

Upon receipt of the R6 *Path_Reg_Req* message, if the Target ASN GW is unable to support the requested establishment of the data path(s), then it SHALL send a R6 *Path_Reg_Rsp* message with suitable error code.

Upon receipt of the R6 *Path_Reg_Rsp* message with suitable error code, the Target BS SHALL stop T$_{R6\_DP\_Reg\_Req}$ (if running). The Target BS MAY re-send the R6 *Path_Reg_Req* message according to the error code. If the Target BS does not resend the R6 *Path_Reg_Req* message or if subsequent attempts are also unsuccessful, the Target BS SHALL force the MS to perform a full network re-entry.

7.1.2.7.3 R6 Path_Prereg_Rsp Error

Upon receipt of the R6 *Path_Prereg_Req* message, if the Target ASN GW is unable to support DP pre-establishment, then it SHALL send a R6 *Path_Prereg_Rsp* message with suitable error code.

Upon receipt of the R6 *Path_Prereg_Rsp* message with suitable error code, the Target BS SHALL stop $T_{R6-DP\_Pre-Reg}$ (if running).

7.1.2.8 R4 HO_Rsp Error

Upon receipt of the R4 *HO_Req* message, if the Target BS is unable to support the HO, then it SHALL send R4 *HO_Rsp* message with suitable error code included in the Result Code TLV. Upon receipt of the R4 *HO_Rsp*

1 message indicating HO cannot be supported, the Serving BS SHALL stop $T_{R4\text{-}HO\_Request}$ (if running). The Serving BS
2 MAY re-send the R4 *HO_Req* message to a different Target BS. If the Serving BS does not re-send the R4 *HO_Req*
3 message, or if all subsequent Target BSs cannot support the HO, in the case of MS Initiated handover, the Serving
4 BS SHALL send a MOB_BSHO_RSP with mode = 0b111 to the MS.

5 7.2   ASN Profile B

6 Since profile B is a black box within an ASN and since R6 is not exposed in profile B, no R6 specific call flows and
7 optimizations are provided for this profile in this section. However, the R4 specific call flows and text in section 4
8 are applicable to profile B.

9 7.2.1   RRM

10 In Profile B, ASN internal signaling over R6 is not exposed. Hence, the RRM procedures are handled internally
11 within the ASN. In Profile B realizations with multi-nodes option, if the RRA and RRC are co-located, similar to
12 Profile C, a "RRC Relay" function may be introduced within the Profile B ASN.

13 7.3   ASN Profile C

14 7.3.1   Authentication and Re-Authentication

15 From Authentication and Re-authentication perspective, profiles A and C are equivalent since the Authenticator
16 resides in the ASN-GW in both profiles. Refer to section TBD.

17 7.3.2   RRM

18 7.3.2.1   R6: Per-BS Spare Capacity Reporting Procedure

19 This procedure MAY be used by a BS (i.e. by the RRC in the BS) to retrieve information about the current load
20 situation of any other BS, in particular of those neighboring Base Stations which MAY become candidate Target
21 BSs (TBSs) for Handover decisions.

22 Since the BS cannot communicate directly to neighboring BSs, it SHALL send the RRM primitives to a Relay RRC
23 in an ASN GW. The Relay RRC SHALL forward that message to the destination BS, or to another Relay RRC if the
24 destination BS can't be reached directly.

25 So the same RRM-Spare-Capacity-Req/Report procedure SHALL also be used by the "Relay" RRC in the ASN GW
26 to request Spare Capacity reports from destination Base Stations, in response to *Spare_Capacity_Req* messages
27 received from source BSs.

28 Figure 7-24 shows the application of this procedure between two BSs (Requesting BS and Reporting BS) with an
29 ASN GW performing the Relay RRC function.

1
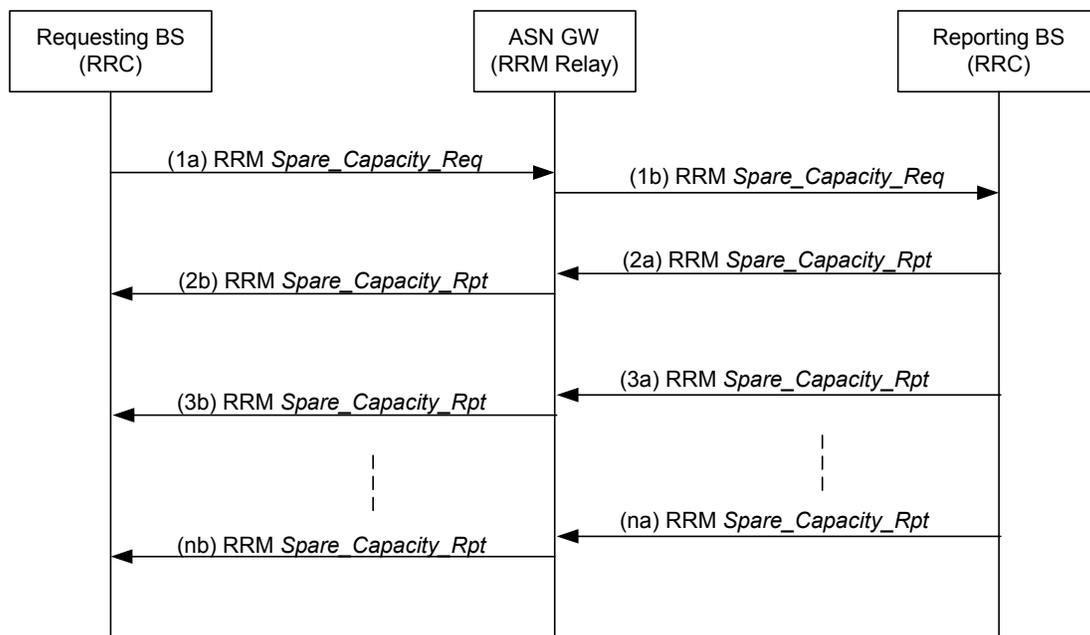
2 **Figure 7-24 – Per-BS Spare Capacity Reporting Procedure**

3 **STEP 1 a, b**

4 The "requesting BS" sends an RRM R6 *Spare_Capacity_Req* to the ASN GW, requesting it to report about the
5 available radio resources of a certain "Reporting BS"; reporting SHALL be done once, or periodically, or event
6 driven.

7 ASN GW, in its role as RRC Relay, sends the same RRM R6 *Spare_Capacity_Req* to the indicated Reporting BS. If
8 that BS can't be reached directly, ASN GW will send the request to other ASN GW working as RRC Relay.

9 **STEP 2 a, 2b, 3a, 3b, …, na, nb**

10 The Reporting BS sends RRM *Spare_Capacity_Rpt* to ASN-GW, either in direct response to the Request, or
11 subsequently in response to predefined events. ASN-GW relays that message to the Requesting BS.

12 Signaling between RRC Relays over R4 is as specified in section 4.

13 **7.3.2.1.1 R6 Messages for Per-BS Spare Capacity Reporting Procedure, Profile C**

14 The message definition for the RRM R6 *Spare_Capacity_Req* message is the same as the corresponding R4 message
15 definition as specified in section 4.9.3.1.1 – except that on R6, the RRM R6 *Spare_Capacity_Req* message sent from
16 ASN GW to a BS can include a single BS only.

17 **Table 7-26 – RRM R6 Spare_Capacity_Req**

IE	Reference	M/O	Notes
RRM Spare Capacity Report Type	Section 5.3.2.164	M	
BS ID (one or more)	Section 5.3.2.25	M	Identifier of the BS whose Spare Capacity SHALL be reported. In the message from a BS to an RRC Relay in ASN GW, multiple BS ID TLVs MAY be included. In the message from ASN GW to a BS, a single BS only can be included.

IE	Reference	M/O	Notes
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. If the optional reporting characteristics field is not included, then the *Spare_Capacity_Rpt* SHALL be sent only once by the reporting entity. – TLV may be included based on local RRC policy. Decision to include this TLV is implementation specific.
RRM Averaging Time T	Section 5.3.2.158	O	The Time T is used by BS (RRA) as the measurement interval for producing the information requested by RRC. – If omitted, the BS SHALL apply a default value.
RRM Reporting Period P	Section 5.3.2.163	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
RRM Absolute Threshold Value J	Section 5.3.2.157	O	The threshold value J is used by BS (RRA) as the absolute threshold for reporting.
RRM Relative Threshold RT	Section 5.3.2.161	O	The threshold value RT is used by BS (RRA) to keep track of the threshold from the last measurement period.

1 The message definition for the RRM R6 *Spare_Capacity_Rpt* message is the same as the corresponding R4 message
2 definition as specified in section 4.9.3.1.1.

3 Signaling between RRC Relays over R4 is as specified in section 4.9.

4 **7.3.2.2   R6: Per-BS Radio Configuration Update Reporting Procedure, Profile C**

5 This procedure MAY be used by a BS to report some critical radio resource configuration update to the serving
6 BS(RRC), such as DCD, UCD burst profile changes.

1
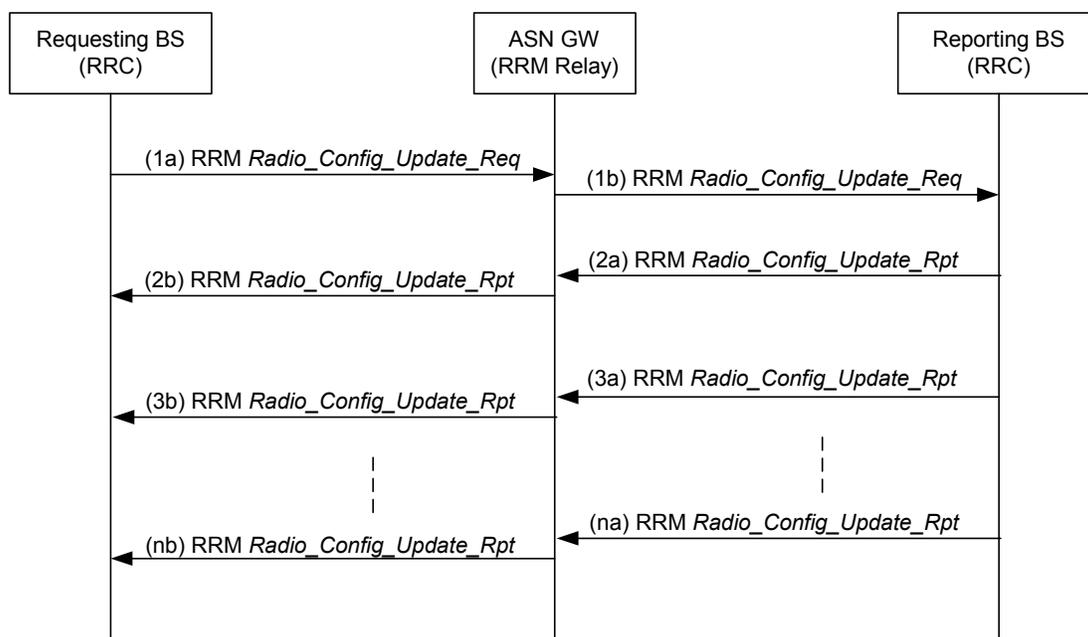
2 **Figure 7-25 – Per-BS Radio Configuration Update Reporting Procedure**

3 **STEP 1a, 1b**

4 The "requesting BS" sends an "RRM: R6 Radio configuration update-Request" to the ASN GW, requesting it to
5 report about the radio configuration parameters of one or more "Reporting BSs"; reporting SHALL be done once, or
6 periodically, or event driven. to indicate the Radio Configuration parameters whenever these change.

7 ASN GW, in its role as RRC Relay, sends the same "RRM: R6 Radio configuration update-Request" to the
8 indicated reporting BSs. If a BS can't be reached directly, ASN GW will send the request to other ASN GW working
9 as RRC Relay.

10 **STEP 2a, 2b, 3a, 3b, …, na, nb**

11 A reporting BS sends "RRM: R6 Radio Configuration update-Report" to ASN-GW, either in direct response to the
12 Request, or subsequently in response to predefined events. ASN-GW relays that message to the Requesting BS.

13 **7.3.2.2.1 R6 Messages for Per-BS Radio Configuration Update Procedure, Profile C**

14 The message definition for the RRM R6 *Radio_Config_Update_Req* messages is the same as the corresponding R4
15 message definition as specified in section 4.9.3.2.1 – except that on R6, the RRM R6 *Radio_Config_Update_Req*
16 message sent from ASN GW to a BS can include a single BS only.

17 **Table 7-27 – RRM R6 Radio_Config_Update_Req**

IE	Reference	M/O	Notes
BS ID (one or more)	Section 5.3.2.25	M	Identifier of the BS whose Radio-Configuration SHALL be reported. In the message from a BS to an RRC Relay in ASN GW, multiple BS ID TLVs MAY be included. In the message from ASN GW to a BS, a single BS only can be included.
RRM Reporting Characteristics	Section 5.3.2.162	O	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified. In this message, only Bit#0 (periodic

IE	Reference	M/O	Notes
			reporting) and Bit#1 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset. If *Radio_Config_Update_Rpt* needs to be sent based on multiple events, then the corresponding bits have to be set to 1. If the optional reporting characteristics field is not specified, then the *Radio_Config_Update_Rpt* SHALL be sent only once. – This TLV is included based on local RRC policy. Decision to include this TLV is implementation specific.
RRM Reporting Period P	Section 5.3.2.163	O	The Time P is used by BS (RRA) as the reporting period. – If omitted, the BS SHALL apply a default value. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.

1　The message definition for the RRM R6 *Radio_Config_Update_Rpt* message is the same as the corresponding R4
2　message definition as specified in section 4.9.3.1.1.

7.3.3　R6 ASN Anchored Mobility Scenarios

4　This section discusses handover within the Profile C ASN. The Profile C ASN consists of one or more BSs and one
5　or more ASN GWs. The BSs SHALL be connected to the ASN GWs with R6 interfaces. The ASN GWs are
6　interconnected with R4 interfaces. This section discusses only R6 operations. R4 operations, if executed, are
7　identical to those described in Section 5.

8　With respect to R6 operations, the entities that participate in HO process are logically divided into the following
9　types:

10　　a.　Serving BS that hosts Serving HO Function and serves the MS prior to HO.

11　　b.　Target BS that hosts Target HO Function. There might be one or more Target BSs. One of them is selected as
12　　　　the final HO Target and becomes Serving BS after HO completion.

13　　c.　Relay ASN GW that relays HO Control messages between Serving and Target BSs over R6. The Relay
14　　　　ASNGW is an abstract functionality and in implementation can also take the role of any ASN GW that has an
15　　　　R6 interface with the Serving or Target BSs (e.g. Serving or Target ASN GWs). There could be multiple
16　　　　Relay ASN GWs involved in relaying HO Control Messages for a certain MS. The Relay ASNGW can also
17　　　　be a stateless or stateful relay. These are left as implementation options.

18　　d.　Anchor ASN GW that hosts the Anchor DP Function for the MS. Serving ASN GW MAY be located on the
19　　　　path between Anchor ASN GW and Serving BS. Target ASN GW MAY be located on the path between the
20　　　　Anchor ASN GW and Target BS. In this case each such Data Path has R6 segment and R4 segment. Since
21　　　　this section discusses only R6 operations, it is assumed in the text below that the Data Path between BSs and
22　　　　the Anchor GW goes directly over R6.

23　　e.　Authenticator ASN GW that hosts Authenticator/Key Distributor Function for the MS.

24　Data integrity may be optionally applied during the HO procedure to minimize or prevent data loss as a result of the
25　HO.

1 **7.3.3.1 Fully Controlled HO**

2 **7.3.3.1.1 HO Preparation Phase**

3 Upon reception of a MOB-MSHO_REQ message from a mobile station (MS), the Serving BS SHALL initiate a
4 handover to one or more candidate Target BSs by sending an R6 *HO_Req*(s) message(s). The Relay ASN GW
5 SHALL relay the message(s) to the Target BS(s) over the R6 interface(s).

6 The stateless Relay ASN GW used in the Profile C system has no HO related intelligence. In the Profile C system,
7 the Serving BS SHALL send a separate R6 *HO_Req* message for each Target BS.

8 The *R6 HO_Req* message SHALL contain an Authenticator ID TLV that points to the Authenticator/Key Distributor
9 Function hosted in the Authenticator ASN GW.

10 Upon receiving an R6 *HO_Req* message, the Target BS(s) MAY retrieve AK Context TLV from the Authenticator
11 ASN GW. The Target BS(s) is/are not required to retrieve this information immediately upon receipt of the R6
12 *HO_Req* message and MAY postpone the retrieval until the Handover Action Phase. This call flow scenario
13 (subsequently referred to as Scenario 1) is shown in Figure 0-1.

14 After receiving the R6 *HO_Req* message, each Target BS MAY pre-establish the data path for the MS with the
15 Anchor ASN GW, if the R6 *HO_Req* message includes the Anchor ASN GW ID TLV which points to the ASN GW
16 that hosts the Anchor DP Function. Data Path Pre-Registration at the Handover Preparation Phase is optional and
17 may be executed only when all entities involved support this functionality. If the Anchor ASN GW does not support
18 Data Path Pre-Registration and the Target BS attempts to initiate Data Path Pre-Registration procedure, the
19 transaction should be rejected (i.e. *Path_Prereg_Rsp* message with a rejection code TLV will be sent back to the
20 Target BS).

21 The Target BS(s) SHALL respond to the R6 *HO_Req* message with the R6 *HO_Rsp* message. The Relay ASN GW
22 relays the R6 *HO_Rsp* message to the Serving BS.

23 The Serving BS SHALL acknowledge the Handover Preparation transaction completion by sending an R6 *HO_Ack*
24 message back to the Target BS(s).

25 **7.3.3.1.1.1 R6 Data Path Pre-Registration Procedure**

26 The following call flow describes the R6 Path Pre-Registration procedure during handovers. Data Path Pre-
27 Registration is initiated by the Target BS(s).
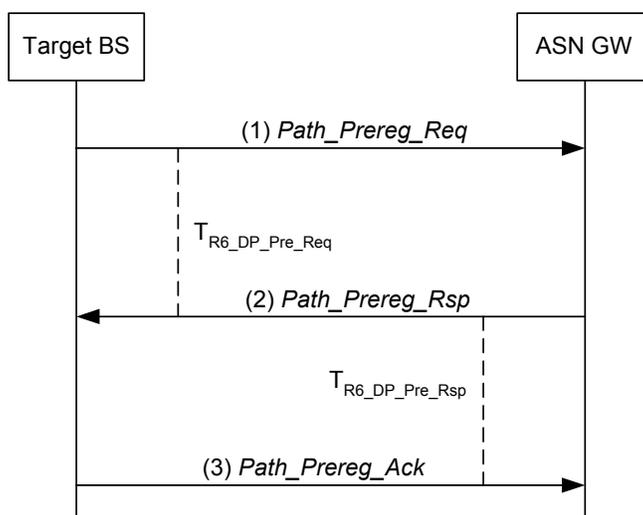
28

29 **Figure 7-26 – R6 Data Path Pre-Registration Procedure**

1 **STEP 1**

2 Target BS initiates pre-establishment of the data path for an MS by sending an R6 *Path_Prereg_Req* message to
3 ASN GW and starts timer $T_{R6\_DP\_Pre\_Req}$.

4 **STEP 2**

5 ASN GW sends an R6 *Path_Prereg_Rsp* message to the Target BS and starts timer $T_{R6\_DP\_Pre\_Rsp}$. Upon receipt of the
6 R6 *Path_Prereg_Rsp* message, Target BS stops timer $T_{R6\_DP\_Pre\_Req}$.

7 **STEP 3**

8 Target BS sends an R6 *Path_Prereg_Ack* message to ASN GW. Upon receipt of the R6 *Path_Prereg_Ack* message,
9 ASN GW stops timer $T_{R6\_DP\_Pre\_Rsp}$.

10 A transaction responder may reject a transaction by sending negative response with Failure Indication TLV

11 **7.3.3.1.1.2   R6 Authenticator Context Retrieval Procedure**

12 The following call flow describes the R6 Authenticator Context Retrieval procedure from an authenticator located in
13 the local ASN-GW (i.e. an ASN GW which has R6 interface with the BS). If not located locally, the R6
14 *Context_Req* and *Context_Rpt* messages will be further relayed by the local ASN-GW over R4 to the Anchor
15 Authenticator.
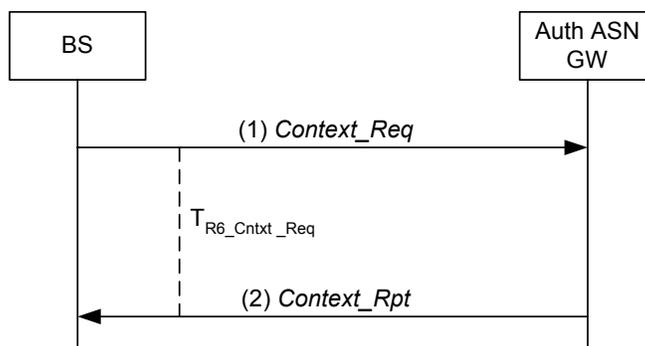
16

17 **Figure 7-27 – R6 Authenticator Context Retrieval Procedure**

18 **STEP 1**

19 BS sends an R6 *Context_Req* message to the Authenticator ASN GW to request the stored context associated with a
20 specified MS. The ASN GW starts timer $T_{R6\_Cntxt\_Req}$.

21 **STEP 2**

22 Authenticator ASN GW responds by sending the requested context information for the mobile in the R6
23 *Context_Rpt* message. Upon receipt of the R6 *Context_Rpt* message, BS stops timer $T_{R6\_Cntxt\_Req}$.

24 A transaction responder may reject a transaction by sending negative response with Failure Indication TLV

25 The following call flows describe the handover preparation scenarios described above. In the call flows it is assumed
26 that the Target BS and Serving BS are connected to the same Relay ASN-GW. If this is not the case, the R4
27 messaging (see section 4.7) is used to forward messages between Relay ASN-GWs

1   **7.3.3.1.1.3   MS Initiated HO Preparation**
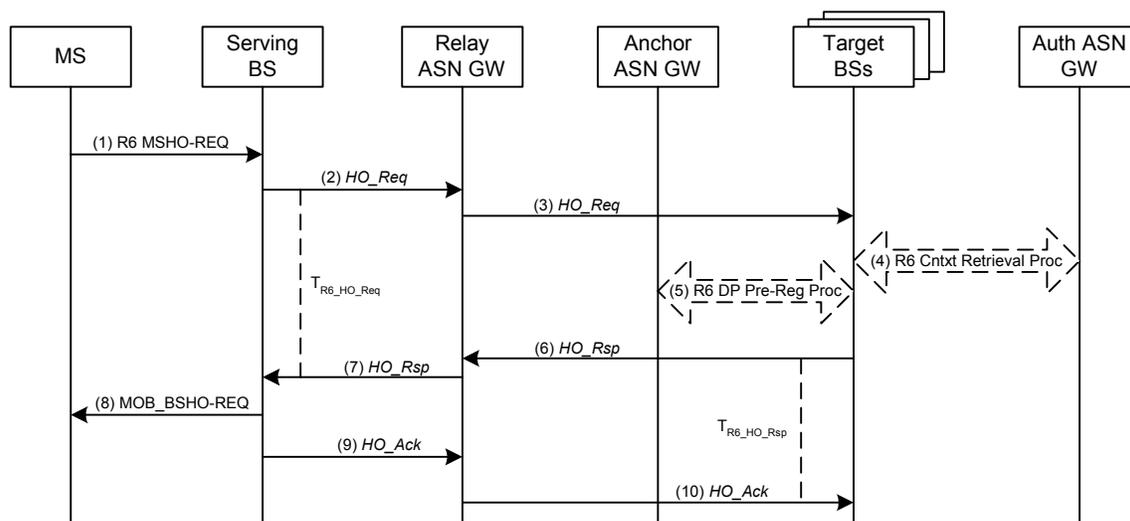
2

3   **Figure 7-28 – Successful MS Initiated HO Preparation Phase**

4   **STEP 1**

5   The MS initiates a handover by sending a MOB_MSHO-REQ message to the Serving BS, which includes one or
6   more potential Target BS's.

7   **STEP 2**

8   The Serving BS sends an R6 *HO_Req* message to each potential target BS selected for the handover and starts timer
9    $T_{R6\_HO\_Req}$ for each message. The message includes an Authenticator GW ID TLV that points to the
10   Authenticator/Key Distributor function at the Authenticator ASN and the Anchor ASN GW ID of the Anchor Data
11   Path function at the Anchor ASN.

12   **STEP 3**

13   The Relay ASN GW relays each R6 *HO_Req* message to the corresponding Target BS.

14   **STEP 4**

15   The Target BS(s) MAY request AK context for the MS by initiating a Context Retrieval procedure with the
16   Authenticator ASN GW. Note: The Target BS(s) may optionally choose to defer this procedure to the Handover
17   Action phase.

18   **STEP 5**

19   The Target BS(s) MAY initiate pre-establishment of a data path for the MS with the Anchor ASN GW. If the
20   Anchor ASN GW does not support the Data Path Pre-Registration, the R6 *Path_Prereg_Req* message from the
21   Target BS will be responded by the R6 *Path_Prereg_Rsp* message with an appropriate failure indication. Note: The
22   Target BS(s) may optionally choose to defer this procedure to the Handover Action phase.

23   **STEP 6**

24   The Target BS(s) sends an R6 *HO_Rsp* message to the Serving BS to respond to the handover request and starts
25   timer $T_{R6\_HO\_Rsp}$.

1 **STEP 7**

2 The Relay ASN GW relays the R6 *HO_Rsp* messages to the Serving BS. Upon receipt of the R6 *HO_Rsp* message,
3 the Serving BS stops timer $T_{R6\_HO\_Req}$.

4 **STEP 8**

5 The Serving BS sends a MOB_BSHO-RSP message to the MS containing one or more potential Target BS's
6 selected by the network for the MS to handover to.

7 **STEP 9**

8 The Serving BS sends an R6 *HO_Ack* message to the Target BS(s).

9 **STEP 10**

10 The Relay ASN GW relays the R6 *HO_Ack* message(s) to the corresponding Target BS(s). Upon receipt of the R6
11 *HO_Ack* message, the Target BS(s) stops timer $T_{R6\_HO\_Rsp}$.

12 **7.3.3.1.1.4   Network Initiated HO Preparation**
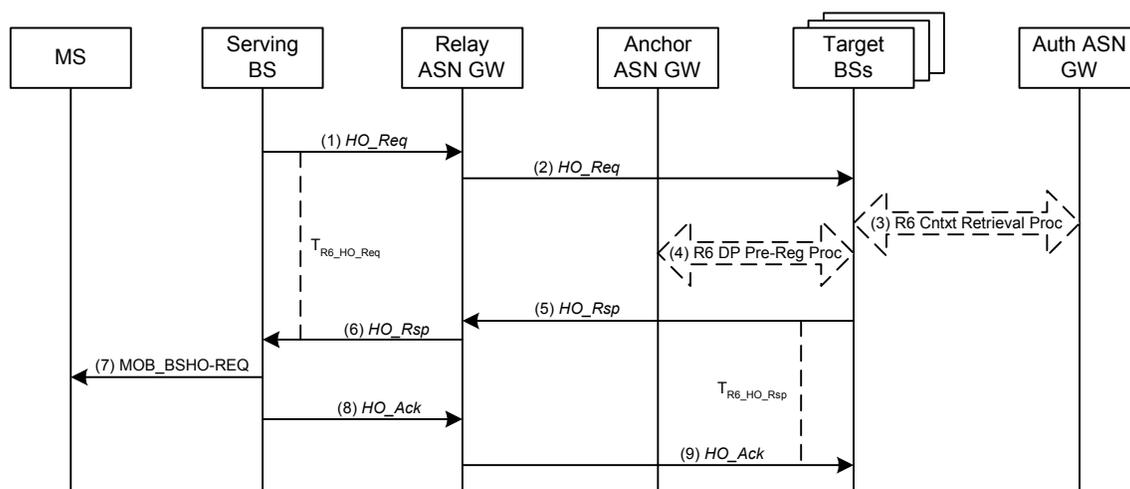
14 **Figure 7-29 – Successful Network Initiated HO Preparation Phase**

15 **STEP 1**

16 The Serving BS initiates a handover by sending an R6 *HO_Req* message to each potential target BS selected for the
17 handover and starts timer $T_{R6\_HO\_Req}$ for each message. The message includes an Authenticator GW ID TLV that
18 points to the Authenticator/Key Distributor function at the Authenticator ASN and the Anchor ASN GW ID of the
19 Anchor Data Path function at the Anchor ASN.

20 **STEP 2**

21 The Relay ASN GW relays the R6 *HO_Req* messages to the corresponding Target BS.

22 **STEP 3**

23 The Target BS(s) requests AK context for the MS by initiating a Context Retrieval procedure with the Authenticator
24 ASN GW. Note: The Target BS(s) may optionally choose to defer this procedure to the Handover Action phase.

1 **STEP 4**

2 The Target BS(s) MAY initiate pre-establishment of a data path for the MS with the Anchor ASN GW. If the
3 Anchor ASN GW does not support the Data Path Pre-Registration, the R6 *Path_Prereg_Req* message from the
4 Target BS will be responded by the R6 *Path_Prereg_Rsp* message with an appropriate falure indication. Note: The
5 Target BS(s) may optionally choose to defer this procedure to the handover action phase.

6 **STEP 5**

7 The Target BS(s) sends an R6 *HO_Rsp* message to the Serving BS to respond to the handover request and starts
8 timer $T_{R6\_HO\_Rsp}$.

9 **STEP 6**

10 The Relay ASN GW relays each R6 *HO_Rsp* message to the Serving BS. Upon receipt of the R6 *HO_Rsp* message,
11 the Serving BS stops timer $T_{R6\_HO\_Req}$.

12 **STEP 7**

13 The Serving BS sends a MOB_BSHO-REQ message to the MS containing one or more potential Target BS's
14 selected by the network for the MS to handover to.

15 **STEP 8**

16 The Serving BS sends an R6 *HO_Ack* message to the Target BS(s).

17 **STEP 9**

18 The Relay ASN GW relays the R6 *HO_Ack* message(s) to the corresponding Target BS(s). Upon receipt of the R6
19 *HO_Ack* message, the Target BS(s) stops timer $T_{R6\_HO\_Rsp}$.

20 **7.3.3.1.1.5   HO Preparation Stage Timers and Timing Considerations**

21 This section identifies the timer entities participating in the HO Preparation Phase. The following timers are defined
22 over R6:

23 • $T_{R6\_DP\_Pre\_Req}$: is started by the BS initiating pre-registration of the data path for an MS, upon sending the R6
24   *Path_Prereg_Req* message and is stopped upon receiving a corresponding R6 *Path_Prereg_Rsp* message.

25 • $T_{R6\_DP\_Pre\_Rsp}$: is started by the Anchor ASN GW responding to pre-establishment of the data path for an
26   MS, upon sending the R6 *Path_Prereg_Rsp* message and is stopped upon receiving a corresponding R6
27   *Path_Prereg_Ack* message.

28 • $T_{R6\_Cntxt\_Req}$: is started by the BSrequesting context for a specific MS, upon sending the R6 *Context_Req*
29   message and is stopped upon receiving a corresponding R6 *Context_Rpt* message.

30 • $T_{R6\_HO\_Req}$: is started by a Serving BS upon sending the R6 *HO_Req* message for an MS to a Target BS and
31   is stopped upon receiving a corresponding R6 *HO_Rsp* message from the Target BS.

32 • $T_{R6\_HO\_Rsp}$: is started by a Target BS upon sending the R6 *HO_Rsp* message for an MS to a Serving BS and
33   is stopped upon receiving a corresponding R6 *HO_Ack* message from the Serving BS.

34 Table 7-28 shows the default value of timers and also indicates the range of the recommended duration of these
35 timers.

36 **Table 7-28 – HO Preparation Phase Timer Values for R6**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\text{-}DP\_Pre\text{-}Req}$	TBD		TBD
$T_{R6\_DP\_Pre\_Rsp}$	TBD		TBD

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_Cntxt\_Req}$	TBD		TBD
$T_{R6\_HO\_Req}$	TBD		TBD
$T_{R6\_HO\_Rsp}$	TBD		TBD

1 **7.3.3.1.1.6   HO Preparation Stage Error Conditions**

2 This section describes error conditions associated with the HO Preparation Phase.

3 **7.3.3.1.1.6.1   Timer Expiry**

4 Table 7-29 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
5 expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s)
6 should be performed as indicated in Table 7-29.

7 **Table 7-29 – Timer Expiry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_DP\_Pre\_Req}$	BS initiating Path Pre-Registration procedure	No action required
$T_{R6\_DP\_Pre\_Rsp}$	ASN GW responding to *Path_Prereg_Req* message	No action required
$T_{R6\_Cntxt\_Req}$	BS Requesting context information	No action required
T_{R6-HO_Req}	Serving BS	The BS may re-try HO to another Target BS. If no Target BS can be reached, it SHALL send MS a MOB_BSHO-RSP with Mode set to 0b111
$T_{R6\_HO\_Rsp}$	Target BS	No action required

8 **7.3.3.1.1.6.2   R6 Context_Rpt Error**

9 Upon receipt of the R6 *Context_Req* message, if the ASN GW is unable to provide the requested information it
10 SHALL send an R6 *Context_Rpt* message with the Failure Indication TLV to the sender of the R6 *Context_Req*
11 message. Upon receipt of the R6 *Context_Rpt* message with Failure Indication TLV, the BSSHALL stop timer
12 $T_{R6\_Cntxt\_Req}$ (if running), and MAY resend the R6 *Context_Req* message. If the BS does not resend the R6
13 *Context_Req* message or if subsequent attempts are also unsuccessful, then the BS MAY send a R6 *HO_Rsp*
14 message with suitable error code included in the Result Code TLV.

15 **7.3.3.1.1.6.3   R6 HO_Rsp Error**

16 Upon receipt of the R6 *HO_Req* message, if the Target BS is unable to support the requested HO, then it SHALL
17 send R6 *HO_Rsp* message with suitable error code included in the Result Code TLV. Upon receipt of the R6
18 *HO_Rsp* message indicating HO cannot be supported at a Target BS, the Serving BS SHALL stop $T_{R6\_HO\_Req}$ (if
19 running), and MAY re-send the R6 *HO_Req* message to a different Target BS. If the Serving BS does not re-send
20 the R6 *HO_Req* message, or if all subsequent Target BSs cannot support the HO, in the case of MS Initiated
21 handover, the Serving BS SHALL send a MOB_BSHO_RSP with mode = 0b111 to the MS.

22 **7.3.3.1.1.6.4   R6 Path_Prereg_Rsp Error**

23 Upon receipt of the R6 *Path_Prereg_Req* message, if the ASN GW is unable to support the pre-establishment of a
24 data path, then it SHALL send a R6 *Path_Prereg_Rsp* message with suitable error code.

1 Upon receipt of the R6 *Path_Prereg_Rsp* message with suitable error code, the BS SHALL stop $T_{R6-DP\_Pre-Req}$ (if
2 running).

7.3.3.1.2 HO Action Phase

4 The HO Action Phase begins when the MS leaves the Serving BS. The MS sends a MOB_HO-IND message to the
5 Serving BS in which it specifies which of the Target BSs has been selected for the handover. The MOB_HO-IND
6 message is the last message the MS sends to the Serving BS. After sending MOB_HO-IND the MS may start
7 ranging with the Target BS.

8 Upon receiving MOB_HO-IND, the Serving BS SHALL generate an R6 *HO_Cnf* message and send it to the Target
9 BS via Relay ASN GW as shown in Figure 0-3. The R6 *HO_Cnf* message includes the "most recent MAC context"
10 at the Serving BS.

11 Upon receiving R6 *HO_Cnf* message with the HO_Indication type whose value is not set to "Cancel", the Target BS
12 SHALL retrieve the AK Context if this information was not retrieved during the Handover Preparation Phase. This
13 call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 7-34.

14 If the data path between the Anchor ASN GW and the Target BS was not pre-established during the Preparation
15 Phase, it MAY be pre-established after receiving R6 *HO_Cnf* message and before the MS starts Network Re-Entry
16 at the Target BS.

17 The data paths between the Anchor ASN GW and the Target BS SHALL be established via Data Path Registration
18 procedure after the MS either starts or completes Network Re-Entry at the Target BS[35].

19 If Data Path Registration procedure is invoked after the data paths had been pre-registered, the procedure only
20 confirms final establishment of the pre-registered data paths and does not convey any parameters of the data paths
21 except MSID. In this case, all the parameters that are related to the data paths SHALL be exchanged during the
22 preceding Data Path Pre-Registration transaction. Furthermore, the Data Path Registration transaction is completed
23 with a two-way handshake; *Path_Reg_Req* and *Path_Reg_Rsp* message exchange and no *Path_Reg_Ack* message
24 (i.e. two-way handshake).

25 If no Data Path Pre-Registration procedure had been completed prior to the Data Path Registration procedure, the R6
26 *Path_Reg_Req* and *Path_Reg_Rsp* messages SHALL convey all parameters relevant for the setup of Data Paths. In
27 this case the R6 *Path_Reg_Ack* message SHALL be sent in response to R6 *Path_Reg_Rsp* message (i.e. three-way
28 handshake).

29 Upon completion of Data Path Registration procedure, the Anchor ASN GW SHALL initiate de-registration of all
30 the pre-registered data paths to the candidate Target BSs that have not been selected for the final handover target.
31 Also, the Anchor ASN GW SHALL initiate de-registration of the data path between the (old) Serving BS and itself.

32 If the Serving BS determines that the MOB_HO_IND message was not received from the MS due to a
33 communication loss with the mobile[36], for example upon expiration of internal timer[37], the Serving BS MAY send
34 the R6 *HO_Cnf* message - value for the HO_Indication type should be set to a "Unconfirmed"- which may include
35 all "most recent MAC context".   The R6 *HO_Cnf* message SHALL be sent to the set of Target BSs (via the Relay
36 ASN GW) that were included in the previous MOB_BSHO-REQ or MOB_BSHO-RSP message that was sent by the
37 Serving BS to the MS. The R6 *HO_Cnf* message may also be sent to target BSs which weren't notified of a potential
38 impending handover from the MS during the handover preparation phase and whose target BSs weren't included in
39 the MOB_BSHO-REQ or MOB_BSHO-RSP messages (e.g candidate target BSs which were included in the
40 MOB_MSHO-REQ message sent by the MS but weren't notified of the handover in the handover preparation
41 phase). The message includes authenticator context and latest MAC context for the MS. Upon sending the R6

---

[35] If Path Registration is initiated before MS completes Network Reentry there is a probability that MS will not complete the
Network Re-Entry where it has started because the RNG-RSP might be lost in the air. In this case the Data Path will have to be
registered again, possibly with another Target BS.

[36] MOB_HO-IND message could be lost over the air or not sent by the MS because it didn't receive the MOB_BSHO-RSP
message from the BS in the MS initiated handover case, or it didn't receive the MOB_BSHO-REQ from the BS in the network
initiated handover case.

[37] For example, $T_{MOB\_HO\_IND}$

1 *HO_Cnf* message to the candidate Target BS(s), the Serving BS SHALL stop all the downlink and uplink scheduling
2 for the data transmission and reception from the MS respectively.

3 Upon sending the R6 *HO_Cnf* message, if the Resource_Retain flag was not set, the Serving BS SHALL discard all
4 MS's connections resource information including the MAC state machine and all outstanding buffered PDUs, else
5 the Serving BS SHALL retain the connections, MAC state machine and PDUs associated with the MS for service
6 continuation until the expiration of Resource Retain Timer.

7 The Serving BS SHALL release all MAC context and MAC PDUs associated with the MS upon reception of a R6
8 *HO_Complete* message from the Target BS indicating MS committed Network Attachment at the Target BS.

9 If the Target BS does not receive the R6 *HO_Cnf* message before the MS starts Network Reentry, the Target BS
10 MAY request the "most recent MAC Context" via *Context_Req* and *Context_Rpt* exchange with the Serving BS as
11 shown in Scenario 2.

12 Immediately after the MS completes Network Re-entry, the Target BS (which at that moment becomes new Serving
13 BS) SHALL send CMAC Key Count Update message to the Authenticator ASN GW to notify the successful HO
14 completion at the selected Target BS. The message SHALL deliver to the Authenticator the value of the
15 CMAC_KEY_COUNT which is received from the MS. or details of CMAC Key Count Update, refer to section
16 4.3.4.2.

17 As soon as the MS Network Re-entry procedure at the Target BS is completed, the Target BS MAY send an R6
18 *HO_Complete* message to the Serving BS to expedite the resource release in the Serving BS.

19 **7.3.3.1.2.1   Data Path Registration Procedure**

20 Data Path Registration procedure takes place between the Target BS and ASN GW immediately after the MS has
21 arrived at the Target BS.
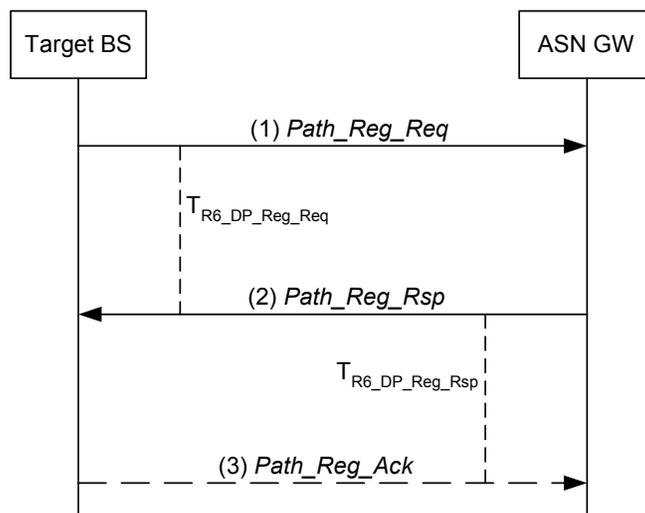
22

23 **Figure 7-30 – Data Path Registration Procedure**

24 **STEP 1**

25 Target BS initiates Data Path Registration procedure by sending an R6 *Path_Reg_Req* message to ASN GW and
26 starts timer $T_{R6\_DP\_Reg\_Req}$.

27 **STEP 2**

28 ASN GW sends an R6 *Path_Reg_Rsp* message to Target BS and, if no Data Path Pre-Registration procedure has
29 been completed prior to the Data Path Registration transaction, starts timer $T_{R6\_DP\_Reg\_Rsp.}$ Upon receipt of the R6
30 *Path_Reg_Rsp* message, Target BS stops timer $T_{R6\_DP\_Reg\_Req}$

1 **STEP 3**

2 If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then
3 Target BS sends an R6 *Path_Reg_Ack* message to ASN GW. Upon receipt of the R6 *Path_Reg_Ack* message, ASN
4 GW stops timer $T_{R6\_DP\_Reg\_Rsp.}$

5 A transaction responder may reject a transaction by sending negative response with Failure Indication TLV

6 **7.3.3.1.2.2   Path De-Registration Procedure**

7 Path De-Registration Procedure is shown in Figure 7-31:
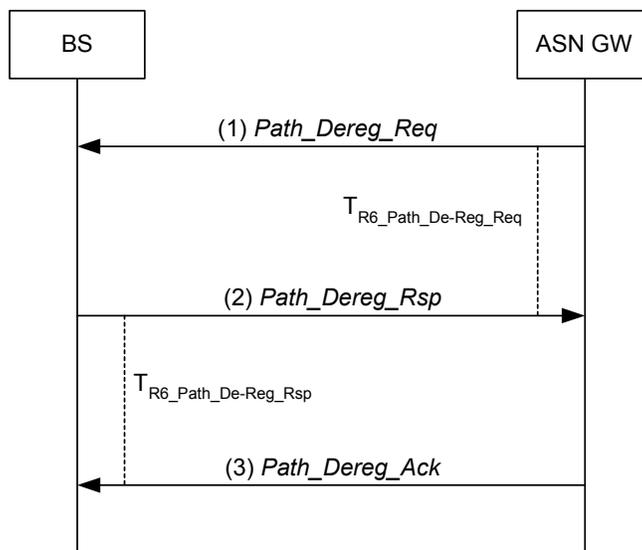
8

9 **Figure 7-31 – Path De-Registration Procedure**

10 **STEP 1**

11 ASN GW initiates Data Path De-Registration procedure by sending an R6 *Path_Dereg_Req* message to BS and
12 starts timer $T_{R6\_Path\_De-Reg\_Req}$.

13 **STEP 2**

14 BS sends an R6 *Path_Dereg_Rsp* message to ASN GW. Upon receipt of the R6 *Path_Dereg_Rsp* message, ASN
15 GW stops timer $T_{R6\_Path\_De-Reg\_Req}$.

16 **STEP 3**

17 ASN GW sends an R6 *Path_Dereg_Rsp* message to BS. Upon receipt of the R6 *Path_ Dereg_Rsp* message, BS
18 stops timer $T_{R6\_Path\_De-Reg\_Rsp}$.

19 **7.3.3.1.2.3   CMAC Key Count Update Procedure**

20 CMAC Key Count Update procedure appears below and assumes the authenticator is located in the local ASN-GW
21 (i.e. an ASN GW which has R6 interface with the BS). If not located locally, the R6 CMAC Key Count Update and
22 Acknowledge messages will be further relayed by the local ASN-GW over R4 to the Anchor Authenticator.

1
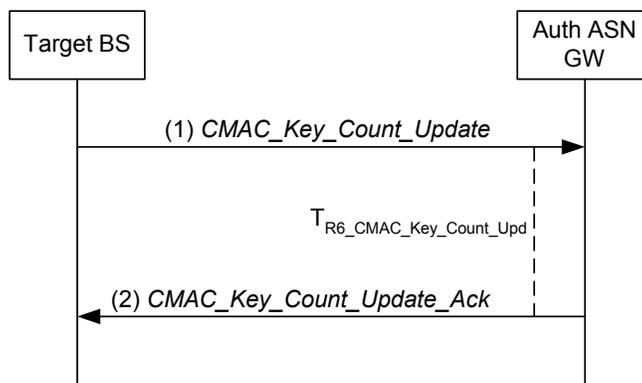
2 **Figure 7-32 – CMAC Key Count Update Procedure**

3 **STEP 1**

4 Target (New Serving) BS initiates CMAC Key Count Update procedure by sending an R6
5 *CMAC_Key_Count_Update* message to ASN GW and starts timer $T_{R6\_CMAC\_Key\_Count\_Upd}$. If the ASN GW is not
6 hosting the Authenticator for the MS, it will forward this message to the Authenticator ASN via the R4
7 *CMAC_Key_Count_Update* message (see section 5.7.2.1.3).

8 **STEP 2**

9 Upon receipt of R4 *CMAC_Key_Count_Update_Ack* message from the Authenticator ASN, the ASN-GW sends an
10 R6 *CMAC_Key_Count_Update_Ack* message to Target BS. Upon receipt of the R6 *CMAC_Key_Count_Update_Ack*
11 message, Target BS stops timer $T_{R6\_CMAC\_Key\_Count\_Upd}$.

12 **7.3.3.1.2.4   MAC Context Retrieval Procedure**

13 MAC Context Retrieval Procedure is shown in Figure 7-33.

14
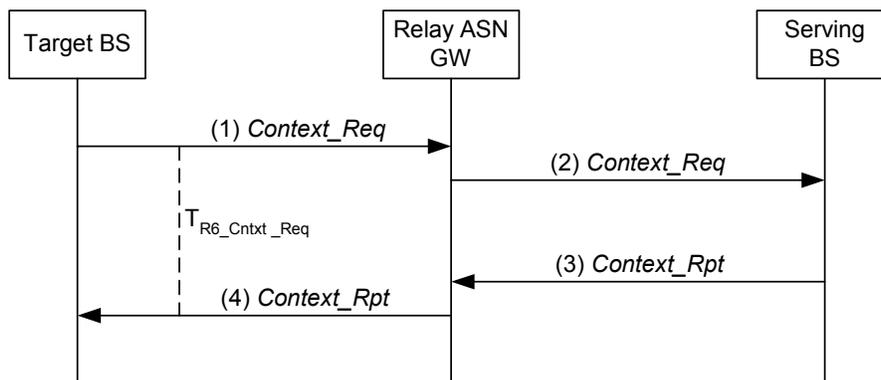
15 **Figure 7-33 – MAC Context Retrieval Procedure**

16 **STEP 1**

17 Target BS sends an R6 *Context_Req* message to request the context associated with a specified MS stored in the
18 Serving BS. The Target BS starts timer $T_{R6\_Cntxt\_Req}$.

19 **STEP 2**

20 Relay ASN GW relays the message to the Serving BS

1   **STEP 3**

2   Serving BS responds by sending the requested context information for the mobile in the R6 *Context_Rpt* message.

3   **STEP 4**

4   Relay ASN GW relays the message to the Target BS. Upon receipt of the R6 *Context_Rpt* message, Target BS stops
5   timer T$_{R6\_Cntxt\_Req}$.

6   The following sections describe call flows associated with the Handover Action Phase. In the call flows it is
7   assumed that the target BS and Serving BS are connected to the same Relay ASN-GW. If this is not the case, the R4
8   messaging (see xxxx) is used to forward messages between Relay ASN-GWs

9   **7.3.3.1.2.5   Handover Action Scenario 1: Serving BS Sends R6 HO_Cnf after receiving MOB_HO-IND**

10   The following call flow describes a successful handover action scenario where the Serving BS receives MOB_HO-
11   IND and sends the R6 *HO_Cnf* message to the Target BS (via Relay ASN GW).

12
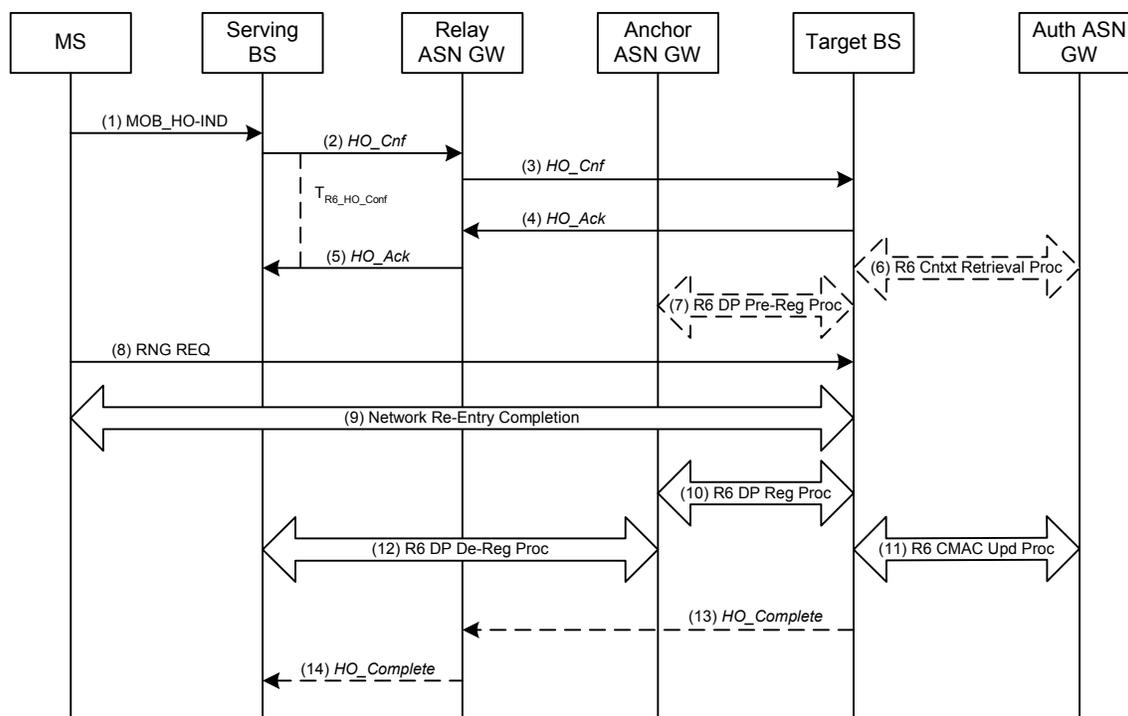
13   **Figure 7-34 – Successful HO Action Phase, Scenario 1**

14   **STEP 1**

15   The MS sends a MOB_HO-IND to the Serving BS to notify a handover to one of the Target BSs selected by the
16   Serving BS in the Handover Preparation phase.

17   **STEP 2**

18   Upon reception of the MOB_HO-IND the Serving BS sends an R6 *HO_Cnf* message and starts timer T$_{R6\_HO\_Conf}$.

19   **STEP 3**

20   Relay ASN GW relays the R6 *HO_Cnf* message over R6.

STEP 4

The Target BS sends an R6 *HO_Ack* message.

STEP 5

Relay ASN GW relays the R6 *HO_Ack* message over R6. Upon receipt of the R6 *HO_Ack* message, the Serving BS stops timer T$_{R6\_HO\_Conf}$.

STEP 6

If AK context for the MS was not retrieved during the Handover Preparation phase, the Target BS requests AK context for the MS by initiating a Context Retrieval procedure with the Authenticator ASN. Otherwise, this step SHALL be skipped.

STEP 7

If the Data Path Pre-Registration procedure did not occur during the Preparation Phase, the Data Path Pre-Registration procedure may take place at this moment.

STEP 8

The MS initiates network re-entry with the Target BS by sending RNG-REQ.

STEP 9

The Target BS responds with RNG-RSP and the MS and the Target BS complete Network Reentry.

STEP 10

Target BS initiates Data Path Registration procedure with the Anchor ASN GW. This procedure MAY take place immediately after STEP 8.

STEP 11

Immediately after completing Network Reentry, Target BS initiates CMAC Key Count Update procedure and updates the Authenticator ASN GW with the latest CMAC Key Count value received from MS.

STEP 12

Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN GW initiates Path De-Registration procedure with the old Serving BS. Also, the Anchor ASN GW SHALL de-register all the pre-registered data paths with the other unselected candidate Target BSs. See discussion in 7.3.3.1.2.8 for more details.

STEP 13

Upon completion of network re-entry, the Target BS may send an R6 *HO_Complete* message to notify the completion of the handover.

STEP 14

Relay ASN GW relays the R6 *HO_Complete* message over R6 to the Serving BS. Upon receipt of the R6 *HO_Complete* message, the Serving BS releases the MS context.

7.3.3.1.2.6   Handover Action Scenario 2: Serving BS Proactively Sends HO_Cnf

The following call flow describes a successful handover action scenario where the Serving BS doesn't receive MOB_HO-IND because the message is lost in the air, and sends the R6 *HO_Cnf* messages to the entire set of the Target BSs (via Relay ASN GW). See also section 4.7.2.2.4.

1
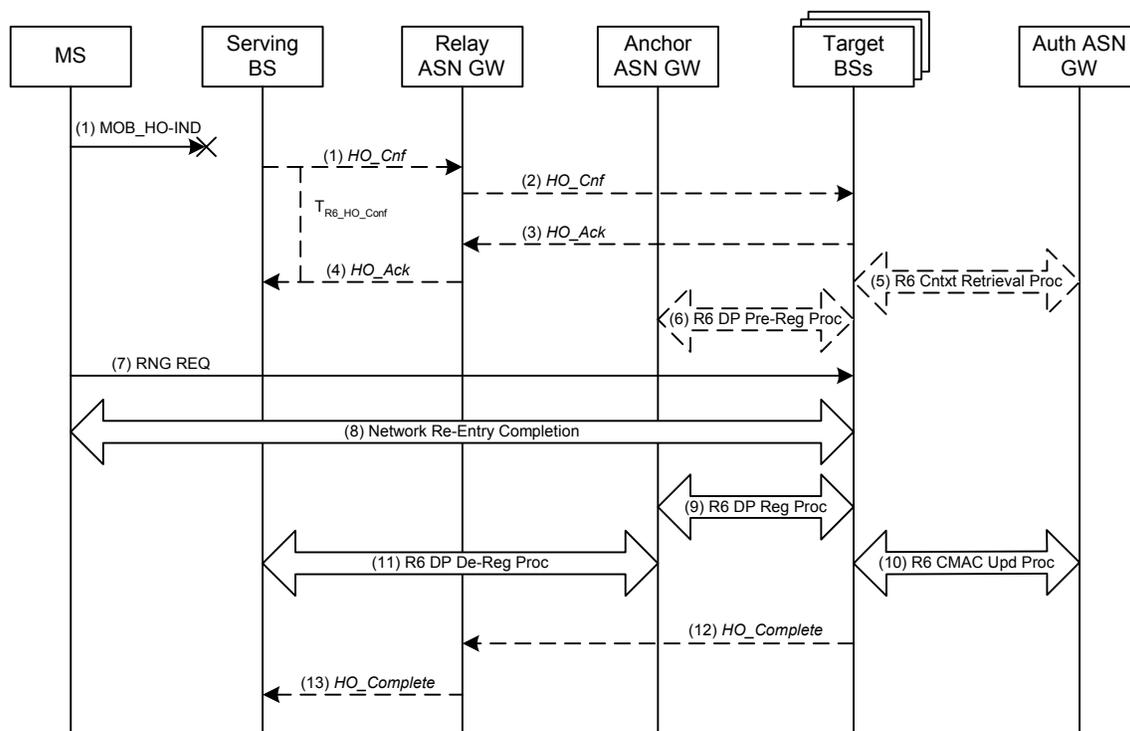
2   **Figure 7-35 – Successful HO Action Phase, Scenario 2**

3   The step description is the same as in 7.3.3.1.2.5 with one difference – in this case, in step 1, the serving BS sends
4   multiple R6 *HO_Cnf* messages. The R6 *HO_Cnf* message may also be sent to candidate targets BSs the MS may
5   chose to handover to which weren't previously notified of a potential handover from the MS during handover
6   preparation. The R6 *HO_Cnf* message includes the HO_Indication Type set to "Unconfirmed", authenticator context
7   information for the MS, and the most recent MAC content for the MS.

8   **7.3.3.1.2.7   Handover Action Scenario 3: Serving BS Does Not Send R6 HO_Cnf**

9   The following call flow describes a successful Handover Action scenario where the MOB_HO-IND sent by the MS
10   to the Serving BS was lost over the air and not received by the Serving BS, and/or the R6 *HO_Cnf* message sent by
11   the Serving BS to the Target BS was either delayed or not received. The MS completes network re-entry at one of
12   the Target BSs selected by the Serving BS during the Handover Preparation phase.

1
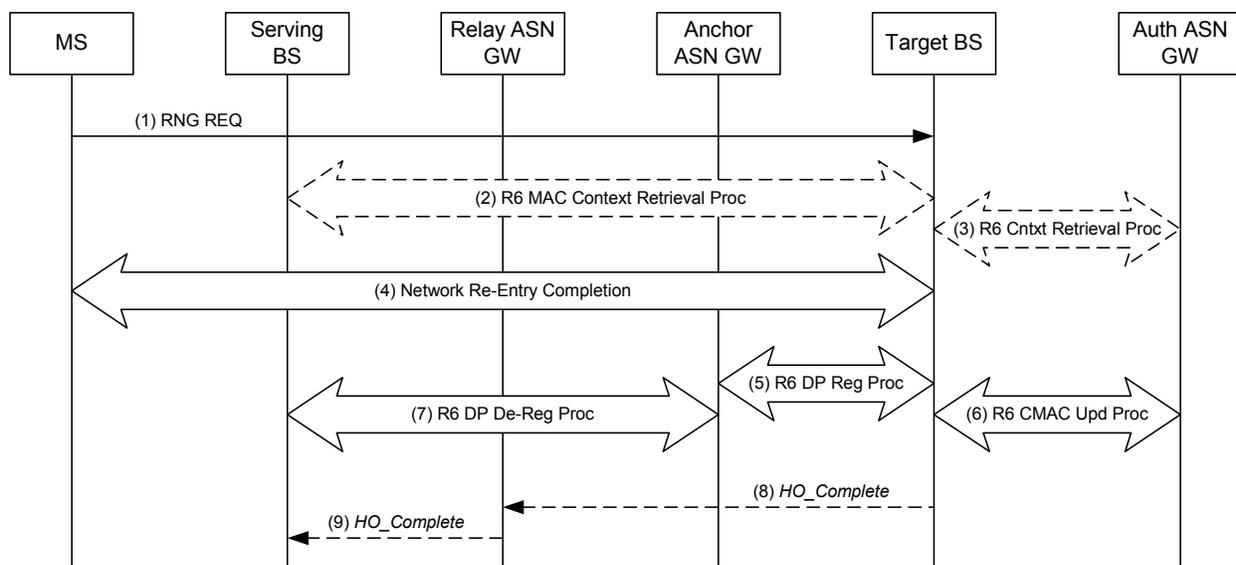
2 **Figure 7-36 – Successful HO Action Phase, Scenario 3**

3 **STEP 1**

4 The MS initiates network re-entry with the Target BS by sending RNG-REQ.

5 **STEP 2**

6 If the Target BS needs to synchronize the dynamic MAC context it initiates a Context Request procedure with the
7 Serving BS to retrieve the latest MAC context for the MS.

8 **STEP 3**

9 If AK Context was not obtained during the Handover Preparation phase, the Target BS requests AK context for the
10 MS by initiating a Context Retrieval procedure with the Authenticator ASN. This step might have been executed in
11 the Preparation stage and shown as optional in the Action Phase.

12 **STEP 4**

13 The Target BS responds with RNG-RSP and the MS and the Target BS complete Network Reentry.

14 **STEP 5**

15 Target BS initiates Data Path Registration procedure with the Anchor ASN GW. This procedure MAY take place
16 immediately after STEP 3.

17 **STEP 6**

18 Immediately after completing Network Reentry, Target BS initiates CMAC Key Count Update procedure and
19 updates the Authenticator ASN GW with the latest CMAC Key Count value received from MS.

20 **STEP 7**

21 Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN GW initiates Data Path
22 De-Registration procedure with the old Serving BS. Also, the Anchor ASN GW SHALL de-register all the pre-
23 registered data paths with the other not selected Target BSs. See discussion in 7.3.3.1.2.8 for more details.

1   **STEP 8**

2   Upon completion of network re-entry, the Target BS may send an R6 *HO_Complete* message to notify the
3   completion of the handover.

4   **STEP 9**

5   Relay ASN GW relays the R6 *HO_Complete* message over R6 to the Serving BS. Upon receipt of the R6
6   *HO_Complete* message, the Serving BS releases the MS context.

7   **7.3.3.1.2.8   Path De-Registration with Old Serving and Unselected Target BSs**

8   R6 Path Registration Procedure between the finally selected Target BS and Anchor ASN GW triggers R6 Path
9   Deregistration of the Data Path between the Anchor ASN GW and the old Serving BS as well as between the
10   Anchor ASN GW and each of the Unselected Target BSs. In the later case the procedure takes place if the
11   corresponding Data Paths were previously pre-registered. The scenario is shown in Figure 7-37.
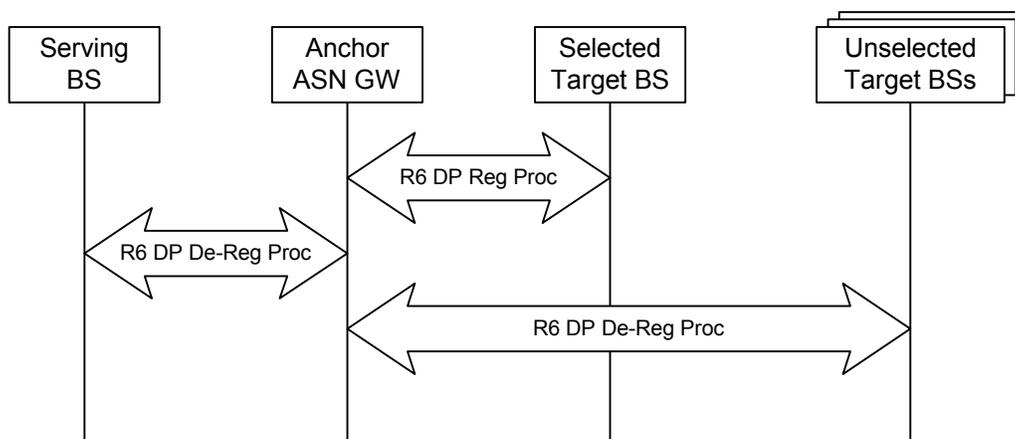
12

13   **Figure 7-37 –Path De-Registration with Old Serving and Unselected Target BSs**

14   All R6 Path Deregistration Procedures shown are independent of each other and may happen simultaneously.

15   **7.3.3.1.2.9   HO Action Phase Timers and Timing Considerations**

16   This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over
17   R6:

18   • $T_{R6\_DP\_Reg\_Req}$: is started by the Target BS to initiate establishment or provide confirmation of the data paths
19   for an MS, upon sending the R6 *Path_Reg_Req* message, and is stopped upon receiving a corresponding
20   R6 *Path_Reg_Rsp* message.

21   • $T_{R6\_DP\_Reg\_Rsp}$: is started by the Anchor ASN GW upon sending the R6 *Path_Reg_Rsp* message if no data
22   path has been pre-established for the MS, and is stopped upon receiving a corresponding R6 *Path_Reg_Ack*
23   message.

24   • $T_{R6\_DP\_Dereg\_Req}$: is started by the Anchor ASN GW after completion of the Data Path Registration procedure
25   for an MS, upon sending the R6 *Path_Dereg_Req* message, and is stopped upon receiving a corresponding
26   R6 *Path_Dereg_Rsp* message.

27   • $T_{R6\_CMAC\_Key\_Count\_Upd}$: is started by a Target (now new Serving) BSafter MS completes network re-entry,
28   upon sending the R6 *CMAC_Key_Count_Update* message to the Authenticator ASN, and is stopped upon
29   receiving a corresponding R6 *CMAC_Key_Count_Update_Ack* message from the Authenticator ASN.

30   • $T_{R6\_HO\_Conf}$: is started by the Serving BS when sending a R6 *HO_Cnf* message to a Target BS, and is
31   stopped upon receiving a R6 *HO_Ack* message from the corresponding Target BS.

1   Table 7-30 shows the default value of timers and also indicates the range of the recommended duration of these
2   timers.

3   **Table 7-30 – HO Action Phase Timer Values for R6**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_DP\_Reg\_Req}$	TBD		TBD
$T_{R6\_DP\_Reg\_Rsp}$	TBD		TBD
$T_{R6\_Path\_De-Reg\_Req}$	TBD		TBD
$T_{R6\_Path\_De-Reg\_Req}$	TBD		TBD
$T_{R6\_CMAC\_Key\_Count\_Upd}$	TBD		TBD
$T_{R6\_HO\_Conf}$	TBD		TBD

4   **7.3.3.1.2.10   HO Action Phase Error Conditions**

5   This section describes error conditions associated with the HO Action Phase.

6   **7.3.3.1.2.10.1   Timer Expiry**

7   Table 7-31 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer
8   expiry, if the maximum retries has not exceeded, the related message is retransmitted and the timer is restarted.
9   Otherwise, the corresponding action(s) should be performed as indicated in Table 7-31.

10   **Table 7-31 – Timer Expiry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_DP\_Reg\_Req}$	Target BS	BS SHALL force MS to perform initial network entry
$T_{R6\_DP\_Reg\_Rsp}$	Anchor ASN-GW	ASN GW SHALL defer sending the downlink packets until it receives any packets for MS from Target(new Serving) BS. ASN GW SHALL reset data paths for MS if no packets are received until a pre-specified system timer expires.
$T_{R6\_Path\_De-Reg\_Req}$	Anchor ASN-GW	No action required
$T_{R6\_Path\_De-Reg\_Req}$		
$T_{R6\_CMAC\_Key\_Count\_Upd}$	Target (new Serving) BS	BS SHALL force MS to perform initial network entry
$T_{R6\_HO\_Conf}$	(old) Serving BS	No action required

11   **7.3.3.1.2.10.2   R6 Path_Reg_Rsp Error**

12   Upon receipt of the R6 *Path_Reg_Req* message, if the Anchor ASN-GW is unable to support the requested
13   establishment of the data path(s), then it SHALL send a R6 *Path_Reg_Rsp* message with suitable error code.

14   Upon receipt of the R6 *Path_Reg_Rsp* message with suitable error code, the Target (new serving) BSSHALL stop
15   $T_{R6\_DP\_Reg\_Req}$ (if running).The Target BS MAY re-send the R6 *Path_Reg_Req* message. If the Target BS does not
16   resend the R6 *Path_Reg_Req* message or if subsequent attempts are also unsuccessful, the Target BS SHALL force
17   the MS to perform a full network re-entry

1   **7.3.3.2   Uncontrolled HO**

2   An Uncontrolled (Unpredictive) handover occurs when an MS starts ranging at a Target BS that was not previously
3   notified of an impending handover from an MS and did not participate in the Handover Preparation Phase. This may
4   occur due to suboptimal radio planning conditions or MS implementation (handover notification to the Serving BS
5   by MS is optional).

6   If an MS starts ranging with a BS that doesn't have MS Context information including Authenticator GW and
7   Anchor ASN GW identifiers, the RNG-REQ message from the MS cannot be authenticated. In a worst case scenario
8   a full Network Re-Entry will be required which results in a large delay, because some authentication methods may
9   take seconds to complete, especially if the Home AAA Server is located far away and the communication is slow.

10   However if the MS includes the Serving BS ID TLV in the RNG-REQ message, the handover can still be completed
11   in a reasonable delay and the period of traffic unavailability can be greatly reduced. When an MS re-enters at a
12   Target BS and supplies its Serving BS ID in the RNG-REQ message, the Target BS may retrieve the relevant MS
13   Context from the Serving BS including the Authenticator GW ID and Anchor ASN GW ID. Thus it becomes
14   possible for the Target BS to authenticate the RNG-REQ and perform data path registration with the Anchor ASN
15   GW. This call flow scenario is described in Figure 5-29.

16   Network Re-Entry might be completed immediately after receiving the MS Context or after data path establishment
17   (the latter case is shown in the call flows). The former method requires a lower Ranging Response Timeout in the
18   MS, however it also requires holding the uplink traffic until the data path is established. The latter method doesn't
19   require traffic holding but relies on larger Ranging Response Timeout in the MS. The moment of Network Re-Entry
20   completion does not affect interoperability and is left as a vendor implementation option.

21   The following call flow provides an example of a successful uncontrolled handover scenario. A MS begins ranging
22   at a Target BS that wasn't contacted by the Serving BS to participate in the Handover Preparation phase. Therefore
23   the Target BS was unaware of an impending arrival of the MS. The Target BS retrieves the MS context and
24   Authentication information, and successfully completes the handover.
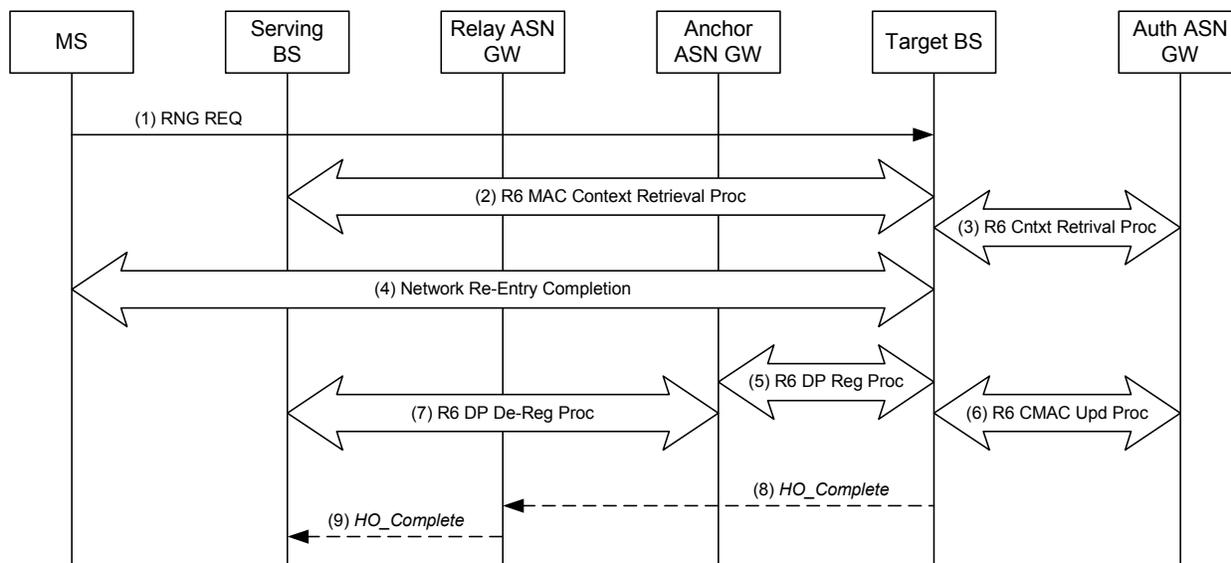
26   **Figure 7-38 – Uncontrolled (Unpredictive) HO**

27   **STEP 1**

28   An MS performs an uncontrolled handover by sending an RNG-REQ message to perform contention based ranging
29   at a Target BS that didn't receive prior notification of an impending handover from the MS and therefore did not
30   participate in the Handover Preparation phase. The MS includes the Serving BS ID TLV in the RNG-REQ message.

STEP 2

The Target BS initiates a MAC Context Retrieval procedure with the Serving BS to retrieve context information for the MS. The Serving BS responds by sending the context information that includes the Authenticator GW ID and Anchor ASN GW ID.

STEP 3

The Target BS requests AK context for the MS by initiating a Context Retrieval procedure with the Authenticator ASN GW.

STEP 4

Target BS uses the Authenticator context to authenticate the MS message. The Target BS sends a RNG-RSP message to the MS acknowledging the HMAC/CMAC tuple (expedited security authentication) and containing the HO Process Optimization TLV.

STEP 5

The Target BS initiates data path registration for the MS with the Anchor ASN GW. Note: This step may occur any time after STEP 3.

STEP 6

Upon successful completion of MS Network Re-entry, the Target BS initiates a CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key Count.

STEP 7

The Anchor ASN GW initiates an R6 Path De-Registration procedure with the Serving BS.

STEP 8

Upon completion of network re-entry, the Target BS may send an R6 *HO_Complete* message to notify the completion of the handover.

STEP 9

Relay ASN GW relays the R6 *HO_Complete* message over R6 to the Serving BS. Upon receipt of the R6 *HO_Complete* message, the Serving BS releases the MS context.

7.3.3.3   Message Definitions

The composition of the R6 messages is identical to the composition of the corresponding R4 messages described in section 5.7.1.2.x